



CIS Community Defense Model

Version 2.0

Acknowledgments

The Center for Internet Security[®] (CIS) would like to thank the many security experts who volunteer their time and talent to support the CIS Controls[®] and other CIS work, especially the Community Defense Model (CDM). CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

We also acknowledge and greatly appreciate the work of the Verizon Data Breach team, CrowdStrike[®], and the many contributors to the MITRE ATT&CK[®] framework. They are representative of the large community of technical excellence, good will, and open sharing that allows all of us to build greater confidence into the cyber world.

Editor Valecia Stocchetti, CIS

Contributors

Ginger Anderson, CIS Jennifer Jarose, CIS Joshua M. Franklin, CIS Joshua Palsgraf, CIS/MS-ISAC Leanna Caton, CIS/MS-ISAC Michael Woodward, CIS/MS-ISAC Patrick Araya, CIS Philippe Langlois, Verizon Phyllis Lee, CIS Randy Rose, CIS/MS-ISAC Richard Nelson, CIS/MS-ISAC Robin Regnier, CIS Samuel P. Farnan, CIS/MS-ISAC Stephen E. Jensen, CIS/MS-ISAC Thomas Sager, CIS Tiffany Bergeron, The MITRE Corp. Tony Sager, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode).

To further clarify the Creative Commons license related to the CIS Controls content, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (https://www.cisecurity.org/controls/) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS).

Contents

Executive Summary	1
Results Summary	2
Overview	
What's New in CDM v2.0	
Glossary	
Methodology	
Security Function vs. Security Value	8
ATT&CK Structure	8 10
Mapping Relationships	10
How to Use This Document	11
Security Function Analysis	
ATT&CK Mitigations	12
ATT&CK (Sub-)Techniques	14
CIS Safeguards	15
Data Source Analysis	
Data Types Attack Type Data Sources	18
Top Attack Types	19
Attack Pattern Data Sources	21
Security Value Analysis	22
Malware	22
Ransomware	23
Web Application Hacking	24
Targeted Intrusions	25
Summary	20
Conclusion	
Closing Notes	30
Euturo Work	

Appendix A Acronyms and Abbreviations. A1 **Appendix B** Links and Resources B1 Appendix C Background C1 **Appendix D** ATT&CK (Sub-)Techniques With No Mapping to CIS Safeguards. D1 Appendix E ATT&CK (Sub-)Techniques With No Mapping to ATT&CK Mitigations E1 **Appendix F** Unmapped CIS Safeguards to ATT&CK Framework F1 Appendix G **ATT&CK Navigator Visualizations** for Attack Patterns G1 Malware G1 G2 Ransomware Web Application Hacking G3 G4 Insider and Privilege Misuse **Targeted Intrusions** G5 **Appendix H** Unmapped ATT&CK (Sub-)Techniques to CIS Safeguards Within an Attack Pattern H1 Appendix I ATT&CK (Sub-)Techniques With No ATT&CK Mitigation Mapped Within an Attack Pattern 11

Executive Summary

This guide is the second edition of the Center for Internet Security[®] (CIS) Community Defense Model (CDM). The same security experts who help create the CIS Critical Security Controls[®] (CIS Controls[®]) work with CIS to apply the CDM to current threat data.

Enterprises that adopt the CIS Controls have repeatedly asked us to identify "What should we do first?" In response, the Controls Community sorted the Safeguards in the CIS Controls into three Implementation Groups (IGs) based on their difficulty and cost to implement.

Implementation Group 1 (IG1), the group that is least costly and difficult to implement, is what we call essential cyber hygiene (formerly basic cyber hygiene) and are the Safeguards we assert that every enterprise should deploy. For enterprises that face more sophisticated attacks or that must protect more critical data or systems, these Safeguards also provide the foundation for the other two Implementation Groups (IG2 and IG3).

Enterprises naturally want to know "How effective are the CIS Controls against the most prevalent types of attacks?" The CDM was created to help answer that and other questions about the value of the Controls based on currently available threat data from industry reports.

Our methodology is straightforward.

The MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK $^{\circ}$) framework allows us to express any attack type as a set of attack techniques, which we refer to as *attack patterns*. For each of the five most prevalent attack types, such as ransomware, we collect the corresponding attack patterns through analysis of industry threat data. We then track which Safeguards defend against each of the techniques found in those attack patterns. This methodology allows us to measure which Safeguards are most effective overall for defense across *attack types*.

Our results this year increased our confidence that our conclusions from the first CDM were correct. Based on additional industry threat data sources, the use of the updated version 8 of the CIS Controls and version 8.2 of the MITRE ATT&CK framework, we verified that the CIS Controls are effective at defending against 86% of the ATT&CK (sub-)techniques found in the ATT&CK framework. More importantly, the Controls are highly effective against the top five attack types found in industry threat data. The bottom line is that the CIS Controls, and specifically IG1, are a robust foundation for your cybersecurity program.

Our results also confirm that establishing and maintaining a secure configuration process (CIS Safeguard 4.1) is a linchpin Safeguard for all five attack types, which reinforces the importance of configurations, such as those found in the CIS Benchmarks[™].

Results Summary

Overall, the findings from this year's CDM both reaffirmed and strengthened, with objective data, what we already thought to be true—IG1 provides a viable defense against the top five attacks.

For CDM v2.0, the top five attack types are: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions. Our analysis found that, overall, implementing IG1 Safeguards defends against 77% of ATT&CK (sub-)techniques used across the top five attack types. That percentage goes up to 91% if all CIS Safeguards are implemented. These results strongly reinforce the value of a relatively small number of well-chosen and basic defensive steps (IG1) and also support IG1 as the preferred on-ramp to implementing the CIS Controls. We also found that CIS Safeguard 4.1 "Establish and Maintain a Secure Configuration Process" is most effective in defending against the top five attacks, reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

Additionally, independent of any specific attack type, implementing IG1 Safeguards defends against 74%¹ of ATT&CK (sub-)techniques in the MITRE ATT&CK framework, and implementation of all CIS Safeguards defends against 86% of ATT&CK (sub-)techniques in the framework. Since many ATT&CK (sub-)techniques are used across multiple attack types, we can extrapolate that the CIS Controls defend against more than the top five attacks mentioned in this guide.

We also analyzed each attack type individually. As an example, our analysis determined that implementing IG1 Safeguards defends against 78% of Ransomware ATT&CK (sub-) techniques, and implementing all CIS Safeguards defends against 92% of those techniques. This, and other attack pattern findings, can be seen in Figure 1 below. It is worth noting that 100% coverage of all attacker techniques for any attack type is difficult, as some techniques are not able to be defended against. Additionally, some IG1 Safeguards are foundational and process-oriented, such as enterprise and software asset management. While these foundational Safeguards may not be included in the ATT&CK model as defensive measures, they are necessary in order to successfully implement other Safeguards that map to ATT&CK.

		IG1 CIS Safeguards		All CIS Safeguards
Top 5 Attacks		IG1 can defend against XX% of ATT&CK (Sub-)Techniques		CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware		77%	-	94%
Ransomware	-	78%	-	92%
Web Application Hacking	-	86%	-	98%
Insider and Privilege Misuse	-	86%	-	90%
Targeted Intrusions	-	83%	-	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

1 All percentages based on ATT&CK (sub-)techniques that are assigned to an ATT&CK mitigation, and can therefore be defended.

Figure 1. CDM v2.0 attack pattern analysis

Overview

In this guide, we present the CDM v2.0. Our goal is to bring another level of rigor and detail to support the development and prioritization of the CIS Controls. The CDM process takes data sources (such as the Verizon Data Breach Investigations Report (DBIR)), drives them into models (such as the MITRE ATT&CK framework), and then translates them into action— creating our best practices (e.g., CIS Controls and CIS Benchmarks). The CDM is continuous, with each cycle starting the process again.



As a part of the CDM process, we use the MITRE Enterprise ATT&CK framework v8.2, the industry-accepted way to describe the individual technical details of a cyber-attack, which provides answers to questions, such as: "Which ATT&CK tactics (the objectives of an attacker) does an attacker use?"; "What are the ATT&CK (sub-)techniques (specific technical actions) used within those tactics?"; and "What are the general ATT&CK mitigations that could help defend against them?" Equally important in the CDM process is using industry threat data (i.e., data sources) of the most prevalent and relevant attacks plaguing enterprises. As part of the CDM process, we research authoritative, industry-recognized data sources, both national and international, which allow us to determine the top five attack types and create comprehensive attack patterns. Our work with the CIS Controls and ATT&CK framework, combined with using authoritative data sources to back our analysis, is the backbone of the CDM.

The CDM was constructed using the following process:

- We mapped CIS Safeguards to the ATT&CK framework.
- We identified the security function—independent of any specific attack, the ability of a CIS Safeguard to defend against one or more attacker techniques (e.g., ATT&CK (sub-) techniques).
- Using authoritative data sources, we identified the top five *attack types* that enterprises should defend against. For CDM v2.0, the top five attack types are: *Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse,* and *Targeted Intrusions*.

Figure 2. CDM Process

- For each attack type, we used authoritative data sources to determine the *attack pattern* the set of attacker techniques (e.g., ATT&CK (sub-)techniques) used in each attack type.
- We then identified the *security value*—the benefit of implementing a CIS Safeguard to defend against an individual attack or a group of attacks.

There are several ways that CDM analysis can be used to design, prioritize, implement, and improve an enterprise's security program. Our analysis affirms that enterprises should begin with implementing IG1 first (followed by IG2 and IG3, as appropriate) in order to, at a minimum, defend against the top five attacks. Our CDM v2.0 mappings also provide enterprises with more granularity, if needed. For example, if an enterprise implements CIS Safeguard "4.1–Establish and Maintain a Secure Configuration Process," our mappings can provide a list of ATT&CK (sub-)techniques that the Safeguard defends against. Attack Cards for each individual attack type, and all attack types combined, are also available on CIS WorkBench, to provide a listing of Safeguards that are the most effective in defending against specific ATT&CK (sub-)techniques.

CIS is dedicated to taking a "community-first" approach. Please join our CDM Community on CIS WorkBench to take advantage of these and other great resources, as well as to participate in next year's CDM (v3.0).

What's New in CDM v2.0

First, let's recap what we did in v1.0. Released in 2020, v1.0 made use of two publiclyavailable, authoritative industry resources: the MITRE ATT&CK framework and the Verizon DBIR. To establish the baseline model, a master mapping was created, starting with the 171 CIS Safeguards in CIS Controls v7.1. Following this, CIS Safeguards were mapped to the 41 ATT&CK mitigations in Enterprise ATT&CK v6.3, which MITRE already had mapped to the 266 ATT&CK techniques. This gave us the security function relationship between CIS Safeguards and ATT&CK techniques, identifying the ATT&CK techniques that could be defended against by implementing the CIS Safeguards.

We then selected the five most prevalent attack types (Malware, Ransomware, etc.) from the Verizon DBIR, and the ATT&CK techniques used within those attack types, forming what we call an attack pattern. Using the master mapping of the CIS Safeguards to ATT&CK, we then mapped each ATT&CK technique in the attack pattern back to the relevant CIS Safeguards. This allowed us to analyze the security value of the CIS Safeguards against these five attack types.

To build off of the foundational principles in v1.0, we made a few updates to v2.0, including the following:

- Updated Version of the CIS Controls. We used CIS Controls v8 as the basis for our mappings and analysis.
- Updated Version of the ATT&CK Framework. We used Enterprise ATT&CK v8.2, which
 is made up of 178 ATT&CK techniques, 352 ATT&CK sub-techniques (530 combined
 "ATT&CK (sub-)techniques"), and 42 ATT&CK mitigations. Note that the term "ATT&CK
 (sub-)techniques" is used throughout this guide to refer to ATT&CK techniques and
 ATT&CK sub-techniques as a whole, unless otherwise indicated.
- Additional Data Sources Added. We used several additional national and international data sources, such as the 2020 Verizon DBIR, ENISA Threat Landscape-The Year in Review, and more, to determine the top five attacks. Additional data sources were used in CDM v2.0 to create more comprehensive attack patterns. A full listing of data sources used to identify attack types and create attack patterns can be found here.²
- Updated Master Mapping. We mapped at the ATT&CK (sub-)technique level, in order to
 provide more granularity and clarity for our analysis. ATT&CK mitigations were used as
 a guide to map to the ATT&CK (sub-)techniques, which allowed us to select the specific
 ATT&CK (sub-)techniques that can be defended against through the implementation of
 one or more CIS Safeguards.

² Attack Types and Attack Patterns Attack Types and Attack Patterns

Glossary

The following are terms used throughout this guide and their specific meanings:

ATT&CK (sub-)technique	The combination of ATT&CK techniques and ATT&CK sub-techniques. Collectively referred to as ATT&CK (sub-) techniques, there are 530 in total for Enterprise ATT&CK v8.2.
ATT&CK mitigation	A list of defensive actions that can be taken to defend against an ATT&CK (sub-)technique.
ATT&CK sub-technique	The specific actions that an attacker takes to achieve an ATT&CK tactic, nested within ATT&CK techniques.
ATT&CK tactic	The objectives of an attacker such as reconnaissance, credential access, and exfiltration. A specific set of ATT&CK (sub-) techniques can be found within any given ATT&CK tactic.
ATT&CK technique	The specific actions that an attacker takes to achieve an ATT&CK tactic, listed under each ATT&CK tactic.
Attack pattern	The set of attacker techniques (e.g., ATT&CK (sub-)techniques) required to execute an attack. Attack patterns can change from year to year.
Attack type	The high-level grouping of attacks. For CDM v2.0, they are: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions.
Attacker techniques	A general term referring to actions that an attacker takes to compromise a system or network that's not assigned to a specific security framework.
CIS Critical Security Controls (CIS Controls)	A set of 18 best practice recommendations that help enterprises focus their resources on the most critical actions to defend against the most prevalent real-life attacks. Each CIS Control consists of a subset of Safeguards.
CIS Safeguards	A set of 153 specific recommendations that make up the CIS Controls. Organized into Implementation Groups, grouped as IG1, IG2, and IG3 Safeguards.
Data source	A threat report, or other dataset, that provides an analysis of attacks, attacker tactics, techniques, and procedures (TTPs), or other specific information related to cybersecurity. Also referred to as industry threat data sources. Used to determine attack types and attack patterns.
Data type	Can be one of multiple categorizations of data that are incorporated into a data source (e.g., self-reported data, sensor data, incident response data, product usage data, and open-source intelligence).
Implementation Group 1 (IG1)	Implementation Group 1, also known as essential cyber hygiene (formerly basic cyber hygiene). IG1 includes defensive actions that are applicable to even the smallest and least-funded enterprises.
Implementation Groups	A simple and accessible way to help enterprises prioritize the implementation of the CIS Controls.
Security function	Independent of a specific attack type, the ability of a CIS Safeguard to defend against one or more attacker techniques (e.g., ATT&CK (sub-)techniques).
Security value	The benefit a CIS Safeguard provides in defending against an individual attack type or a group of attack types.

Methodology

Implementation Groups and the CDM

In CIS Controls v7.1, we introduced a new prioritization scheme referred to as Implementation Groups (IGs). There are three IGs: IG1, IG2, and IG3. To develop the IGs, CIS identified a core set of CIS Safeguards that enterprises with limited resources, expertise, and risk exposure should focus on. This is IG1, or essential cyber hygiene. IG1 includes defensive actions that are applicable to even the smallest and least-funded enterprises. Each IG builds upon the previous one. IG2 identifies additional CIS Safeguards for enterprises with more resources and expertise than those in IG1, and also greater risk exposure. IG3, for enterprises that have the highest level of risk exposure, includes all 153 CIS Safeguards.

The CDM tells us that IG1 defends against the top five attacks. Specifically, the CDM can also help an enterprise focus on which technical IG1 Safeguards are most effective in defending against specific attacks. We at CIS feel that this is a powerful approach to an enterprise's risk management strategy. Additionally, some IG1 Safeguards are foundational and process-oriented, such as enterprise and software asset management. These foundational Safeguards may not be included in the ATT&CK model as defensive measures; however, they must be implemented before the more technical Safeguards that do map to ATT&CK can be properly implemented.



The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into. 153 TOTAL SAFEGUARDS

 IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.
 23

 IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.
 74

 IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.
 566

Figure 3. CIS Controls Implementation Group overview

Security Function vs. Security Value	Throughout the CDM v2.0, we focus on two main concepts: the <i>security function</i> and the <i>security value</i> of the CIS Safeguards. The security function can best be defined as the ability of a CIS Safeguard to defend against one or more ATT&CK (sub-)techniques, independent of any specific attack type. The security function does not necessarily answer the question of why we should implement a particular CIS Safeguard, or the benefit in doing so. Rather, the security function provides the foundation that allows us to analyze the security value, defined as the benefit a CIS Safeguard provides in defending against one or more attack types.		
Overall Process	The CDM is comprised of a series of seven steps to get us to the end result. They are:		
	1 Create master mapping. We created a master mapping from CIS Controls v8 to Enterprise ATT&CK v8.2, mapping the CIS Safeguards to the ATT&CK (sub-)techniques. ATT&CK mitigations were used as a guide to map at the ATT&CK (sub-)technique level.		
	2 Analyze security function. We analyzed the security function of the CIS Safeguards against ATT&CK (sub-)techniques using the master mapping in Step 1.		
	3 Identify top five attack types. Using multiple data sources, we identified the five most prevalent attack types experienced by enterprises in 2020-2021: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions.		
	4 Construct attack patterns. For each attack type, we used multiple data sources to create comprehensive attack patterns—the set of attacker techniques (e.g., ATT&CK (sub-) techniques) used in an attack type.		
	5 Perform reverse mapping. We used the master mapping of the CIS Controls to ATT&CK (in Step 1) to map each ATT&CK (sub-)technique associated with an attack type back to the CIS Safeguards.		
	6 Analyze security value. The reverse mapping allowed us to analyze the security value of implementing the CIS Safeguards against one or more attack types, meaning, how well do the CIS Controls defend against the top five attacks.		
	7 Create visualizations. The MITRE ATT&CK Navigator allows users to create interactive "layers" of ATT&CK. This tooling allowed us to visualize each attack pattern individually and combined across all attack types. These layers can be found on CIS WorkBench here.		
	The detailed CDM process can be seen in Figure 4.		



ATT&CK Structure

In order to fully understand the CDM methodology, it is fundamental to understand how the ATT&CK framework is organized and interconnects. The highest level within ATT&CK is called a tactic. These are, as previously mentioned, the objectives of an attacker, such as reconnaissance, credential access, and exfiltration. There are 14 tactics in ATT&CK v8.2, represented with a "TA" before their unique identifier. Each ATT&CK tactic contains multiple ATT&CK *techniques*, which contain ATT&CK *sub-techniques*, where applicable. ATT&CK (sub-)techniques are the specific actions that an attacker takes to achieve an ATT&CK tactic. They are represented with a "T" before their unique identifier, with ATT&CK sub-techniques having ".0XX" after the main unique identifier. There are 530 ATT&CK (sub-)techniques in total for v8.2.

ATT&CK also has *mitigations*, each including several ATT&CK (sub-)techniques. ATT&CK mitigations provide a list of actions that can be taken to defend against a specific ATT&CK (sub-)technique. The ATT&CK mitigations begin with the letter "M" followed by a unique identifier (e.g., M1047). There are 42 ATT&CK mitigations in v8.2. It is worth noting that ATT&CK techniques and their child sub-technique(s) do not always map back to the same ATT&CK mitigation. For example, "M1036–Account Use Policies" mitigates against "T1110–Brute Force," which has four ATT&CK sub-techniques. However, the mitigation M1036 is effective against only three of the four (sub-)techniques (T1110.001, T1110.003, and T1110.004), as indicated on the ATT&CK website. This warranted us to map at the ATT&CK (sub-) technique level for the CDM master mapping for accuracy.

It is important to note that out of the 530 ATT&CK (sub-)techniques in v8.2, 84 have no assignment to an ATT&CK mitigation, meaning that no matter what security framework is being implemented, these 84 ATT&CK (sub-)techniques cannot be easily mitigated, based on information provided on the ATT&CK website. An example of one of these ATT&CK (sub-)techniques is "T1546-Event Triggered Execution," which "cannot be easily mitigated with preventive controls since it is based on the abuse of system features," according to the ATT&CK website. Our assessment of these ATT&CK (sub-)techniques found that the majority are used in what is often referred to as "Living off the Land (LotL)" attacks, where attackers use existing tools and tactics on the targeted system or network to carry out an attack, rather than exploit a specific system or control weakness; these attacks are therefore difficult to defend against. Unless otherwise noted, all calculations in this guide do not take into account these ATT&CK (sub-)techniques. Additional information on ATT&CK v8.2 can be found on the ATT&CK website.

Mapping Relationships

As part of Step 1 of the CDM process, the CIS Safeguards are mapped to ATT&CK mitigations and then to ATT&CK (sub-)techniques. Ultimately, this high-level mapping (from CIS Safeguards to ATT&CK mitigations) serves as the guide for connecting CIS Safeguards to ATT&CK (sub-)techniques, and therefore it is worthwhile to analyze both: how well the CIS Safeguards map to ATT&CK mitigations and then to ATT&CK (sub-)techniques. The CIS Safeguard mapping to ATT&CK is available separately from this guide on CIS WorkBench and via the CIS website. Figure 5 below demonstrates the mapping relationship. It should be noted that the mapping creates a many-to-many relationship between CIS Safeguards and ATT&CK (sub-)techniques, meaning that implementing a single CIS Safeguard defends against multiple ATT&CK (sub-)techniques, and a single ATT&CK (sub-)technique can be defended through implementation of one or more CIS Safeguards.

Each CIS Safeguard can defend against one or more ATT&CK (Sub-)Techniques



Each ATT&CK (Sub-)Technique can be defended by one or more CIS Safeguards

It is worth noting that the ATT&CK mitigations represent defensive cybersecurity actions at a different level of abstraction than the CIS Safeguards. The CIS Safeguards cover a larger number of defensive cybersecurity concepts than the ATT&CK mitigations. This difference in granularity is perhaps best demonstrated through the number of defensive actions within each collection: CIS Controls v8 contains 153 CIS Safeguards, whereas ATT&CK v8.2 contains 42 ATT&CK mitigations.

How to Use This Document	For those looking to understand more about the CDM process, this guide is a perfect start to give readers:
	An overview of how the CDM works
	 An explanation for why the CDM is helpful to build an enterprise's cybersecurity program A high-level overview of results from this year's CDM
	 An in-depth analysis of ATT&CK (sub-)techniques that can be defended against through implementation of the CIS Safeguards, overall and for each attack type
	Additional links and resources
	For those who wish to dive deeper into the CDM, we also provide the following:
	 CDM Master Mapping: A Microsoft[®] Excel[®] spreadsheet containing³: CIS Controls v8 to ATT&CK mapping: High-Level (to ATT&CK mitigations) CIS Controls v8 to ATT&CK mapping: Low-Level (to ATT&CK (sub-)techniques)
	 ATT&CK Visualizations: JavaScript Object Notation (JSON) files for each attack type, as well as one for all attack types combined⁴ A guide on how to visualize these JSON files
	• CDM Attack Cards: IG1 Safeguards to implement for each attack type and all attack types combined (in terms of effectiveness) ⁵
	 CDM Reverse Mapping: A reverse mapping that provides which ATT&CK (sub-)techniques can be defended by implementing one or more CIS Safeguards, as well as which attack type(s) they defend against⁶.
	Please join our CDM Community on CIS WorkBench to take advantage of these and other great resources.

³ Found here: Note that a CIS WorkBench account is needed to obtain these files (free). Microsoft* Excel* workbooks are in database-friendly formats.

⁴ Found here: Note that a CIS WorkBench account is needed to obtain these files (free). JSON files can be imported into MITRE's ATT&CK Navigator tool here

 $^{{\}rm 5} \quad {\rm Found \ here: Note \ that \ a \ CIS \ WorkBench \ account \ is \ needed \ to \ obtain \ this \ file \ (free).}$

⁶ Found here: Note that a CIS WorkBench account is needed to obtain this file (free).

Security Function Analysis

ATT&CK Mitigations

The first step in determining the security function of the CIS Safeguards is to map the CIS Safeguards to the ATT&CK mitigations. Note that a single Safeguard can map to multiple ATT&CK mitigations and vice versa.

All CIS Safeguards

Overall, the CIS Safeguards mapped to 93% of ATT&CK mitigations, or 39 out of 42. Table 1 below shows the top 10 ATT&CK mitigations that mapped to CIS Safeguards. For example, "M1047–Audit" is mapped to 23 CIS Safeguards, indicating that those 23 Safeguards perform some form of auditing activity, and therefore have the ability to defend against one or more ATT&CK (sub-)techniques that are contained within the Audit mitigation. Analysis found that "M1047–Audit" ranked #1 again this year with the most mappings, emphasizing the importance of implementing best practices, such as secure configurations (e.g., CIS Benchmarks), and auditing those configurations.

 Table 1. Number of CIS Safeguards

 mapped to the top 10 ATT&CK

 mitigations

RANK	ATT&CK Mitigation ID	ATT&CK Mitigation Name	NUMBER OF ATT&CK Mitigations mapped to CIS safeguards
1	M1047	Audit	23
2	M1051	Update Software	19
3	M1016	Vulnerability Scanning	17
4	M1018	User Account Management	16
5	M1026	Privileged Account Management	15
6	M1042	Disable or Remove Feature or Program	14
7	M1029	Remote Data Storage	14
8	M1035	Limit Access to Resource Over Network	13
9	M1037	Filter Network Traffic	12
10	M1030	Network Segmentation	10

IG1 CIS Safeguards

In analyzing IG1 Safeguards, it was found that they mapped to 83% of ATT&CK mitigations. Additionally, eight of the ATT&CK mitigations shown in Table 1 above remained in the top 10 for IG1. However, others, such as "M1053-Data Backup," M1017-User Training," and "M1022-Restrict File and Directory Permissions," moved up in rank (since IG1 only focuses on a subset of the CIS Safeguards), as shown below in Table 2.

RANK	ATT&CK Mitigation ID	ATT&CK Mitigation Name	NUMBER OF ATT&CK Mitigations Mapped To CIS Safeguards
1	M1047	Audit	12
2	M1018	User Account Management	11
3	M1029	Remote Data Storage	9
4	M1026	Privileged Account Management	9
5	M1017	User Training	6
6	M1051	Update Software	6
7	M1035	Limit Access to Resource Over Network	6
8	M1030	Network Segmentation	5
9	M1022	Restrict File and Directory Permissions	5
10	M1053	Data Backup	4

Unmapped

Although the majority of ATT&CK mitigations had at least one mapping to a CIS Safeguard, a few mitigations were left unmapped, as shown below in Table 3. For v2.0, we are excited to include an ATT&CK mitigation that was not mapped in v1.0, "M1040–Behavior Prevention on Endpoint." Prior to CIS Controls v8, Safeguards relating to Endpoint Detection and Response (EDR) had not been included. However, we recognized the importance of including Safeguards surrounding EDR in an effort to keep up with the ever-changing threat landscape.

With the addition of CIS Safeguards such as, "13.2–Deploy a Host-Based Intrusion Detection Solution" and "13.7–Deploy a Host-Based Intrusion Prevention Solution," we were able to successfully map to the ATT&CK mitigation, "M1040–Behavior Prevention on Endpoint." We also recognized the addition of an ATT&CK mitigation that was not on this list in v1.0, "M1020–SSL/TLS Inspection." This was due to the retirement of CIS Safeguard (v7.1) 12.10, "Decrypt Network Traffic at Proxy" in v8 of the CIS Controls. While important, we felt that decryption of network traffic may not be appropriate, feasible, or attainable for some enterprises. Additionally, in some cases, privacy requirements/regulations may contradict or interfere with guidance to decrypt all network traffic.

ATT&CK Mitigation ID	ATT&CK MITIGATION NAME	ATT&CK MITIGATION DESCRIPTION
M1019	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.
M1020	SSL/TLS Inspection	Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.
M1055	Do Not Mitigate	This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.

Table 2. Number of IG1 CISSafeguards mapped to the top 10ATT&CK mitigations

Table 3. ATT&CK mitigations withno mapping to CIS Safeguards

ATT&CK (Sub-)Techniques All CIS Safeguards

In addition to analyzing at the ATT&CK mitigation level, we also analyzed the mappings at an ATT&CK (sub-)technique level, providing us with a more granular and clarified dataset for analysis. Shown below in Table 4 is a listing of ATT&CK (sub-)techniques that had the highest number of CIS Safeguard mappings. At first glance, it may appear that in order to defend against a specific ATT&CK (sub-)technique, it would require the implementation of a significant number of CIS Safeguards. However, this is not the case. Since multiple CIS Safeguards can defend against the same ATT&CK (sub-)technique, this provides enterprises with multiple options to select the Safeguards that are most appropriate to implement for their environment. Multiple Safeguards mapping to an ATT&CK (sub-)technique also helps to illustrate defense-in-depth.

Overall, out of 446 ATT&CK (sub-)techniques assigned to an ATT&CK mitigation, 383, or 86%, can be defended against through implementation of all CIS Safeguards. Additional analysis found that almost half of the ATT&CK (sub-)techniques, shown in Table 4 below, related to the exploitation of an external application, protocol, etc., emphasizing the importance of securing externally-facing systems. It also is worth noting that ATT&CK sub-technique "T1021.001–Remote Desktop Protocol (RDP)" had the highest number of CIS Safeguards mapped to it, demonstrating the potential that the CIS Safeguards can provide in protecting RDP. Recently, CIS released a guide about RDP, a protocol attackers often exploit, and which direct mitigations can be implemented to defend against an RDP-based attack.

RANK	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	NUMBER OF CIS SAFEGUARDS Mapped to an Att&CK (SUB-)technique
1	T1021.001	Remote Desktop Protocol	42
2	T1563.002	RDP Hijacking	41
3	T1552	Unsecured Credentials	39
4	T1072	Software Deployment Tools	38
5	T1210	Exploitation of Remote Services	35
6	T1190	Exploit Public-Facing Application	33
7	T1059	Command and Scripting Interpreter	30
8	T1557	Man-in-the-Middle	29
9	T1530	Data from Cloud Storage Object	28
10	T1574	Hijack Execution Flow	27
11	T1003	OS Credential Dumping	25
12	T1133	External Remote Services	24
13	T1543.002	Systemd Service	24
14	T1563	Remote Service Session Hijacking	24
15	T1059.001	PowerShell	24
16	T1021.005	VNC	23
17	T1542.005	TFTP Boot	23
18	T1548	Abuse Elevation Control Mechanism	22
19	T1602.001	SNMP (MIB Dump)	22
20	T1543	Create or Modify System Process	22

IG1 CIS Safeguards

Overall, out of the ATT&CK (sub-)techniques assigned to an ATT&CK mitigation (446), IG1 Safeguards defend against 74% (332). This shows that by implementing IG1 alone, enterprises can defend against the majority of ATT&CK (sub-)techniques. Additionally, it is worth noting that some IG1 Safeguards are foundational and process-oriented, such as enterprise and software asset management. These foundational Safeguards may not be included in the

"T1021.001-Remote Desktop Protocol (RDP)" had the highest number of CIS Safeguards mapped to it, emphasizing the potential that the CIS Safeguards can provide in protecting RDP. Get the CIS RDP guide here.

 Table 4. ATT&CK (sub-)techniques

 that had the highest number of CIS

 Safeguard mappings

ATT&CK model as defensive measures, due to the technical nature of the ATT&CK framework; however, many are pre-requisites to successfully implement the more technical Safeguards that do map to ATT&CK.

 Table 5. ATT&CK (sub-)techniques

 that had the highest number of IG1

 Safeguard mappings

RANK	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	NUMBER OF CIS SAFEGUARDS Mapped to an Att&Ck (Sub-)technique
1	T1552	Unsecured Credentials	22
2	T1021.001	Remote Desktop Protocol	21
3	T1543.002	Systemd Service	20
4	T1563.002	RDP Hijacking	20
5	T1072	Software Deployment Tools	20
6	T1530	Data from Cloud Storage Object	19
7	T1530.006	Systemd Timers	18
8	T1574	Hijack Execution Flow	16
9	T1078.004	Cloud Accounts	16
10	T1543	Create or Modify System Process	16
11	T1601.002	Patch System Image	15
12	T1548	Forge Web Credentials	15
13	T1601	Downgrade System Image	15
14	T1569	Abuse Elevation Control Mechanism	15
15	T1098	Modify System Image	15
16	T1003	System Services	15
17	T1053.002	Account Manipulation	14
18	T1599	OS Credential Dumping	14
19	T1021.002	At (Windows)	14
20	T1599.001	Domain Policy Modification	14

Unmapped

While the majority of the ATT&CK (sub-)techniques can be defended against by one or more CIS Safeguards, 63 ATT&CK (sub-)techniques did not map back to a CIS Safeguard. Many of these ATT&CK (sub-)techniques are listed under ATT&CK mitigations that did not map to a CIS Safeguard, such as "M1055–Do Not Mitigate," "M1020–SSL/TLS Inspection," and "M1019–Threat Intelligence Program." Several ATT&CK (sub-)techniques from "M1056–Pre-compromise" were also among those that were unmapped. A listing of these ATT&CK (sub-) techniques can be found in Appendix D of this guide.

Additionally, the 84 ATT&CK (sub-)techniques with no assignment to an ATT&CK mitigation can be found in Appendix E of this guide. Our assessment of these ATT&CK (sub-)techniques found that the majority are used in LotL attacks, where an attacker uses existing tools and tactics on the targeted system or network to carry out an attack, rather than exploit a specific system or control weakness; these attacks are therefore difficult to defend against.

CIS Safeguards

All CIS Safeguards

In addition to the analysis above, we also analyzed the reverse—which CIS Safeguards defend against one or more ATT&CK (sub-)techniques. Our mapping revealed that out of 153 CIS Safeguards, 68% defend against one or more ATT&CK (sub-)techniques, with 19 CIS Safeguards defending against 50 or more ATT&CK (sub-)techniques, as shown below in Table 6.

We can see that CIS Safeguard "4.1–Establish and Maintain a Secure Configuration Process" defends against the highest number of ATT&CK (sub-)techniques, once again reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

Table 6. CIS Safeguards that hadthe highest number of mappedATT&CK (sub-)techniques

RANK	CIS SAFEGUARD	CIS SAFEGUARD TITLE	NUMBER OF ATT&CK (SUB-) Techniques defended By A CIS safeguard	IG1	IG2	IG3
1	4.1	Establish and Maintain a Secure Configuration Process	342	\checkmark	\checkmark	\checkmark
2	6.1	Establish an Access Granting Process	217	\checkmark	\checkmark	\checkmark
3	6.2	Establish an Access Revoking Process	217	\checkmark	\checkmark	\checkmark
4	18.3	Remediate Penetration Test Findings	214		\checkmark	\checkmark
5	6.8	Define and Maintain Role-Based Access Control	206			\checkmark
6	4.7	Manage Default Accounts on Enterprise Assets and Software	188	\checkmark	<	<
7	18.5	Perform Periodic Internal Penetration Tests	187			\checkmark
8	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	164	\checkmark	<	<
9	5.3	Disable Dormant Accounts	155	\checkmark	\checkmark	\checkmark
10	2.5	Allowlist Authorized Software	101		\checkmark	\checkmark
11	2.7	Allowlist Authorized Scripts	81			\checkmark
12	3.3	Configure Data Access Control Lists	75	\checkmark	\checkmark	\checkmark
13	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	73	√	<	<
14	2.3	Address Unauthorized Software	67	\checkmark	\checkmark	\checkmark
15	4.4	Implement and Manage a Firewall on Servers	60	\checkmark	\checkmark	\checkmark
16	4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	54		<	<
17	13.8	Deploy a Network Intrusion Prevention Solution	53			\checkmark
18	13.3	Deploy a Network Intrusion Detection Solution	53		\checkmark	\checkmark
19	12.2	Establish and Maintain a Secure Network Architecture	51		\checkmark	\checkmark
20	5.2	Use Unique Passwords	47	\checkmark	\checkmark	\checkmark

IG1 CIS Safeguards

Overall, it was found that 86% of IG1 Safeguards defend against one or more ATT&CK (sub-)techniques, with many defending against 60 or more, as shown below in Table 7. This reinforces that implementing a relatively small set of defensive actions (IG1) provides an enterprise with the ability to defend against a wide array of potential attacks.

As previously mentioned, some of the IG1 Safeguards do not directly map to the ATT&CK framework. These are considered foundational Safeguards, such as keeping inventory of enterprise assets and software (CIS Controls 1 and 2) and implementing logging (CIS Control 8). These foundational Safeguards are important, since without them, there is no way of knowing which devices are, or could be, compromised. These foundational Safeguards may not be included in the ATT&CK model as defensive measures; however, they must be implemented before more technical Safeguards that do map to ATT&CK can be properly implemented.

RANK	CIS SAFEGUARD	TITLE	NUMBER OF ATT&CK (SUB-) Techniques defended By A CIS safeguard
1	4.1	Establish and Maintain a Secure Configuration Process	342
2	6.1	Establish an Access Granting Process	217
3	6.2	Establish an Access Revoking Process	217
4	4.7	Manage Default Accounts on Enterprise Assets and Software	188
5	5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	164
6	5.3	Disable Dormant Accounts	155
7	3.3	Configure Data Access Control Lists	75
8	4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	73

Table 7. IG1 Safeguards that hadthe highest number of mappedATT&CK (sub-)techniques

9	2.3	Address Unauthorized Software	67
10	4.4	Implement and Manage a Firewall on Servers	60
11	5.2	Use Unique Passwords	47
12	6.5	Require MFA for Administrative Access	33
13	6.4	Require MFA for Remote Network Access	31
14	7.1	Establish and Maintain a Vulnerability Management Process	27
15	7.2	Establish and Maintain a Remediation Process	27
16	11.3	Protect Recovery Data	27
17	14.1	Establish and Maintain a Security Awareness Program	25
18	7.3	Perform Automated Operating System Patch Management	24
19	11.4	Establish and Maintain an Isolated Instance of Recovery Data	20
20	6.3	Require MFA for Externally-Exposed Applications	17

Unmapped

In total, 49 CIS Safeguards were not mapped to ATT&CK, only eight of which were IG1 Safeguards. As previously mentioned, some of these unmapped Safeguards are foundational Safeguards, such as "CIS Control 8: Audit Log Management" and "CIS Control 3: Data Protection." Other Safeguards, such as those in "CIS Control 15: Service Provider Management" and "CIS Control 17: Incident Response Management," as examples, are also not specifically addressed by any of the ATT&CK mitigations in the ATT&CK framework, and therefore are unable to be mapped.

A list of unmapped CIS Safeguards can be found in Appendix F of this guide.

Data Source Analysis

After determining the security function of the CIS Safeguards, based on their mapping to ATT&CK, we then determined the top five attack types and attack patterns. First, we selected the most common attack types that enterprises should defend against, through reviewing various data sources. Attack types are the high-level grouping of attacks. For v2.0, they are: Malware, Ransomware, Web Application Hacking, Insider and Privilege Misuse, and Targeted Intrusions.

Following this, we used additional data sources to determine the attack pattern—the set of ATT&CK (sub-)techniques required to execute the attack. Attack patterns are constructed with the most recent attacker techniques and can change from year to year. Lastly, we leveraged the master mapping to ATT&CK, to perform a reverse mapping back to the CIS Safeguards, which allowed us to analyze the security value of the Safeguards.

Data Types

Each year, multiple data sources (i.e., industry threat data sources) are published that contain various metrics, such as top malware, top ransomware, top attack types, etc. The data behind these reports contains valuable information and can be categorized into one of the following data types, all of which the CDM leverages:

- Self-Reported Data: Analysts and researchers are employed to contact companies and obtain first-hand information about how breaches occurred.
- Sensor Data: Vendors offering network and other types of cybersecurity monitoring or prevention services have access to raw network and other types of data.
- Incident Response Data: Created from incident response activities, the data obtained here
 is often rich and extremely granular; however, it may be unstructured and is provided in
 narrative form.
- Product Usage Data: Vendors offering software-as-a-service and cloud-based products may gather security-relevant data for customers using their products.

If you're a vendor with data that fits into one or more categories, please contact us at controlsinfo@ cisecurity.org.

publicly-available incident response reports, and other security-related publications.

Open-Source Intelligence: Information available from sources such as intelligence reports,

In addition to data type, the longevity of the report and access to underlying datasets are also taken into consideration.

Attack Type Data Sources

Table 8. Attack type data sources

We evaluated multiple data sources to determine the top five attack types, as shown below in Table 8.

DATA SOURCE	PUBLISH DATE	ТҮРЕ	LONGEVITY	CIS ACCESS TO Underlying data
Verizon DBIR	May 19, 2020	Self-reported data, Sensor data, Incident response data	2008	No ⁷
IBM X-Force Threat Intelligence Index	February 24, 2021	Sensor data, Incident response data	2017	No
ENISA Threat Landscape – The Year in Review	October 20, 2020	Open-source intelligence	2012	No
CrowdStrike Services Cyber Front Lines Report	2020	Sensor data, Incident response data, Product usage data	2020	No
Akamai The State of the Internet: A Year in Review	2020	Sensor data, Product usage data	2008	No

Several sources were reviewed and some carried a heavier weight, such as the 2020 Verizon DBIR, since their dataset encompasses several different data sources, both public and private, and is based on multiple data types. As data sources may change from time to time, we are confident that our analysis and the data that backs it provides enterprises with the knowledge they need to put forth a robust security program and protect against the most pervasive cyber threats.

Top Attack Types

The top attack types for v2.0 are shown below in Table 9, in order of prevalence. The attack types remain unchanged from v1.0; however, the rank has changed, based on the cumulative analysis of the various data sources listed above in Table 8.

With these attack types, there is likely to be some overlap (e.g., a nation-state attacker that is working as an insider, a targeted intrusion attack that uses malware). However, every effort is made to group these top attack types into categories that have valuable data sources to determine their respective attack patterns. Therefore, some top attack types, such as general, non-specific categories (e.g., everything else, other, etc.) or a category that cannot be easily mitigated (e.g., Denial of Service (DoS), stolen assets, etc.), were not considered.

Table 9. Top 5 attack types forCDM v2.0

RANK	ATTACK TYPE	CHANGE FROM CDM V1.0
1	Malware	Moved up in rank
2	Ransomware	Moved up in rank
3	Web Application Hacking	Moved down in rank
4	Insider and Privilege Misuse	Moved down in rank
5	Targeted Intrusions	Rank remained the same

The following sections briefly describe each attack type and the justification for inclusion.

7 However, the Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database (VCDB) is a random sample of only public breaches and is available at: https://github.com/vz-risk/VCDB. This data is a part of the larger DBIR dataset.

Malware

Malware continues to plague enterprises year after year. The Verizon DBIR describes malware as "...the common type of commodity malware that everyone has probably seen on some email claiming to be a fax or a missed delivery package. These incidents and breaches tend to be opportunistic and financially motivated." (Verizon DBIR, 2020).⁸ The DBIR refers to this attack type as "crimeware," which includes malware that did not fall into another attack type. According to the 2020 DBIR, malware ranked #4 in breaches and #2 in incidents (Verizon DBIR, 2020). Malware continues to affect enterprises globally, as malware ranked #1 in ENISA's The Year in Review 2020 report (ENISA, 2020)⁹. Each month, the Multi-State Information Sharing and Analysis Center[®] (MS-ISAC[®]) publishes the Top 10 Malware impacting SLTTs, a data source also used in the CDM.

Ransomware

Ransomware involves the encryption of files on a system or network, rendering them useless until a decryption key is used or backups are restored. Ransomware has taken its toll across all sectors over the years, and the threat continues to grow into 2021. According to the 2020 DBIR, 27% of malware incidents were categorized as ransomware (Verizon DBIR, 2020). Due to the differences in attacker tactics, techniques, and procedures (TTPs) and motives, we separated Ransomware from the Malware attack type. According to IBM^{er}s 2021 X-Force Threat Intelligence Index report, ransomware ranked as their number one threat type, totaling 23% of their X-Force[®] caseload (IBM X-Force, 2021)¹⁰. Additionally, X-Force estimated a staggering profit of \$123 million from just one of the ransomware groups, Sodinokibi (aka REvil) (IBM X-Force, 2021). According to Bitdefender[®]'s 2020 Mid-Year Threat Landscape Report, there was a 715.08% increase of ransomware reports across the globe (Bitdefender, 2020)¹¹. These findings stress the importance of protecting against ransomware attacks, as no one sector is immune.

Web Application Hacking

The DBIR defines this as "anything that has a web application as the target." Over 80% of breaches involved some type of web application hacking, according to the 2020 Verizon DBIR. Additionally, web applications were ranked #1 for breaches and #4 for incidents (Verizon DBIR, 2020). When it comes to the cloud, the report also states that 73% of the time, cloud-based breaches attacked an email or web application server, stressing the importance of protecting both on-premises and cloud assets (Verizon DBIR, 2020). It should come as no surprise that externally-facing applications are much more vulnerable to an attack, especially for those with misconfigurations and protocols that are left open and unprotected. At the top of the list for web application attacks are "Injections" (e.g., SQL, NoSQL, etc.) and "Cross-site Scripting (XSS)," according to the OWASP® Top 10¹² and 2020 CWE Top 25¹³, respectively.

Insider and Privilege Misuse

Insider and Privilege Misuse can be defined as incidents that are intentionally carried out by an insider, according to the 2020 Verizon DBIR. These are incidents where the insider has malicious intent to cause harm. According to the 2021 IBM X-Force Threat Intelligence Report, *"25% of attacks against transportation in 2020 involved a malicious insider or misconfiguration."* Additionally, out of the 13% of insider threat incidents in the industrial control systems (ICS) and operational technology (OT) fields, 60% involved insiders with malicious intent (IBM X-Force, 2021).

- 8 2020 Verizon Data Breach Investigations Report (DBIR) https://enterprise.verizon.com/resources/reports/dbir/2020/introduction/
- 9 ENISA Threat Landscape-The Year in Review (Published October 20, 2020) https://www.enisa.europa.eu/publications/year-in-review
- 10 IBM X-Force Threat Intelligence Index 2021 https://www.ibm.com/security/data-breach/threat-intelligence
- 11 Bitdefender Mid-Year Threat Landscape Report 2020 https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf
- 12 OWASP Top 10 https://owasp.org/www-project-top-ten/
- 13 2020 CWE Top 25 https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

According to Bitdefender's 2020 Mid-Year Threat Landscape Report, there was a 715.08% increase in ransomware reports across the globe.

Malware ranked #1 in

2020 report.

ENISA's The Year in Review

Targeted Intrusions

This attack type includes nation-state activity or state-affiliated actors that are looking for the crown jewels, such as an enterprise's data (Verizon DBIR, 2020). Additionally, the intent of Targeted Intrusions differs from other patterns, focusing on social, economic, and political gain. The 2020 DBIR states that these types of attacks typically focus on the social and malware vectors of the VERIS framework, with 81% using phishing and 92% using malware (Verizon DBIR, 2020).

Attack Pattern Data Sources

attack type)

Table 10. Data sources used to create attack patterns (for each

Once the top attack types were determined, data sources were selected in a similar fashion to create comprehensive attack patterns. Attack patterns are the selection of ATT&CK (sub-) techniques that are used in a given attack type. We focus on the most common and recently used techniques to form the attack patterns, as patterns can and will change from year to year. Several data sources were used to create the attack patterns, which can be seen in Table 10 below.

ATTACK TYPE	ATTACK PATTERN DATA SOURCE
Malware	 Multi-State Information Sharing and Analysis Center[®] (MS-ISAC[®]) Top 10 Malware CrowdStrike 2021 Global Threat Report¹⁴ IBM X-Force Threat Intelligence Index 2021 ESET Threat Report Q4 2020¹⁵ Check Point 2021 Cyber Security Report¹⁶
Ransomware (as a subset of Malware)	 Multi-State Information Sharing and Analysis Center (MS-ISAC) Data CrowdStrike 2021 Global Threat Report IBM X-Force Threat Intelligence Index 2021 Group-IB Ransomware Uncovered 2020-2021¹⁷ ESET Threat Report Q4 2020
Web Application Hacking	 OWASP Top 10 2020 CWE Top 25
Insider and Privilege Misuse	 Verizon Insider Threat Report 2019¹⁸ Securonix 2020 Insider Threat Report¹⁹ G-Research Introducing the Insider Attack Matrix²⁰
Targeted Intrusions	 CrowdStrike 2021 Global Threat Report CISA SolarWinds and Active Directory/M365 Compromise Threat Report²¹

14 CrowdStrike 2021 Global Threat Report https://www.crowdstrike.com/resources/reports/global-threat-report/

- 15 ESET Threat Report Q4 2020 https://www.welivesecurity.com/wp-content/uploads/2021/02/ESET_Threat_Report_Q42020.pdf
- 16 Check Point 2021 Cyber Security Report https://www.checkpoint.com/pages/cyber-security-report-2021/

¹⁷ Group-IB Ransomware Uncovered 2020-2021 https://www.group-ib.com/resources/threat-research/ransomware-2021.html

¹⁸ Verizon Insider Threat Report 2019 https://enterprise.verizon.com/resources/reports/insider-threat-report/

¹⁹ Securonix 2020 Insider Threat Report https://www.securonix.com/resources/2020-insider-threat-report/

²⁰ G-Research Introducing the Insider Attack Matrix https://www.gresearch.co.uk/article/introducing-the-insider-attack-matrix/

²¹ CISA SolarWinds and Active Directory/M365 Compromise Threat Report: https://us-cert.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf

Security Value Analysis

There are several different ways to analyze the security value of the CIS Safeguards against the top five attack types. The next few sections provide an analysis of how well each attack pattern²² is covered by the CIS Safeguards, against ATT&CK tactics and ATT&CK (sub-) techniques. Note that for the ATT&CK tactic analysis, multiple ATT&CK (sub-)techniques can appear across multiple ATT&CK tactics.

Malware

Figure 6. Malware attack pattern coverage against CIS

Safeguards (by IG) across ATT&CK tactics

Shown below in Figure 6 is the Malware attack pattern analysis, by IG, across all ATT&CK tactics. Overall, nine of the 14 ATT&CK tactics had 75% or more coverage. Table 11 shows the percentage of Malware ATT&CK (sub-)techniques, within each ATT&CK tactic, that CIS Safeguards defend against.



Table 11. Percentage of ATT&CK(sub-)techniques that can bedefended against for the Malwareattack pattern

94% of ATT&CK (sub-) techniques in the Malware attack pattern can be defended against through implementation of CIS Safeguards.

The Malware attack pattern mapped to 209 unique ATT&CK (sub-)techniques²³, with CIS Safeguards defending against 152 of them. This number may seem low; however, out of the 209 ATT&CK (sub-)techniques, only 162 were assigned to an ATT&CK mitigation, which indicates the highest possible number of techniques that can be defended against across any security framework. Taking this into consideration, it was found that 94% of ATT&CK (sub-)techniques in the Malware attack pattern can be defended against through implementation of the CIS Safeguards, as shown below in Table 12.

Furthermore, out of the 162, 125 ATT&CK (sub-)techniques, or 77%, can be defended through implementation of IG1. This reinforces the security value that IG1 Safeguards can bring to an enterprise to defend against malware.

Table 12. Malware attack pattern data table	# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-) Techniques assigned To an att&CK mitigation	# OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	# OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By IG1 CIS Safeguards
	209	162	152	94%	125	77%

22 The set of ATT&CK (sub-)techniques required to execute an attack.23 Out of 530 total ATT&CK (sub-)techniques

Ransomware

Analysis found that 75% or more of the ATT&CK (sub-)techniques in 10 of the 14 ATT&CK tactics for the Ransomware attack pattern can be defended against through implementation of the CIS Safeguards, as shown below in Figure 7 and Table 13.



Figure 7. Ransomware attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

Table 13. Percentage of ATT&CK(sub-)techniques that canbe defended against for theRansomware attack pattern

Table 14. Ransomware attack

pattern data table

The Ransomware attack pattern mapped to a total of 229 unique ATT&CK (sub-)techniques (Table 14). Out of the 229, 182 ATT&CK (sub-)techniques were assigned an ATT&CK mitigation, indicating the highest possible number of techniques that can be defended against. Factoring this into the analysis, it was found that CIS Safeguards defend against 92% of the ATT&CK (sub-)techniques. Additionally, IG1 alone defend against 78% of Ransomware ATT&CK (sub-)techniques.

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES Assigned to an Att&CK mitigation	# OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	% OF ATT&CK (SUB-)TECHNIQUES Defended by The CIS Safeguards	# OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards
229	182	167	92%	142	78%

Web Application Hacking

Analysis of the Web Application Hacking attack pattern found that the CIS Safeguards defend against 75% or more ATT&CK (sub-)techniques in 11 of the 14 ATT&CK tactics, with six of those ATT&CK tactics having 100% coverage, as shown below in Figure 8 and Table 15.



In total, 143 unique ATT&CK (sub-)techniques were mapped to the Web Application Hacking attack pattern (Table 16). Of the 143, 120 ATT&CK (sub-)techniques were assigned to an ATT&CK mitigation and 117, or 98%, are defended through implementation of the CIS Safeguards. Of the 120, IG1 defends against 86% of the ATT&CK (sub-)techniques in this pattern.

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES Assigned to an Att&CK mitigation	# OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	# OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards
143	120	117	98%	103	86%

Figure 8. Web Application Hacking attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

 Table 15. Percentage of ATT&CK

 (sub-)techniques that can be

 defended against for the Web

 Application Hacking attack pattern

Table 16. Web Application Hackingattack pattern data table

Insider and Privilege Misuse

Analysis of the Insider and Privilege Misuse attack pattern found that the CIS Safeguards defend against 85% or more of the ATT&CK (sub-)techniques in 10 of the 14 ATT&CK tactics, seven of which have 100% coverage (shown in Figure 9 and Table 17 below).



Overall, 149 unique ATT&CK (sub-)techniques mapped to the Insider and Privilege Misuse attack pattern, with 112 having an assignment to an ATT&CK mitigation (Table 18). Analysis found that the CIS Safeguards defend against 90% of Insider and Privilege Misuse ATT&CK (sub-)techniques assigned to an ATT&CK mitigation, with IG1 defending against 86% of ATT&CK (sub-)techniques.

# OF MAPPED ATT&CK (SUB-)techniques	# OF ATT&CK (SUB-)TECHNIQUES Assigned to an Att&CK mitigation	# OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	# OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards
149	112	101	90%	96	86%

Figure 9. Insider and Privilege Misuse attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

 Table 17. Percentage of ATT&CK

 (sub-)techniques that can be

 defended against for the Insider

 and Privilege Misuse attack pattern

Table 18. Insider and Privilege

 Misuse attack pattern data table

Targeted Intrusions

In 10 of the 14 ATT&CK tactics, the CIS Safeguards defend against 75% or more ATT&CK (sub-)techniques associated with the Targeted Intrusions attack pattern, with five of those ATT&CK tactics having 100% coverage (shown in Figure 10 and Table 19 below).



Table 19. Percentage of ATT&CK(sub-)techniques that can bedefended against for the TargetedIntrusions attack pattern

Table 20. Targeted Intrusions attack

pattern data table

Overall, 197 unique ATT&CK (sub-)techniques were mapped to the Targeted Intrusions attack pattern (Table 20). Of the 197, 154 were assigned to an ATT&CK mitigation. As a result, CIS Safeguards defend against 95% of the Targeted Intrusions ATT&CK (sub-)techniques, with IG1 defending against 83%.

# OF MAPPED ATT&CK (SUB-)TECHNIQUES	# OF ATT&CK (SUB-)TECHNIQUES Assigned to an Att&Ck mitigation	# OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By the CIS safeguards	# OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards	% OF ATT&CK (SUB-) Techniques defended By IG1 CIS safeguards
197	154	146	95%	128	83%

Figure 10. Targeted Intrusions attack pattern coverage against CIS Safeguards (by IG) across ATT&CK tactics

Summary

One of the goals of the CDM is to determine the security value of IG1. We determined that an enterprise implementing IG1 can defend itself against the top five attack types. Overall, IG1 defends against 77% or more of ATT&CK (sub-)techniques²⁴. Implementing all of the CIS Safeguards defends against 90% or more of the ATT&CK (sub-)techniques. Shown in Table 21 below are the individual percentages for each attack type, broken down by IG1 Safeguards and all CIS Safeguards.

Table 21. Overall security value analysis

ATTACK TYPE	% OF ATT&CK (SUB-)TECHNIQUES Defended Against by Ig1 CIS safeguards	% OF ATT&CK (SUB-)TECHNIQUES Defended Against by CIS Safeguards
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider and Privilege Misuse	86%	90%
Targeted Intrusions	83%	95%

We also looked at CIS Safeguard coverage for the superset of ATT&CK (sub-)techniques used across all five attack types. Shown below in Figure 11 is the number of ATT&CK (sub-) techniques, by ATT&CK tactic and IG, that the CIS Safeguards defend against. When analyzed, it was found that the CIS Safeguards defend against 77% or more of the ATT&CK (sub-)techniques in 10 of the 14 ATT&CK tactics, as shown in Table 22 below. Also of note, was a particularly low percentage in ATT&CK tactics: TA0007, TA0009, TA0042, and TA0043. This is due to the majority of these ATT&CK (sub-)techniques having no assignment to an ATT&CK mitigation, or assigned, but difficult to defend against (e.g., LotL techniques).



Figure 11. CIS Safequard coverage (by IG) across all five attack types combined

Table 22. Data table showing number of ATT&CK (sub-) techniques mapped across all five attack types combined

CDM data also allowed us to look at a smaller subset of ATT&CK (sub-)techniques that apply to all five attack types, and the specific CIS Safeguards that can defend against those techniques. Shown below in Figures 12 and 13 are two heat maps, one for IG1 and one for all CIS Safeguards. The checkmarks symbolize that a specific CIS Safeguard can defend against a particular ATT&CK (sub-)technique. The varying "temperatures" of the charts tell us that the higher the total, the higher the effectiveness. This is yet another way that our analysis can be used to determine the effectiveness of implementing the CIS Safeguards in terms of defending against attacks.

Figure 12. IG1 CIS Safeguard heatmap against the top ATT&CK (sub-)techniques across all attack types

ATT&CK (SUB-)TECHNIQUE	ATT&CK (SUB-)TECHNIQUES USED ACROSS ALL ATTACK PATTERNS							IG1 CIS SAFEGUARDS (IN ORDER OF EFFECTIVENESS)																					
(SUB-)TECHNIQUE ID	(SUB-)TECHNIQUE NAME	4	1	4.7	5.3	6.1	6.2	5.4	6.4	6.5	5.2	2.3	4.2	4.4	6.3	11.3	3.3	5.1	10.1	10.2	11.4	3.1	3.4	8.1	8.2	8.3	14.1	14.3	TOTAL
T1098	Account Manipulation			V	0	Ø	Ø	Ø	Ø	Ø			0	0	0	0	V				0								14
T1136	Create Account				V	0	Ø	Ø	0	0			0	0	0	Ø					0								13
T1003	OS Credential Dumping				0	Ø	Ø	Ø			Ø					0											(10
T1021.001	Remote Desktop Protocol				0	Ø	Ø		0	Ø		0	0	0															10
T1070	Indicator Removal on Host					Ø	Ø	Ø									V					V	V	0	((10
T1078.002	Domain Accounts				V	Ø	V	Ø		Ø	Ø							0											9
T1059	Command and Scripting Interpreter				0	Ø	Ø	Ø				V							0	0									9
T1110	Brute Force				Ø					Ø	Ø				Ø														7
T1078	Valid Accounts				0	Ø	Ø	Ø			Ø							V											7
T1543.003	Windows Service				0	Ø	Ø	Ø																					6
T1027	Obfuscated Files or Information																		0	V									2
T1127	Trusted Developer Utilities Proxy Execution																												2
T1078.001	Default Accounts										Ø																		2
T1087	Account Discovery																												1
		TOTAL 1	0 :	10	9	9	9	8	5	5	5	3	3	3	3	3	2	2	2	2	2	1	1	1	1	1	1	1	

Figure 13. CIS Safeguard heatmap against the top ATT&CK (sub-)techniques across all attack types

ATT&CK (SUB-)TECHNIQU	ES USED ACROSS ALL ATTACK PATTERNS	CIS SA	FEGUAR	OS (IN OR	DER OF E	FFECTIV	/ENESS)	G1 I	G2	G3																																					
(SUB-)TECHNIQUE ID	(SUB-)TECHNIQUE NAME	4.1	4.7	5.3 6	.1 6.2	2 5.4	18.3	18.5	6.8	4.8	8 <mark>.12</mark> 5.	2 6.4	6.5 1	2.8 2	2.3 2.5	4.2	4.4	6.3 1	1.3 1	2.2 16.1	l <mark>o</mark> 2.7	3.11	3.3	5.1 5.5	10.1	10.2 10	0.7 11.	.4 13.2	13.7	16.1 16	.9 2.6	3.1	3.10	3.4 <mark>4.10</mark>	7.6	7.7 8.	.1 8.2	8.3	8.9 8	.10 9.	3 9.6	9.7	12.7 13.5	13.10 1	4.1 14.3	16.8 TI	OTAL
T1021.001	Remote Desktop Protocol	Ø	Ø	0			Ø	0	0	0	V	0	Ø	0	0 0					00															 Image: A start of the start of	<u> </u>							V V	V		1	24
T1059	Command and Scripting Interpreter		Ø	0					Ø	Ø					0 0)				<						0	>	 ✓ 																		1	22
T1098	Account Manipulation			0							V	0	Ø	>				Ø	0	V			V				 																			I	21
T1003	OS Credential Dumping		0	0					Ø		0								V			Ø								0															0 0		19
T1136	Create Account			0							V	0	Ø	>				Ø	0	V							 																			;	18
T1070	Indicator Removal on Host								Ø		V			>								()	V									Ø	()	/						V							17
T1078	Valid Accounts			0																				0						0																;	11
T1078.002	Domain Accounts			0					Ø															0																							11
T1543.003	Windows Service			0					0																																						9
T1110	Brute Force		0	V														Ø																													8
T1127	Trusted Developer Utilities Proxy Execution						0													<																											8
T1027	Obfuscated Files or Information																								Ø	0	>	0	0																		5
T1087	Account Discovery						0																																								4
T1078.001	Default Accounts		0																																												2
	ΤΟΤΑ	10	10	9	9 9	8	8	8	7	6	5 5	5	5	4	33	3	3	3	3	33	2	2	2	2 2	2	2	2 2	2 2	2	2 2	1	1	1	1 1	1	1 1	1 1	1	1	1 1	1	1	1 1	1	1 1	1	

Additionally, we created "attack cards" for each attack type, which provide a list of IG1 CIS Safeguards, in order of effectiveness, along with the corresponding ATT&CK (sub-)techniques that an enterprise will defend against through implementation. These, and other resources, can be found onCIS WorkBench.

It is worth noting that some ATT&CK (sub-)techniques were mapped to an attack pattern and were assigned an ATT&CK mitigation, but had no mapping to a CIS Safeguard. This list can be found in Appendix H of this guide.

Lastly, some ATT&CK (sub-)techniques were mapped to an attack pattern, but were not assigned to an ATT&CK mitigation (and therefore, had no mapping to a CIS Safeguard). This list can be found in Appendix I of this guide.

Conclusion

CDM v2.0 affirms the prioritization of the CIS Critical Security Controls and Implementation Groups. In particular, CDM data backs the premise that all enterprises should start with essential cyber hygiene, or IG1, as a way to defend against the top five attacks.

In summary, our analysis provides us with three key findings:

- IG1 provides a viable defense against the top five attack types. Enterprises achieve a high level of protection and are well-positioned to defend against the top five attack types through implementation of essential cyber hygiene, or IG1. These results strongly reinforce the value of a relatively small number of well-chosen and basic defensive steps (IG1). As such, enterprises should aim to start with IG1 to obtain the highest value and work up to IG2 and IG3, as appropriate.
- Independent of any specific attack type, the CIS Controls are effective at defending against a wide array of attacks. Specifically, the CIS Controls are effective at defending against 86% of the ATT&CK (sub-)techniques found in the ATT&CK framework. More importantly, the Controls are highly effective against the five attack types found in industry threat data. The bottom line is that the CIS Controls, and specifically IG1, are a robust foundation for your cybersecurity program.
- Establishing and maintaining a secure configuration process (CIS Safeguard 4.1) is a linchpin Safeguard for all five attack types. CIS Safeguard 4.1 is most effective in defending against the top five attack types, reinforcing the importance of secure configurations, such as those contained within the CIS Benchmarks.

Join our CDM Community on CIS WorkBench to take advantage of these and other great resources. CIS is dedicated to taking a "community-first" approach. Further resources can be found on our WorkBench site here. Please join our CDM Community on CIS WorkBench to take advantage of these and other great resources, as well as to participate in next year's CDM (v3.0).

Closing Notes

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this guide are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information Center for Internet Security 31 Tech Valley Drive East Greenbush, NY 12061 518.266.3460 controlsinfo@cisecurity.org

Future Work

The CDM is very much a continuous process, and will change as new threats emerge, new technologies are released, and new data is published. Our work is dynamic, and for all the right reasons. Results of this work feed into the evolution of the CIS Controls, as well as other CIS products and services.

For CDM v3.0, we hope to address the following:

- Additional data sources. Find additional data sources for the top attack types and patterns. This will help to further strengthen our analysis and provide additional insight to other sectors that may not be represented in the current data sources.
- Re-categorization of top attack types. During the writing of v2.0, and after analysis was
 completed, the 2021 Verizon DBIR was published along with their new categorization
 for attack patterns (what we call attack types). These attack patterns take a whole
 new approach to the way that attacks are viewed. We hope to further review the DBIR
 categorization schemas, as well as other data sources, to continually improve our
 categorization of attack types.
- More specific analyses. As we evolve with future versions of the CDM, our analysis will seek to perform even more in-depth analyses, to answer questions such as: "What is the specific 'point' in an attack where it can be thwarted completely?" and "What are the minimal set of Safeguards within IG1 that I need to implement to stop that attack?"
- More collaboration and correlation. As CIS Security Best Practices continues to mature our mappings to ATT&CK, we hope to incorporate CIS Benchmark mappings in next year's CDM.
- More external stakeholder engagement. As we all know, CIS is appreciative of our many volunteers within the CIS Community. None of this is possible without all of you. Next year, we will look to collaborate with even more enterprises to enhance and evolve future versions of the CDM.

We believe that future versions of the CDM can also provide a foundation for more detailed and specific analyses. For example, combined with other information (e.g., cost estimates for CIS Safeguards or through using different data sets), we could answer questions, such as:

- What is the most cost-effective way to obtain the security value of IG1?
- How can I make best security use of what I already own before I add technology, expense, and processes?
- If I use attack data that is unique to my industry sector, or threat intelligence that is unique to my company, which Safeguards should I implement to achieve an appropriate defensive strategy?
- Will my defenses be effective at multiple steps or tactics of the attack lifecycle?
- If I know the effectiveness of a specific CIS Safeguard (or its absence), can I intelligently 'tailor' my defenses to accommodate specific operational constraints (like the need to run legacy applications)?

We encourage readers to join our communities on CIS WorkBench to get updates, as well as contribute to future versions of the CDM. Email controlsinfo@cisecurity.org to get information on how to become a community member and more.

APPENDIX A Acronyms and Abbreviations

ATT&CK (sub-)techniques	ATT&CK techniques + ATT&CK sub-techniques
CDM	Community Defense Model
CISA®	Cybersecurity and Infrastructure Security Agency
CWE	Common Weakness Enumeration
DMARC	Domain-based Message Authentication, Reporting & Conformance
DNS	Domain Name System
DoS	Denial of Service
EDR	Endpoint Detection and Response
ENISA	European Network and Information Security Agency
ESET	Executive Security & Engineering Technologies, Inc.
IBM	International Business Machines Corporation
ICS	Industrial Control Systems
IG	Implementation Group
IG1	Implementation Group 1
JSON	JavaScript Object Notation
LotL	Living off the Land
MBR	Master Boot Record
MFA	Multi-Factor Authentication
MIB	Management Information Base
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST [®] CSF	National Institute of Standards and Technology Cybersecurity Framework
05	Operating System
ОТ	Occupational Technology
OWASP [®]	Open Web Application Security Project®
RDP	Remote Desktop Protocol
SLTT	State, Local, Tribal, and Territorial
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
ТТР	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator
VERIS Community Database	Vocabulary for Event Recording and Incident Sharing Community Database
Verizon DBIR	Verizon Data Breach Investigations Report
VNC	Virtual Network Computing
XSS	Cross-Site Scripting

APPENDIX B Links and Resources

- CIS Controls: https://www.cisecurity.org/controls/
- MITRE ATT&CK: https://attack.mitre.org/
- CIS Critical Security Controls v8: https://www.cisecurity. org/controls/v8/
- CDM v1.0: https://www.cisecurity.org/white-papers/ciscommunity-defense-model/
- CIS WorkBench: https://workbench.cisecurity.org/
- CIS Controls Navigator: https://www.cisecurity.org/ controls/cis-controls-navigator/
- CIS Controls Guide: Exploited Protocols: Remote Desktop Protocol: https://www.cisecurity.org/white-papers/ exploited-protocols-remote-desktop-protocol-rdp/
- 2020 Verizon¹ Data Breach Investigations Report (DBIR): https://enterprise.verizon.com/resources/reports/ dbir/2020/introduction/
- IBM X-Force² Threat Intelligence Index 2021: https://www. ibm.com/security/data-breach/threat-intelligence
- ENISA Threat Landscape The Year in Review (Published October 20, 2020): https://www.enisa.europa.eu/ publications/year-in-review
- CrowdStrike Services Cyber Front Lines Report 2020: https://www.crowdstrike.com/services/cyber-front-lines/
- Akamai The State of the Internet: A Year in Review 2020: https://www.akamai.com/our-thinking/the-state-of-theinternet
- Bitdefender³ Mid-Year Threat Landscape Report 2020: https://www.bitdefender.com/files/News/CaseStudies/ study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

- Multi-State Information Sharing and Analysis Center (MS-ISAC) Top 10 Malware: https://www.cisecurity.org/ ms-isac/
- CrowdStrike 2021 Global Threat Report: https://www. crowdstrike.com/resources/reports/global-threat-report/
- ESET Threat Report Q4 2020: https://www.welivesecurity. com/wp-content/uploads/2021/02/ESET_Threat_Report_ Q42020.pdf
- Check Point 2021 Cyber Security Report: https://www. checkpoint.com/pages/cyber-security-report-2021/
- Group-IB Ransomware Uncovered 2020-2021: https:// www.group-ib.com/resources/threat-research/ ransomware-2021.html
- OWASP Top 10⁴: https://owasp.org/www-project-top-ten/
- 2020 CWE Top 25: https://cwe.mitre.org/top25/ archive/2020/2020_cwe_top25.html
- Verizon Insider Threat Report 2019: https://enterprise. verizon.com/resources/reports/insider-threat-report/
- Securonix 2020 Insider Threat Report: https://www. securonix.com/resources/2020-insider-threat-report/
- G-Research Introducing the Insider Attack Matrix: https:// www.gresearch.co.uk/article/introducing-the-insiderattack-matrix/
- CISA SolarWinds and Active Directory/M365 Compromise Threat Report: https://us-cert.cisa.gov/sites/default/files/ publications/Supply_Chain_Compromise_Detecting_ APT_Activity_from_known_TTPs.pdf

- 1 Verizon is a registered trademark of Verizon Trademark Services, LLC.
- 2 IBM and X-Force are registered trademarks of International Business Machines Corporation.
- 3 Bitdefender is a registered trademark of Bitdefender IPR Management Ltd.
- 4 OWASP is a registered trademark of OWASP Foundation, Inc.

APPENDIX C Background

The CIS Critical Security Controls (CIS Controls) are a prioritized set of CIS Safeguards to mitigate the most common cyber-attacks against systems and networks. The volunteer experts who develop the CIS Controls come from a wide range of sectors including defense, education, government, healthcare, manufacturing, retail, transportation, and others.

The earliest versions of the CIS Controls were based on the consensus judgment of a relatively small number of experienced people and validated with public feedback from across the industry. The analysis was supported by a simple list of important attacks against which to examine possible CIS Controls. Over more recent versions, CIS has started to develop more data and rigor to underpin the process.

CIS started by working with the emerging marketplace of authoritative summaries of "real world" data about attacks beginning with the Verizon Data Breach Investigations Report (DBIR) in 2013. After the Verizon® team completed their initial attack analysis, a CIS volunteer team worked with Verizon to map the most important categories or types of attacks seen in the prior year's data to the CIS Controls, and this map became part of the Verizon DBIR Recommendations. Over the next couple of years, we repeated this process with several other security vendors.

While this approach is useful and based on summaries of data derived by each vendor from their own business model, there were several areas that had to be resolved:

- The vendor reports typically came from marketing departments, so the use of language was inconsistent across vendors and tended to be buzzword heavy
- There was no rigorous way to normalize the data and conclusions across different vendors
- The mapping from summaries and patterns of attack to the CIS Controls was still informal and based on the judgment of relatively few people

In our next step (in 2016), we developed the CIS Community Attack Model as a way to structure the discussion and the mapping from classes of attacks to the CIS Controls. Our goal was to create an open, high-level model in which classes of countermeasures (CIS Safeguards) were organized in two dimensions:

- 1 Steps of the attacker's lifecycle (similar to the well-known Lockheed Martin Cyber Kill Chain)
- 2 Categories of defensive effect, for which we used the Core Functions of the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

This approach helped CIS focus on questions like, "What types of countermeasures could help prevent the delivery phase of an attacker's lifecycle?"

You could also take a strategic view of defense by asking: "Am I over-invested in tools for detecting and preventing the early stages of attack, and under-invested if the initial steps of an attack succeed?"

While it was never fully operationalized, the Community Attack Model was a useful way to structure and capture the discussion about the value of Control selection. Ultimately, the Community Attack Model laid the groundwork for what we now know to be the Community Defense Model.

APPENDIX D ATT&CK (Sub-)Techniques with No Mapping to CIS Safeguards

The following ATT&CK (sub-)techniques were assigned to an ATT&CK mitigation; however, they had no mapping back to a CIS Safeguard.

ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME
T1090.004	Domain Fronting	T1586.001	Social Media Accounts	T1591.002	Business Relationships
T1480	Execution Guardrails	T1586.002	Email Accounts	T1591.003	Identify Business Tempo
T1480.001	Environmental Keying	T1587	Develop Capabilities	T1591.004	Identify Roles
T1583	Acquire Infrastructure	T1587.001	Malware	T1592	Gather Victim Host Information
T1583.001	Domains	T1587.002	Code Signing Certificates	T1592.001	Hardware
T1583.002	DNS Server	T1587.003	Digital Certificates	T1592.002	Software
T1583.003	Virtual Private Server	T1587.004	Exploits	T1592.003	Firmware
T1583.004	Server	T1588	Obtain Capabilities	T1592.004	Client Configurations
T1583.005	Botnet	T1588.001	Malware	T1593	Search Open Websites/Domains
T1583.006	Web Services	T1588.002	ТооІ	T1593.001	Social Media
T1584	Compromise Infrastructure	T1588.003	Code Signing Certificates	T1593.002	Search Engines
T1584.001	Domains	T1588.004	Digital Certificates	T1594	Search Victim-Owned Websites
T1584.002	DNS Server	T1588.005	Exploits	T1596	Search Open Technical Databases
T1584.003	Virtual Private Server	T1588.006	Vulnerabilities	T1596.001	DNS/Passive DNS
T1584.004	Server	T1589	Gather Victim Identity Information	T1596.002	WHOIS
T1584.005	Botnet	T1589.001	Credentials	T1596.003	Digital Certificates
T1584.006	Web Services	T1589.002	Email Addresses	T1596.004	CDNs
T1585	Establish Accounts	T1589.003	Employee Names	T1596.005	Scan Databases
T1585.001	Social Media Accounts	T1590.003	Network Trust Dependencies	T1597	Search Closed Sources
T1585.002	Email Accounts	T1591	Gather Victim Org Information	T1597.001	Threat Intel Vendors
T1586	Compromise Accounts	T1591.001	Determine Physical Locations	T1597.002	Purchase Technical Data

APPENDIXE ATT&CK (Sub-)Techniques with No Mapping to ATT&CK Mitigations

The following are the 84 MITRE ATT&CK (sub-)techniques that had no assignment to an ATT&CK mitigation. As per MITRE, these ATT&CK (sub-)techniques "cannot be easily mitigated with preventative controls since it is based on the abuse of system features," and therefore had no mapping to a CIS Safeguard (MITRE, 2021)¹.

ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME
T1005	Data from Local System	T1069.003	Cloud Groups	T1518.001	Security Software Discovery
T1006	Direct Volume Access	T1070.004	File Deletion	T1526	Cloud Service Discovery
T1007	System Service Discovery	T1070.005	Network Share Conn. Removal	T1529	System Shutdown/Reboot
T1010	Application Window Discovery	T1070.006	Timestomp	T1531	Account Access Removal
T1012	Query Registry	T1074	Data Staged	T1534	Internal Spearphishing
T1014	Rootkit	T1074.001	Local Data Staging	T1542.002	Component Firmware
T1016	System Network Config. Discovery	T1074.002	Remote Data Staging	T1546	Event Triggered Execution
T1018	Remote System Discovery	T1082	System Information Discovery	T1546.001	Change Default File Association
T1020	Automated Exfiltration	T1083	File and Directory Discovery	T1546.005	Тгар
T1025	Data from Removable Media	T1087.003	Email Account	T1546.007	Netsh Helper DLL
T1027.001	Binary Padding	T1113	Screen Capture	T1546.012	Image File Exec. Options Injection
T1027.003	Steganography	T1115	Clipboard Data	T1546.015	Component Obj. Model Hijacking
T1027.004	Compile After Delivery	T1120	Peripheral Device Discovery	T1547	Boot or Logon Autostart Execution
T1027.005	Indicator Removal from Tools	T1123	Audio Capture	T1547.001	Registry Run Keys / Startup Folder
T1033	System Owner/User Discovery	T1124	System Time Discovery	T1547.010	Port Monitors
T1036.002	Right-to-Left Override	T1125	Video Capture	T1553.002	Code Signing
T1036.004	Masquerade Task or Service	T1134.004	Parent PID Spoofing	T1555.002	Securityd Memory
T1036.006	Space after Filename	T1137.006	Add-ins	T1560.002	Archive via Library
T1039	Data from Network Shared Drive	T1140	Deobfuscate/Decode Files or Info.	T1560.003	Archive via Custom Method
T1049	System Network Conn. Discovery	T1202	Indirect Command Execution	T1564	Hide Artifacts
T1056	Input Capture	T1207	Rogue Domain Controller	T1564.001	Hidden Files and Directories
T1586.001	Social Media Accounts	T1217	Browser Bookmark Discovery	T1564.005	Hidden File System
T1586.002	Email Accounts	T1496	Resource Hijacking	T1568.001	Fast Flux DNS
T1056.001	Keylogging	T1497	Virtualization/Sandbox Evasion	T1568.003	DNS Calculation
T1056.004	Credential API Hooking	T1497.001	System Checks	T1578.004	Revert Cloud Instance
T1057	Process Discovery	T1497.002	User Activity Based Checks	T1600	Weaken Encryption
T1069	Permission Groups Discovery	T1497.003	Time Based Evasion	T1600.001	Reduce Key Space
T1069.001	Local Groups	T1505.003	Web Shell	T1600.002	Disable Crypto Hardware
T1069.002	Domain Groups	T1518	Software Discovery		

¹ MITRE ATT&CK https://attack.mitre.org/

APPENDIX F Unmapped CIS Safeguards to ATT&CK Framework

The following CIS Safeguards had no mapping to an ATT&CK mitigation or (sub-)technique.

CONTROL	SAFEGUARD	TITLE	IG1	IG2	IG3	CONTROL	SAFEGUARD	TITLE	IG1	IG2	IG3
1	1.3	Utilize an Active Discovery Tool		\checkmark	\checkmark	14	14.8	Train Workforce on the Dangers of	\checkmark	\checkmark	\checkmark
1	1.5	Use a Passive Asset Discovery Tool			\checkmark			Connecting to and Transmitting Enterprise			
3	3.5	Securely Dispose of Data	\checkmark	\checkmark	\checkmark			Data Over Insecure Networks		,	
3	3.7	Establish and Maintain a Data Classification Scheme		✓	<	15	15.1	Establish and Maintain an Inventory of Service Providers	~	 Image: A start of the start of	
3	3.8	Document Data Flows		√	\checkmark	15	15.2	Establish and Maintain a Service Provider		\checkmark	\checkmark
3	3.9	Encrypt Data on Removable Media		\checkmark	1	45	45.0	Management Policy		,	,
3	3.13	Deploy a Data Loss Prevention Solution			\checkmark	15	15.3	Classify Service Providers		V	V
3	3.14	Log Sensitive Data Access			1	15	15.4	Ensure Service Provider Contracts Include		V	V
4	4.3	Configure Automatic Session Locking on	✓	<	<	15	15.5	Assess Service Providers			1
4	111	Enferço Rometo Wino Canability en Portable		1	1	15	15.6	Monitor Service Providers			\checkmark
4	4.11	End-User Devices		•	×	16	16.6	Establish and Maintain a Severity Rating System and Process for Application		✓	✓
4	4.12	Separate Enterprise workspaces on Mobile End-User Devices			•			Vulnerabilities			
5	5.6	Centralize Account Management		✓	✓	16	16.7	Use Standard Hardening Configuration Templates for Application Infrastructure		√	 Image: A start of the start of
6	6.6	Establish and Maintain an Inventory of Authentication and Authorization Systems		✓	✓	16	16.10	Apply Secure Design Principles in Application Architectures		√	1
6	6.7	Centralize Access Control		\checkmark	\checkmark	16	16.14	Conduct Threat Modeling			1
8	8.4	Standardize Time Synchronization		\checkmark	\checkmark	17	17.1	Designate Personnel to Manage Incident	\checkmark	\checkmark	1
8	8.6	Collect DNS Query Audit Logs		\checkmark	\checkmark			Handling			
8	8.7	Collect URL Request Audit Logs		\checkmark	\checkmark	17	17.2	Establish and Maintain Contact Information	\checkmark	\checkmark	\checkmark
8	8.8	Collect Command-Line Audit Logs		\checkmark	\checkmark			for Reporting Security Incidents			
8	8.12	Collect Service Provider Logs			\checkmark	17	17.3	Establish and Maintain an Enterprise Process	\checkmark	\checkmark	\checkmark
9	9.5	Implement DMARC		\checkmark	\checkmark	17		for Reporting Incidents			
10	10.4	Configure Automatic Anti-Malware Scanning of Removable Media			 Image: A start of the start of	17	17.4	Establish and Maintain an Incident Response Process		V	v
10	10.6	Centrally Manage Anti-Malware Software		\checkmark	\checkmark	17	17.5	Assign Key Roles and Responsibilities		\checkmark	\checkmark
12	12.3	Securely Manage Network Infrastructure		\checkmark	\checkmark	17	17.6	Define Mechanisms for Communicating		\checkmark	\checkmark
12	12.4	Establish and Maintain Architecture		<	✓	17	17.7	During Incident Response		5	J
12	121	Contralize Socurity Event Morting		1	1			Exercises			1
13	13.1	Collect Network Traffic Flow Logs			× ·	17	17.8	Conduct Post-Incident Reviews		\checkmark	1
13	13.11	Tune Security Event Alerting Thresholds		V	V ./	17	17.9	Establish and Maintain Security Incident			1
1/	1/17	Train Workforce on How to Identify and	./	./	× ./			Thresholds			
14	141	Report if Their Enterprise Assets are Missing Security Updates	v	v	v	18	18.4	Validate Security Measures			✓

APPENDIX G ATT&CK Navigator¹ Visualizations for Attack Patterns

A full listing of JavaScript Object Notation (JSON) files can be found on CIS WorkBench here.



	TA0011: Command and Control	
ata	T1071: Application Laver	T1
ustom	Protocol	Ť
aotom	T1071.004: DNS	Ť1
ibrary	T1071.002: File Transfer	Alt
tility	Protocols	
	T1071.003: Mail Protocols	
on	T1071.001: Web Protocols	
	T1092: Communication Through	
ation	Removable Media	
	T1132: Data Encoding	
ion	T1132.002: Non-Standard	
	Encoding	
stem	T1132.001: Standard Encoding	
	T1001: Data Obfuscation	T1
	T1568: Dynamic Resolution	Ch
ole	T1568.003: DNS Calculation	T1
	T1568.002: Domain Generation	Ne
	Algorithms	T1
aging	T1568.001: Fast Flux DNS	Me
	T1573: Encrypted Channel	T1
	T1573.002: Asymmetric	Se
	Cryptography	
rding	11573.001: Symmetric	
	Cryptography	
	11008: Fallback Channels	
	T1105: Ingress Tool Transfer	11
	T1005: Nen Application Laws	
	Distance	
	PTOLOCOI T1571: Non Standard Part	
	T1571: NOII-Stalluaru Fort	
	T1000: Provy	
	T1090 004: Domain Fronting	
	T1090.004: External Provy	
	T1090.001: Internal Provy	
	T1090.003: Multi-hon Proxy	
	T1219: Remote Access Software	
	T1205: Traffic Signaling	
	T1102: Web Service	
	T1102.002: Bidirectional	
	Communication	
	T1102.001: Dead Drop	
	Resolver	
	T1102.003: One-Way	
	Communication	

TA0010: Exfiltration
T1020: Automated Exfiltration
T1030: Data Transfer Size Limits
T1048: Exfiltration Over
Alternative Protocol
T1048.002: Exfiltration Over
Asymmetric Encrypted Non-C2
Protocol
T1048.001: Exfiltration Over
Symmetric Encrypted Non-C2
Protocol
T1048.003: Exfiltration Over
Unencrypted/Obfuscated
Non-C2 Protocol
T1041: Exfiltration Over C2
Channel
T1011: Exfiltration Over Other
Network Medium
T1052: Exfiltration Over Physical
Medium
T1567: Exfiltration Over Web
Service
T1567.002: Exfiltration to
Cloud Storage
T1567.001: Exfiltration to Code
Repository

- 1029: Scheduled Transfer
- T1531: Account Access T1485: Data Destruction T1486: Data Encrypted f Impact T1565: Data Manipulation T1491: Defacement T1561: Disk Wipe T1499: Endpoint Denial of Service T1495: Firmware Corruption T1490: Inhibit System Recovery T1498: Network Denial of Service T1496: Resource Hijacking T1489: Service Stop T1529: System Shutdown/ ource Hijacking

Ransomware

TA0043: Reconnaissance T1595: Active Scanning T1592: Gather Victim Host naissance T1583: T150 T150 T150 T158 T158 T1592.004: Client T1592.004: Client Configurations T1592.003: Firmware T1592.001: Hardware T1592.002: Software T1589: Gather Victim Identity Serv T158 I1589: Gather Victim Identity Information T1589.001: Credentials T1589.002: Email Addresses T1589.03: Employee Names T1590: Gather Victim Network T1586: T1584: Infrastr T1587: T1587: Cert T15 Information T1591: Gather Victim Org Information T1598: Phishing for Information T15 T1585: T1588: (T1588: (Certifi T1588 T1588 T1598.002: Spearphishing Attachment T1598.003: Spearphishing Link T1598.001: Spearphishing Service T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/ Domains T1594: Search Victim-Owned Website

TA0042: Resource	TA0001: Initial Access	TA0002:
Development	T1189: Drive-by Compromise	T1059: Comman
Acquire Infrastructure	T1190: Exploit Public-Facing	Interpreter
83.005: Botnet	Application	T1059.002: A
83.002: DNS Server	T1133: External Remote	T1059.007: Ja
83.001: Domains	Services	T1059.008: N
83.004: Server	T1200: Hardware Additions	Device CLI
83.003: Virtual Private	T1566: Phishing	T1059.001: P
ver	T1566.001: Spearphishing	T1059.006: P
83.006: Web Services	Attachment	T1059.004: U
Compromise Accounts	T1566.002: Spearphishing	T1059.005: V
Compromise	Link	T1059.003: W
ructure	T1566.003: Spearphishing	Command Sh
Develop Capabilities	via Service	T1203: Exploita
87.002: Code Signing	T1091: Replication Through	Execution
tificates	Removable Media	T1559: Inter-Pro
87.003: Digital Certificates	T1195: Supply Chain	Communication
87.004: Exploits	Compromise	T1106: Native A
87.001: Malware	T1195.003: Compromise	T1053: Schedul
Establish Accounts	Hardware Supply Chain	T1129: Shared
Obtain Capabilities	T1195.001: Compromise	T1072: Software
88.003: Code Signing	Software Dependencies and	Tools
tificates	Development Tools	T1569: System
88.004: Digital Certificates	T1195.002: Compromise	T1569.001: L
88.005: Exploits	Software Supply Chain	T1569.002: S
88.001: Malware	T1199: Trusted Relationship	T1204: User Exe
88.002: 1001	T1078: Valid Accounts	11204.002: N
88.006: Vulnerabilities	11078.004: Cloud Accounts	11204.001: N
	11078.001: Default Accounts	11047: Window
	11078.002: Domain Accounts	Instrumentation
	110/8.003: Local Accounts	

Execution	TA0003: Persistence
nd and Scripting	T1098: Account Manipulation
	T1197: BITS Jobs
AppleScript	T1547: Boot or Logon Autostar
avaScript/JScript	Execution
Vetwork	T1037: Boot or Logon
	Initialization Scripts
PowerShell	T1037.002: Logon Script
Python	(Mac)
Jnix Shell	T1037.001: Logon Script
/isual Basic	(Windows)
Vindows	T1037.003: Network Logon
hell	Script
ation for Client	T1037.004: Rc.common
	T1037.005: Startup Items
ocess	T1176: Browser Extensions
n	T1554: Compromise Client
API	Software Binary
led Task/Job	T1136: Create Account
Modules	T1543: Create or Modify Syste
e Deployment	Process
	T1546: Event Triggered
Services	Execution
aunchctl	T1133: External Remote
Service Execution	Services
ecution	T1574: Hijack Execution Flow
Malicious File	T1137: Office Application
Malicious Link	Startup
/s Management	T1137.006: Add-ins
n	T1137 001 Office Template

ogon ms ins nt

Domain: Enterprise ATT&CK v8

System

nplate

Macros T1137.002: Office Test T1137.003: Outlook Forms T1137.004: Outlook Home Page T1137.005: Outlook Rules T1542: Pre-OS Boot T1053: Scheduled Task/Job T1505: Server Software

Component T1505.001: SQL Stored

Procedures T1505.002: Transport Agent T1505.003: Web Shell T1205: Traffic Signaling T1078: Valid Accounts

ice	TA0004: Privilege Escalation	
Ilation	T1548: Abuse Elevation Control Mechanism	T1548: /
	T1548.002: Bypass User Account Control	T1134: /
utostart	T1548.004: Elevated Execution with Prompt	T113
	11548.001: Setuid and Setgid	T113
	T1548.003: Sudo and Sudo Caching	T113
rint	T1134 ACCESS TOKEN Wallipulation	T113
npt	T1134.002: Make and Impersonate Token	T1197
ript	T1134.004: Parent PID Spoofing	T1140: I
	T1134.005: SID-History Injection	T1006:
Logon	T1134.001: Token Impersonation/Theft	T1484: I
-	T1547: Boot or Logon Autostart Execution	T148
on	T1547.002: Authentication Package	T148
ems	T1547.006: Kernel Modules and Extensions	T1480: I
ions	1154/.008: LSASS Driver	11211:1
ent	T1547.011: Plist Modification	
	T1547.010: Port Monitors	T1504: 1
v System	T1547.012. Fill Flocessors	T150
, oystem	T1547.001: Registry Run Keys / Startup Folder	T156
	T1547.005: Security Support Provider	T156
	T1547.009: Shortcut Modification	T156
e	T1547.003: Time Providers	T156
	T1547.004: Winlogon Helper DLL	T156
n Flow	T1037: Boot or Logon Initialization Scripts	T1574: I
on	T1543: Create or Modify System Process	T157
	11543.001: Launch Agent	115/
nnloto	T1543.004: Launch Daemon	<u>115/</u>
lipiale	T1543.002: Systemu Service	T157
t	T1484: Domain Policy Modification	T157
orms	T1546: Event Triggered Execution	T157
lome	T1546.004: .bash profile and .bashrc	T157
	T1546.008: Accessibility Features	T157
lules	T1546.009: AppCert DLLs	T157
	T1546.010: AppInit DLLs	T157
/Job	T1546.011: Application Shimming	T1562: I
	11546.001: Change Default File Association	1156
d	T1546.015: Component Ubject Model Hijacking	T150
u	T1546.012: Image File Execution Options	T156
Agent	Injection	T150
	T1546.006: LC_LOAD_DYLIB Addition	T1070: I
	T1546.007: Netsh Helper DLL	T107
	T1546.013: PowerShell Profile	T107
	T1546.002: Screensaver	T107
	T1546.005: Trap	T107
	11546.003: Windows Management	T107
	Instrumentation Event Subscription	110/
	T1574: Hijpek Execution Flow	T1026
	T1055: Process Injection	T1030.1
	T1055.004: Asynchronous Procedure Call	T103
	T1055.001: Dynamic-link Library Injection	T103
	T1055.011: Extra Window Memory Injection	T103
	T1055.002: Portable Executable Injection	T103
	T1055.009: Proc Memory	T103
	T1055.013: Process Doppelgänging	T1556:
	T1055.012: Process Hollowing	1155
	T1055 002: Thread Execution Hildebing	<u>1155</u>
	T1055.005: Thread Local Storage	1155 T1F5
	T1055.005: Tileau Local Storage	T1112-
	T1053: Scheduled Task/lob	T1601
	T1053.001: At (Linux)	T1599: I
	T1053.002: At (Windows)	T1027: 0
	T1053.003: Cron	T102
	T1053.004: Launchd	T102
	T1053.005: Scheduled Task	T102
	T1053.006: Systemd Timers	T102
	11078: Valid Accounts	1102

TA0005: Defense Evasion	TA0006: Credential Acce
T1548: Abuse Elevation Control Mechanism	T1110: Brute Force
T1134: Access Token Manipulation	T1110.004: Credential
T1134.002: Create Process with Token	Stuffing
T1134.003: Make and Impersonate loken	Crocking
T1134.005: SID-History Injection	T1110.001: Password
T1134.001: Token Impersonation/Theft	Guessing
T1197: BITS Jobs	T1110.003: Password
T1140: Deobfuscate/Decode Files or Information	Spraying
11006: Direct Volume Access	11555: Credentials from
T1484.002 Domain Trust Modification	T1555 003 Credentials fr
T1484.001: Group Policy Modification	Web Browsers
T1480: Execution Guardrails	T1555.001: Keychain
T1211: Exploitation for Defense Evasion	T1555.002: Securityd Mer
T1222: File and Directory Permissions Modification	T1212: Exploitation for
T1564.005: Hiddon File System	T1197: Forced Authonticati
T1564.001: Hidden Files and Directories	T1606: Forge Web Credenti
T1564.002: Hidden Users	T1056: Input Capture
T1564.003: Hidden Window	T1056.004: Credential AP
T1564.004: NTFS File Attributes	Hooking
T1564.007: VPA Stemping	T1056.002: GUI Input Cap
T1574: Hijack Execution Flow	T1056.003: Web Portal
T1574.012: COR PROFILER	Capture
T1574.001: DLL Search Order Hijacking	T1557: Man-in-the-Middle
T1574.002: DLL Side-Loading	T1557.002: ARP Cache
T1574.004: Dylib Hijacking	Poisoning
T1574.005: EXECUTABLE INSTALLER FILE PERMISSIONS WEAKNESS	Poisoning and SMR Pola
T1574.007: Path Interception by PATH Environment Variable	T1556: Modify Authenticati
T1574.008: Path Interception by Search Order Hijacking	Process
T1574.009: Path Interception by Unquoted Path	T1040: Network Sniffing
11574.010: Services File Permissions Weakness	T1003: OS Credential Dump
110/4.011: Services Registry Permissions Weakness	11003.008: /etc/passwd
T1562.004: Disable or Modify System Firewall	T1003.005: Cached Domo
T1562.001: Disable or Modify Tools	Credentials
T1562.002: Disable Windows Event Logging	T1003.006: DCSync
T1562.003: Impair Command History Logging	T1003.004: LSA Secrets
T1562.006: Indicator Blocking	T1003.001: LSASS Memo
T1070 002: Clear Command History	11003.003: NTD5 T1002.007: Proc Eilocycto
T1070.002: Clear Linux or Mac System Logs	T1003.002: Security Acco
T1070.001: Clear Windows Event Logs	Manager
T1070.004: File Deletion	T1528: Steal Application
T1070.005: Network Share Connection Removal	Access Token
T1070.006: Timestomp	T1558: Steal or Forge Kerbe
T1026: Masquerading	T1520: Stool Wob Soccion
T1036.001: Invalid Code Signature	Conkie
T1036.004: Masguerade Task or Service	T1111: Two-Factor
T1036.005: Match Legitimate Name or Location	Authentication Interception
T1036.003: Rename System Utilities	T1552: Unsecured Credenti
T1036.002: Right-to-Left Override	T1552.003: Bash History
T1556: Modify Authentication Process	In Files
T1556.001: Domain Controller Authentication	T1552.002: Credentials in
T1556.004: Network Device Authentication	Registry
T1556.002: Password Filter DLL	T1552.006: Group Policy
T1556.003: Pluggable Authentication Modules	Preferences
T1601: Modify System Image	11002.004: Private Keys
T1599: Network Boundary Bridging	
T1027: Obfuscated Files or Information	
T1027.001: Binary Padding	
11027.004: Compile After Delivery	
T1027 005: Indianter Removal from Taolo	
T1027.005: Indicator Removal from Tools	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-OS Boot	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-0S Boot T1055: Process Injection	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-05 Boot T1552: Process Injection T1202: Rogue Domain Controller T12012: Rogue Domain Controller	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-OS Boot T1055: Process Injection T1207: Rogue Domain Controller T1014: Rootkit T1214: Since Binary Provy Everytion	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-OS Boot T1055: Process Injection T1055: Process Injection T1207: Rogue Domain Controller T1014: Rootkit T1218: Signed Binary Proxy Execution T1218: 003: CMSTP	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1027: Pro-DS Boot T1055: Process Injection T1027: Roque Domain Controller T1014: Roothit T1218: Signed Binary Proxy Execution T1218:003: CMSTP T1218:003: Compiled HTML File	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1052: Process Injection T1055: Process Injection T1207: Rogue Domain Controller T1218: Signed Binary Proxy Execution T1218: Signed Binary Binary Binary Binary Binary Binary Binary Binary Binar	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Steganography T1542: Pre-OS Boot T1055: Process Injection T1207: Rogue Domain Controller T1214: Sonde Binary Proxy Execution T1218:003: CMSTP T1218.001: Compiled HTML File T1218.001: Control Panel T1218.004: InstallUtil T1218.004: InstallUtil T1218.004: InstallUtil	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1055: Process Injection T1055: Process Injection T1014: Roothit T1014: Roothit T1218.003: CMSTP T1218.003: CMSTP T1218.003: Compiled HTML File T1218.002: Control Panel T1218.003: Mshta T1218.005: Mshta T1218.005: Mshta	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1528: Pre-05 Boot T1055: Process Injection T1207: Rogue Domain Controller T1014: Rootkit T1218: Signed Binary Proxy Execution T1218: Signed Binary Proxy Execu	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1077.003: Steganography T1055: Process Injection T1055: Process Injection T1218: Signed Binary Proxy Execution T1218: Signed Binary Bi	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1055: Process Injection T1055: Process Injection T1055: Process Injection T1014: Roothit T1014: Roothit T1218: Staned Binary Proxy Execution T1218: 003: CMSTP T1218:003: Compiled HTML File T1218:004: InstallUtil T1218:005: Mshta T1218:005: Mshta T1218:009: Regsvcs/Regasm T1218:009: Regsvcs/Regasm	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1077.003: Steganography T1542: Pre-05 Boot T1055: Process Injection T1207: Rogue Domain Controller T1014: Rootkit T1218: Signed Binary Proxy Execution T1218: Signed Binary Proxy Execu	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1077.003: Steganography T1542: Pre-05 Boot T1555: Process Injection T1207: Rogue Domain Controller T1017: Rogue Domain Controller T1218: Silgened Binary Proxy Execution T1218: Solice Binary Proxy Execution T1218: Solice Control Panel T1218: Solice Odbcconf T1218: Solice Odbcconf T1218: Solice Odbcconf T1218: Solice Odsconf	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-05 Boot T1055: Process Injection T1218: Signed Binary Proxy Execution T1218: Signed Script Proxy Execution T1253: Subvert Trust Controls	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1047: Rocuse Sinjection T1055: Process Injection T1017: Rogue Domain Controller T1014: Rootit T1218: Signed Binary Proxy Execution T1218: Ookit T1218: Olitic T1218: Olitic T1218: Olitic T1218: Olitic T1218: Olitic T1218: Signed Script Proxy Execution T1216: Signed Script Proxy Execution T1314: Sourd Code Signing	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1055: Process Injection T1055: Process Injection T1017: Rogue Domain Controller T1014: Rootkit T1218: 003: CMSTP T1218: 003: Compiled HTML File T1218: 004: InstallUtil T1218: 005: Ompiled HTML File T1218: 006: InstallUtil T1218: 007: Misteec T1218: 008: Regswc3/Regasm T1218: 008: Gorigh Corey Execution T1218: 019: Control Fanel T1218: 019: Constrol Fanel T1218: 019: Constrol Fanel T1218: 019: Constrol Fanel T1218: 019: Regswc3/Regasm T1218: 019: Code Signing T1218: 019: Code Signing T1218: 019: Code Signing T153: 001: Gatekeepere Bypass T153: 001: Gatekeepere Bypass	
T1027.005: Indicator Removal from Tools T1027.005: Software Packing T1027.003: Steganography T1542: Pre-05 Boot T1555: Process Injection T1207: Rogue Domain Controller T1017: Rogue Domain Controller T1218: Silgened Binary Proxy Execution T1218: Solice Binary B	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1142: Pre-05 Boot T1055: Process Injection T1055: Process Injection T1055: Process Injection T1014: Roothit T1218: Signed Binary Proxy Execution T1218: 00: Compiled HTML File T1218: 00: Control Panel T1218: 00: Registric T1218: 01: Rundli32 T1218: 01: Rundli32 T1218: 01: Registric T1218: Signed Script Proxy Execution T1553: 00: Gatekeeper Bypass T1553: 00: SiP and Trust Provider Hijacking T1221: T153: 00: SiP and Trust Provider Hijacking	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1077.002: Software Packing T1027.003: Steganography T1555: Process Injection T1055: Process Injection T1055: Process Injection T1218: Signed Binary Proxy Execution T1218: Signed Signed Gript Proxy Execution T1218: Signed Signe	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1055: Process Injection T1055: Process Injection T1218: 003: Completed HTML File T1218: 003: Completed HTML File T1218: 003: Control Panel T1218: 003: Control Panel T1218: 003: Octor Panel T1218: 004: Installutii T1218: 005: Mshta T1218: 009: Regsvcs/Regasm T1218: 009: Regsvcs/Regasm T1218: 010: Gorde Script Proxy Execution T1218: 010: Gatekeeper Bypass T1553: 020: Gorde Signing T1553: 020: Gorde Signing T1553: 030: Install Root Certificate T1553: 040: Install Root Certificate T1553: 051: Raffice Signaling T1553: Taffice Signaling T1553: Taffice Signaling T1554: Beveloper Utilities Proxy Execution	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1047: Rocue Domain Controller T1014: Rockit T1014: Rockit T1218.003: CMSTP T1218.003: CMSTP T1218.003: CMSTP T1218.003: CMSTP T1218.003: CMSTP T1218.004: CMSTP T1218.005: CMSTP T1218.007: CMSTP T1218.007: Majac T1218.007: Majac <	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T155: Process Injection T105: Frocess Injection T1027: Rogue Domain Controller T1014: Roothit T1218: Signed Binary Proxy Execution T1218: Olicity Compiled HML File T1218: 002: Control Panel T1218: 002: Control Panel T1218: 002: Control Panel T1218: 005: Mshta T1218: 006: Mshta T1218: 007: Misexec T1218: 008: Regswc3/Regam T1218: 011: Rundli32 T1218: 012: Verclsid T1218: 012: Code Signing T1553: 000: Code Signing T1553: 000: Signal on Trust Provider Hijacking T1218: 011: Rundli32 T1553: 001: Gatekeeper Bypass T1553: 001: Gatekeeper Bypass T1553: 001: Gatekeeper Bypass T1553: 001: Gatekeeper Hijacking T1226: Tarific Signaling T1257: Trusted Developer Utilities Proxy Execution T127: Trusted Developer Utilities Proxy Execution	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1055: Process Injection T1055: Process Injection T1017: Rogue Domain Controller T1014: Rootkit T1218: 003: CMSTP T1218: 003: Compiled HTML File T1218: 004: InstallUtil T1218: 005: Mshta T1218: 005: Mshta T1218: 006: Mshta T1218: 007: Msixeec T1218: 008: Odboconf T1218: 009: Regswc3/Regasm T1218: 001: Regsw32 T1218: 002: Contol Static T1218: 010: Regsw32 T1218: 010: Regsw33 T	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Steganography T1047: Roque Domain Controller T1014: Rootkit T1218: Signed Binary Proxy Execution T1218: Olio: Compiled HTML File T1218: 003: CMSTP T1218: 003: CMSTP T1218: 003: CMSTP T1218: 004: CMSTP T1218: 003: Compiled HTML File T1218: 004: Compiled HTML File T1218: 005: Mshta T1218: 007: Msiexec T1218: 008: Odbcconf T1218: 008: Odbcconf T1218: 001: Kegsvs2 T1218: 011: Rundil32 T1218: 012: Vercisid T1218: 012: Vercisid T1218: 012: Vercisid T1218: 012: Kegsvs2 T128: 014: Install Wold Certificate T1553: 005: Signing T1553: 005: Signing T1553: 005: Signing T1553: Taffic Signaling T1221: Termplate Injection T1221: Termplate Injection T1221: Taffic Signaling T1221: Taffic Signaling T1227: Tool: MSBuild T1227: Tool: MSBuild T1227: 001: MSBuild	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1128: Pre-05 Boot T1055: Process Injection T1055: Process Injection T1017: Rogue Domain Controller T1014: Rootit T1218: Signed Binary Proxy Execution T1218: Oto; Compiled HTML File T1218: 002: Control Panel T1218: 002: Control Panel T1218: 003: Msitexec T1218: 003: Regsvcs/Regasm T1218: 004: Msitexec T1218: 007: Regsvcs/Regasm T1218: 008: Regsvcs/Regasm T1218: 001: Gatekeeper Bypass T1218: Signed Script Proxy Execution T1218: Signed Script Proxy Execution T1553: 001: Gatekeeper Bypass T1553: 001: Signaling T1553: 001: Signaling T1521: Tistic Bignaling T1221: Tisted Developer Utilities Proxy Execution T1220: Traffic Signaling T1220: Signaling T1220: Signaling T1220: Traffic Signaling T1220: Traffic Signaling T1220: Traffic Signaling T1220: Signaling T1220: Traffic Signaling T1220: Traffic	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.003: Steganography T1542: Pre-05 Boot T1055: Process Injection T1027: Rogue Domain Controller T1014: Rootkit T1218: Signed Binary Proxy Execution T1218: Signed Gorigh Croxy Execution T1218: Signed Gorigh Proxy Execution T1250: Signed Signed Frovy Execution T1260: Traffic Signaling T1227: Trusted Developer Utilities Proxy Execution T1260: Traffic Signaling T120: Traffic Signaling T120: Traffic Signaling T120: Traffic Signaling T122: Trus	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Steganography T1047: Roque Domain Controller T1014: Rootkit T1218: Signed Binary Proxy Execution T1218: Olicity Compiled HTML File T1218: 003: Compiled HTML File T1218: 004: Compiled HTML File T1218: 005: Mshta T1218: 007: Msizece T1218: 001: Registration T1218: 001: Registration T1218: 001: Registration T1218: 002: Control Panel T1218: 001: Msizece T1218: 001: Registration T1218: 001: Gatekeeper Bypass T1553: 002: Code Signing T1553: 002: Code Signing T1553: 003: SIP and Trust Provider Hijacking T1221: Template Injection T1221: Template Injection T1221: Turbalte Injection T1221: Turbalte Injection T1221: Turbalte Injection	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Software Packing T1027.002: Steganography T1128: Pre-05 Boot T1055: Process Injection T1027: Rogue Domain Controller T1014: Rootit T1218: Signed Binary Proxy Execution T1218: Orotit T1218: Origit	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1077.002: Software Packing T1027.002: Software Packing T1055: Process Injection T1055: Process Injection T1055: Process Injection T1218: Signed Binary Proxy Execution T1218: Signed Script Proxy Execution T1218: Signed Script Proxy Execution T1218: Signed Script Proxy Execution T1228: Testife Signaling T1220: Traffe Signaling T1220: Traffe Signaling T1220: Traffe Signaling T1220: Traffe Signaling T1220: Tarife Signaling T1220: Traffe Signaling	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Steganography T1142: Pre-05 Boot T1055: Process Injection T1055: Process Injection T1055: Process Injection T1014: Roothit T1218.003: CMSTP T1218.003: CMSTP T1218.003: CMSTP T1218.003: Compiled HTML File T1218.004: Install/Uli T1218.005: Mshta T1218.006: Objoconf T1218.007: Msizeec T1218.008: Objoconf T1218.009: Registors/Regasm T1218.010: Registors/Regasm T1218.011: Rundil32 T1218.012: Vercisid T1218.002: Controls T1553.002: Code Signing T1553.002: Code Signing T1553.003: SIP and Trust Provide Hijacking T1221: Termplate Injection T1221: Termplate Injection T1221: Termplate Injection T1227: Torgis Developer Utilities Proxy Execution T128: Traffic Signaling T129: Torgis Signing T1260: Use Alternate Authentication Material T1550:002: Pass the Hash T1550:003: Passthe Hash	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Software Packing T1027.002: Steganography T1147: Rocuse Sinjection T1055: Process Injection T1027: Rogue Domain Controller T1014: Roothit T1218: Signed Binary Proxy Execution T1218: ODD: Compiled HTML File T1218: ODD: Compiled HTML File T1218: ODD: Mshta T1218: ODD: Regsvs:2 T1218: ODD: Regsvs:2 T1218: ODD: Regsvs:2 T1218: ODD: Regsvs:2 T1218: ODD: Gatekeeper Bypass T155: ODD: Gatekeeper Bypass T155: ODD: Stepa drug Trovy Execution T1220: Traffic Signaling T1220: Traffic Signaling T1220: Traffic Signaling T1220: Stepa drug trug trug trug trug trug T1220: Traffic Signaling T1220: Traffic Signaling T1220: Traffic	
T1027.005: Indicator Removal from Tools T1027.002: Software Packing T1027.002: Software Packing T1027.003: Steganography T1555: Process Injection T1055: Process Injection T1027.002: Steganography T1218.003: CMSTP T1218.003: CMSTP T1218.003: CMSTP T1218.002: Control Panel T1218.002: Control Panel T1218.002: Control Panel T1218.003: MSTP T1218.004: Install/Util T1218.005: Mshta T1218.005: Mshta T1218.007: Msjexec T1218.008: Mshta T1218.008: Mshta T1218.001: Regsw32 T1218.001: Regsw32 T1218.011: Rundli32 T1218.012: Verclsid T1218.012: Code Signing T1553.002: Code Signing T1553.002: Code Signing T1553.003: SiP and Trust Provider Hijacking T1226: Tarific Signaling T127: Trusted Developer Utilities Proxy Execution T127: Trusted Developer U	

Platforms: Linux®, macOS®, Windows®, Office 365®, Azure® AD, IaaS, SaaS, PRE, Network

Registry T1552.006: Group Policy Preferences T1552.004: Private Keys

TANNNA: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009. Col
T1110: Bruto Eorco	T1097: Account Discovery	T1210: Exploitation of Pomoto	T1560: Archivo Col
T1110. Dittle Force	T1010: Application Window	Somicos	T1560.002: Arch
Stuffing	Discovery	T1534: Internal Spearnhishing	Custom Method
T1110.002: Password	T1217: Browsor Bookmark	T1570: Lateral Tool Transfor	T1560.002: Arch
Cracking	Discovery	T1562: Domoto Sorvico Soccion	Library
T1110.001: Paceword	T1E29: Cloud Service	Hijocking	T1560.001: Arch
Guoceing	Deebboard	T1562 002: DDD Hijacking	T1122: Audio Cant
T1110.002: Password	T1E26: Cloud Service Discovery	T1562 001: SSH Hijacking	T1123. Automated
Spraving	T1492: Domain Trust Discovery	T1021: Pomoto Sonvices	T1115: Automateu
T1555: Crodontials from	T1002: Dollidill Hust Discovery	T1021. Nelliole Services	T1602: Data from (
Password Stores	Discovery	Component Object Medal	Popository
T1555 002: Crodontials from	T1046: Network Service	T1021 001: Romoto Dockton	T1212: Data from I
Web Browsers	Scopping	Protocol	Renositories
T1555 001: Kovebain	T112E: Notwork Shore	T1021 002: SMR/Windows	T1212 001: Cont
T1555.001: Reycham	Discovery	Admin Sharos	T1213.001. Com
T1212: Exploitation for	T1040: Network Spiffing	T1021 004: SSU	T1005: Data from I
Cradential Access	T1201: Decoverd Deliev	T1021.004. 3311	T1005. Data from I
T1197: Forced Authontication	Discovery	T1021.005. Windows Pomoto	Shared Drive
T1606: Forgo Web Credentials	T1100 Designation	Management	T1025: Data from I
T1056: Input Conture	Discourse Discourse	T1001: Poplication Through	Modia
T1056.004: Crodontial API	T1000 Dermission Crowns	Pomovable Media	T107/: Data Stage
Hooking	11069: Permission Groups	T1072: Software Deployment	T1114: Data Staye
T1056 002: CIII Input Conture	T1000 002: Claud Crause	Tools	T1114. Lindii Colle
T1056.002: GOI Input Capture	T1069.003: Cloud Groups	T1080: Toint Shared Content	TITI4.005: Ellid
T1056.002: Web Portal	T1069.002: Domain Groups	T1550: Uso Altornato	T1114 001: Loc
Capture	T1069.001: Local Groups	Authoritication Material	Collection
T1557: Man in the Middle	T1012: Process Discovery	Authentication material	T111/ 002: Por
T1557.002: ARP Cache	T1012: Query Registry		Collection
Poisoning	Disessory		T1056: Input Canti
T1557 001: LLMNR/NRT-NS	Discovery		T1185: Man in the
Poisoning and SMR Belay	T1518: Software Discovery		T1557: Man-in-the
T1556: Modify Authentication	Disession		T1113: Scroon Con
Process	T1002 Sustan Information		T1125: Video Cant
T10/0: Network Sniffing	Disease		11125. video capt
T1003: OS Credential Dumping	T1010: Sustem Naturals		
T1003.008: /etc/nasswd and	Configuration Discovery		
/etc/shadow	T1040: System Network		
T1003 005: Cached Domain	Connections Discovery		
Credentials	T1022: System Owner/User		
T1003 006: DCSvnc	Discovery		
T1003.004: LSA Secrets	T1007: System Service		
T1003.001: LSASS Memory	Discovery		
T1003.003: NTDS	T1124: System Time Discovery		
T1003.007: Proc Filesystem	T1407: Virtualization (Sandboy		
T1003.002: Security Account	Fussion		
Manager	LVdSIOII		
T1528: Steal Application			
Access Token			
T1558: Steal or Forge Kerberos			
Tickets			
T1539: Steal Web Session			
Cookie			
T1111: Two-Factor			
Authentication Interception			
T1552: Unsecured Credentials			
T1552.003: Bash History			
T1552.001: Credentials			
In Files			
T1552.002: Credentials in			

TANNO9. Collection	TA0011: Command and Control
T1560: Archive Collected Data	T1071: Application Lawor
T1560.003: Archive via	Protocol
Custom Method	T1071 004: DNS
T1560.002: Archive via	T1071.004. DN3
Library	Protocols
T1560.001: Archive via Utility	T1071 003: Mail Protocols
T1123: Audio Capture	T1071.001: Web Protocols
T1119: Automated Collection	T1092: Communication
T1115: Clipboard Data	Through Removable Media
T1602: Data from Configuration	T1132: Data Encoding
Repository	T1132.002: Non-Standard
T1213: Data from Information	Encoding
Repositories	T1132.001: Standard
T1213.001: Confluence	Encoding
T1213.002: Sharepoint	T1001: Data Obfuscation
T1005: Data from Local System	T1001.001: Junk Data
T1039: Data from Network	T1001.003: Protocol
Shared Drive	Impersonation
T1025: Data from Removable	T1001.002: Steganography
Media	T1568: Dynamic Resolution
T1074: Data Staged	T1573: Encrypted Channel
T1114: Email Collection	T1573.002: Asymmetric
11114.003: Email Forwarding	Cryptography
Rule	11573.001: Symmetric
11114.001: Local Email	Lryptography T1000: Fallback Channels
T1114 000: Demote Emoil	T1108: Failback Channels
Collection	T1105: Ingress tool transfer
T1056, Input Conture	T104: Multi-Stage Chalinets
T1195: Man in the Browser	Protocol
T1557: Man-in-the-Middle	T1571: Non-Standard Port
T1113: Screen Canture	T1572: Protocol Tunneling
T1125: Video Canture	T1090: Proxy
	T1090.004: Domain Fronting
	T1090.002: External Proxy
	T1090.001: Internal Proxy
	T1090.003: Multi-hop Proxy
	T1219: Remote Access
	Software
	T1205: Traffic Signaling
	T1102: Web Service

TA0010: Exfiltration T1020: Automated Exfiltration T1030: Data Transfer Size Limits T1048: Exfiltration Over Alternative Protocol T1041: Exfiltration Over C2 Channel T1011: Exfiltration Over Other Network Medium T1052: Exfiltration Over Physical Medium T1567: Exfiltration Over Web Service 11567.002: Exfiltration to Cloud Storage T1567.001: Exfiltration to Code Repository T1029: Scheduled Transfer

TA0040: Impact
T1531: Account Access
Removal

- T1485: Data Destruction T1486: Data Encrypted for

- Inpact Inpact T1565: Data Manipulation T1491: Defacement T1561: Disk Wipe T1499: Endpoint Denial of

- 11499: Endpoint Denial of Service 11495: Firmware Corruption 11490: Inhibit System Recovery 11498: Network Denial of Service 11496: Resource Hijacking 11489: Service Stop 11429: System Shutdown/ Behoat

Web Application Hacking

140043: Reconnaissance I1595:002: Kaning P.Bicks, I1595:002: Kuinerzbilly Scanning I1595: Gather Victim Net Hormation 11583:002: Sorrer I1593:002: Sorrer I1593:002: Sorrer I1593:002: Sorrer I1593:002: Sorrer I1594: Comproses I1594: Comproses I1594: Comproses I1594: Comproses I1594: Observed I1594: Obser	TA0002: Execution T1059: Command and Scripting Interpreter T1059:007: JavaScript/JScript T1059:008: Network Device CLI T1059:008: Network Device CLI T1059:003: Windows Command Shell T1059:003: Windows Command Shell T1059:003: Windows Command Shell T1059:004: Unix Shell T1059:003: Windows Command Shell T1203: Exploitation for Client Execution T1559: Inter-Process Communication T1559: Old Discover Client Exchange T11069: Sold: Component Object Model T1059: Sold Clienter Exchange T11059: System Services T1059: System Service Execution T1204: User Execution T1204: User Execution T1204: Windows Management Instrumentation	TA0003: Persistence 11097: BITS Jobs 11147: BITS Jobs 11037: 005 or Logon Script (Windows) 11037: 002: Logon Script (Mac) 11037: 003: Network Logon Script 11037: 004: Re.common 11037: 005: Startup Items 1156: Compromise Client Software Binary 11136: Create Account 1136: Create Account 1137: 0016: Event Triggered Evecution Startup 1154: Scheduled Task/Job 1154: Scheduled Task/Job 1154: Pre-05 Boot 11053: Scheduled Task/Job 1154: Pre-05 Root 11505: Server Software Component 11505: ODI: SQL Stored Procedures 11505: ODI: Scheduled Task/Job 11205: Traffic Signaling 11205: Traffic Signaling 11205: OLI: Port Knocking 1107: Vaiid Accounts	TA0004: Privilege Escalation T1548.002: Bypass User Account Control T1548.002: Bypass User Account Control T1548.002: Bypass User Account Control T1548.002: Setuid and Setgid T1548.002: Setuid and Setgid T1548.002: Create Process with Token T1134.002: Create Process with Token T1134.002: Create Process with Token T134.002: Authentication Package T1547.002: Create Proceed Applications T1547.002: Respenced Applications T1547.002: Respenced Applications T1547.002: Respenced Applications T1547.002: Respenced Applications T1547.002: Windogn Helger DLL T1647.002: Windogn Helger DLL T1543.002: Windogn Helger DLL T1543.002: Apstem Providers T1543.002: Windogn Helger DLL T1543.002: Apstem Daemon T1543.002: Windogn Helger DLL T1543.002: Apstem Providers T1543.003: Windogn Helger DLL T1543.002: Apstem Provider T154	TA0005: Defense Evasion T1548: Abuse Elevation Control Mechanism T1134: Access Token Manipulation T1137: BIS Jobs T1140: Deobfuscate/Decode Files or Information T1006: Direct Volume Access T1484: Domain Policy Modification T1480: Execution Guardrals T1211: Exploitation for Defense Evasion T1221: Exploitation for Defense Evasion T1544: Hide Artifacts T15474: Hide K Execution Flow T15474: DLL Search Order Hilacking T15474: DCL PRELOAD T15474: Searces Registry Permissions T154	TA0006: Credential Access T1110:04: Credential Stuffing, T1110:02: Password Cracking, T1110:001: Password Straving, T1555: Credentials from Password Stores T1555: Credentials from Veb Browsers T1555: Ool: Keychain T1255: Colo: SecurityI Memory T1212: Exploitation for Credential Access T1606:002: SML Tokens T1606:002: SML Tokens T1056: Ool: Keylogging T1056: Ool: Keylogging T1056: Not: Keylogging T1056: Not: Keylogging T1558: Steal or Forge Kerberos Ticket T1558: Ool: Sold: AcketP Poasting T1558: Notal Veb Session Cookie T1552: Unsecured Credentials T1552: Ool: Coul Instance Metadata API T1552: Ool: Credentials In Files T1552: Ool: Credentials In Files	
---	---	--	---	---	---	--

Domain: Enterprise ATT&CK v8

Platforms: Linux[®], macOS[®], Windows[®], Office 365[®], Azure[®] AD, IaaS, SaaS, PRE, Network

006: Credential Access

T1110: Brute Force T1110.004: Credential Stuffing T1110.004: Credential Stuffing T1110.002: Password Cracking T1110.001: Password

T1040: Network Sniffing T1040: Network Sniffing T1003: 0S Credential Dumping T1528: Steal Application Access

Token T1558: Steal or Forge Kerberos

1 11598: Steal of Forge Kerberos Tickets 11558:004: AS-REP Roasting 11558:003: Golden Ticket 11558:003: Kerberoasting 11558:002: Silver Ticket 11539: Steal Web Session Cookie 11111: Two-Factor Authentication Intercention

Authentication Interception T1552: Unsecured Credentials T1552:003: Bash History T1552:005: Cloud Instance

Registry T1552.006: Group Policy

Preferences T1552.004: Private Keys

Metadata API T1552.001: Credentials In Files T1552.002: Credentials in

TA00 T1560: Arcl T1123: Aud T1119: Auto T1115: Clip T1530: Data TA0008: Lateral Movement T1210: Exploitation of Remote Services T1534: Internal Spearphishing T1570: Lateral Tool Transfer T1563: Remote Service Session
 Password
 11110.002: Password Cracking
 T1570: Lateral Tool Transfe

 Password
 Guessing
 T1570: Lateral Tool Transfe

 assword Spraying
 T1110.003: Password Spraying
 T1550: Credentials from

 s
 Password Stores
 T1655: Credentials from

 ychain
 T1555: Credentials from
 T1021.003: Distributed

 curityd Memory
 T1555: Soci: Keychain
 T1021.003: Distributed

 curityd Memory
 T1555: Soci: Securityd Memory
 T1021.003: SNM indens

 on for
 T1065: Oraced Authentication
 T1021.003: SNM indens

 Lokens
 T1056: Input Capture
 T1056:001: Web Cockies

 reT1056:001: Web Cockies
 T1021.005: Windows Remot

 mot Capture
 T1056:002: GUI Input Capture
 T1065:003: Web Portal Capture

 ential API
 T1056:002: GUI Input Capture
 T1056:002: GUI Input Capture

 ridolico
 T1555: Wodfy Authentication
 T1556: Wodfy Authentication

 rutcation
 T1556: Modify Authentication
 T1556: Wodfy Authentication

 rutcation
 T1556: Modify Authentication
 T1550: Use Alternate

 ruthentication
 T1556: Modify Authentication
 T1550: Use Alternate
 Object T1602: Data Repository T1213: Data Repositorie T1005: Data T1039: Data Admin Shares T1021.004: SSH T1021.005: VNC T1021.006: Windows Remote Shared Driv T1025: Dat
 Media

 T1074: Data

 T1174: Ema

 T1056: Inpu

 T1185: Man

 T1557: Man

 T1113: Scree

 T1125: Vide

CIS Community Defense Model v2.0

009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
hive Collected Data	T1071: Application Layer	T1020: Automated Exfiltration	T1531: Account Access Removal
dio Capture	Protocol	T1030: Data Transfer Size Limits	T1485: Data Destruction
tomated Collection	T1071.004: DNS	T1048: Exfiltration Over	T1486: Data Encrypted for
oboard Data	T1071.002: File Transfer	Alternative Protocol	Impact
ta from Cloud Storage	Protocols	T1041: Exfiltration Over C2	T1565: Data Manipulation
-	T1071.003: Mail Protocols	Channel	T1491: Defacement
ta from Configuration	T1071.001: Web Protocols	T1011: Exfiltration Over Other	T1561: Disk Wipe
-	T1092: Communication Through	Network Medium	T1499: Endpoint Denial of
a from Information	Removable Media	T1052: Exfiltration Over Physical	Service
es	T1132: Data Encoding	Medium	T1499.003: Application
a from Local System	T1001: Data Obfuscation	T1567: Exfiltration Over Web	Exhaustion Flood
a from Network	T1568: Dynamic Resolution	Service	T1499.004: Application or
ve	T1573: Encrypted Channel	T1029: Scheduled Transfer	System Exploitation
ta from Removable	T1008: Fallback Channels	T1537: Transfer Data to Cloud	T1499.001: OS Exhaustion
	T1105: Ingress Tool Transfer	Account	Flood
ta Staged	T1104: Multi-Stage Channels		T1499.002: Service Exhaustion
ail Collection	T1095: Non-Application Layer		Flood
ut Capture	Protocol		T1495: Firmware Corruption
n in the Browser	T1571: Non-Standard Port		T1490: Inhibit System Recovery
n-in-the-Middle	T1572: Protocol Tunneling		T1498: Network Denial of
een Capture	T1090: Proxy		Service
eo Capture	T1219: Remote Access Software		T1498.001: Direct Network
	T1205: Traffic Signaling		Flood
	T1102: Web Service		T1498.002: Reflection
			Amplification
			T1496: Resource Hijacking
			T1489: Service Stop
			T1529: System Shutdown/
			Deheat

Reboot

Insider and Privilege Misuse

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion	TA0006: Credential Access	TA0007: Discoverv	TA0008: Lateral Movement	
T1E0E: Active Seenning	T1E92: Acquire Infractructure	T1180, Drive by Compromise	T10E0: Command and Corinting	T1009: Account Manipulation	T1549, Abuse Elevation Control	T1E49: Abuse Elevation Control Machanism	T1110, Pruto Fores	T1097: Account Discovery	T1210 Explaitation of Domoto	T156
11595: Active Scalining	11565: Acquire initastructure	11109: Drive-by Compromise	11059: Command and Scripting	T1096: ACCOUNT Wanipulation	11546: ADUSE Elevation Control	11546: Abuse Elevation Control Mechanism	TITIO: Drute Force	11067: ACCOUNT DISCOVERY	11210: Exploitation of Remote	1130
T1592: Gather Victim Host	T1586: Compromise Accounts	T1190: Exploit Public-Facing	Interpreter	T1197: BITS Jobs	Mechanism	T1134: Access Token Manipulation	T1110.004: Credential Stuffing	T1087.004: Cloud Account	Services	1
Information	T1584: Compromise	Application	T1059.002: AppleScript	T1547: Boot or Logon Autostart	T1134: Access Token	T1197: BITS Jobs	T1110.002: Password Cracking	T1087.002: Domain Account	T1534: Internal Spearphishing	M
T1592 004: Client	Infrastructure	T1133: External Remote	T1059 007: JavaScript/IScript	Execution	Maninulation	T11/0: Deobfuscate/Decode Files or Information	T1110 001: Password	T1087.003: Email Account	T1570: Lateral Tool Transfer	T1
Castinuations	T1507: Develop Conshilition	Camilana	T1050.000; Network Device CI	T1007. Deet en Lenen	T1C47: Deet en Lesen Autostent	T100C: Direct Volume Access	Cuessian	T1007.001. Level Assessment	T1070: Euteral foor mansier	- T1
coningurations	11587: Develop Capabilities	Services	11059.008: Network Device CLI	11037: Boot of Logon	11547: Boot of Logon Autostart	11006: Direct volume Access	Guessing	T1087.001: Local Account	11563: Remote Service Session	11
T1592.003: Firmware	T1587.002: Code Signing	T1200: Hardware Additions	T1059.001: PowerShell	Initialization Scripts	Execution	T1484: Domain Policy Modification	T1110.003: Password Spraying	T1010: Application Window	Hijacking	T112
T1592.001: Hardware	Certificates	T1566: Phishina	T1059.006: Pvthon	T1176: Browser Extensions	T1037: Boot or Logon	T1484.002: Domain Trust Modification	T1555: Credentials from	Discoverv	T1021: Remote Services	T111
T1592 002: Software	T1587 003: Digital Certificates	T1091: Replication Through	T1059 004: Univ Shell	T1554: Compromise Client	Initialization Scrints	T1/8/ 001: Group Policy Modification	Password Stores	T1217: Browser Bookmark	T1021 003: Distributed	T111
T1532.002. Soltware	T1507.003. Digital Certificates	Demovable Media	T1050.005 Viewel Desis	Cofficiente Dimenti	T1542, Create as Madify Custom	T1400, Evenution Cuardunile	T1CCC 000: Credentials from	Discourse Diowser Dookinark	Component Object Model	T100
11589: Gather Victim Identity	11587.004: Exploits	Removable Media	11059.005: VISUAI BASIC	Software Binary	11543: Create or Modify System	11480: Execution Guardralis	11555.003: Credentials from	Discovery	Component Ubject Model	1153
Information	T1587.001: Malware	T1195: Supply Chain	T1059.003: Windows	T1136: Create Account	Process	T1211: Exploitation for Defense Evasion	Web Browsers	T1580: Cloud Infrastructure	T1021.001: Remote Desktop	Objec
T1589.001: Credentials	T1585: Establish Accounts	Compromise	Command Shell	T1543: Create or Modify System	T1543.001: Launch Agent	T1222: File and Directory Permissions Modification	T1555.001: Keychain	Discovery	Protocol	T160
T1590.002; Email Addrossos	T1599: Obtain Canabilities	T1105 002: Compromise	T1202: Exploitation for Client	Process	T1542 004: Lounch Doomon	T1564: Hide Artifacte	T1555 002: Securityd Momony	T1529: Cloud Service Dechboard	T1021 002: SMR /Windows	Dono
T1505.002. Lindii Adulesses	T1500.000 0. d. Olania	11155.005. Compromise		TICLOSS	T1545.004. Launch Daemon	T1504.005 Ulides File Orsten	T1000 Full in the weiling	T1530. Cloud Service Dashboard	11021.002. SWD/ WIII00WS	TIOL
11589.003: Employee Names	_ 11588.003: Code Signing	Hardware Supply Chain	Execution	11546: Event Triggered	11543.002: Systemd Service	11564.005: Hidden File System	11212: Exploitation for	11526: Cloud Service Discovery	Admin Shares	1121
T1590: Gather Victim Network	Certificates	T1195.001: Compromise	T1559: Inter-Process	Execution	T1543.003: Windows Service	T1564.001: Hidden Files and Directories	Credential Access	T1482: Domain Trust Discovery	T1021.004: SSH	Repo
Information	T1588.004: Digital Certificates	Software Dependencies and	Communication	T1133: External Remote	T1484: Domain Policy	T1564.002: Hidden Users	T1187: Forced Authentication	T1083: File and Directory	T1021.005; VNC	T1
T1E01, Cothor Victim Ora	T1E99.00Er Evploite	Dovelopment Toolo	T1106: Notive ADI	Convision	Medification	T1564.002; Hidden Window	T1606: Forgo Web Credentiele	Discovery	T1021 006: Windows Domoto	T1
11591: Gather Vicuin Org	11500.005; EXPIDITS	Development loois	TITUD: Native APT	Services	woullication	T1004.003: HIUdell WIIIdow	11000: Forge web credeniliais	Discovery	TTUZT.000: WITUOWS RETIDLE	
Information	11588.001: Malware	11195.002: Compromise	11053: Scheduled lask/Job	115/4: Hijack Execution Flow	11546: Event Iriggered	11564.004: NTFS File Attributes	11056: Input Capture	11046: Network Service	Management	1100
T1591.002: Business	T1588.002: Tool	Software Supply Chain	T1129: Shared Modules	T1525: Implant Container Image	Execution	T1564.006: Run Virtual Instance	T1056.004: Credential API	Scanning	T1091: Replication Through	T103
Relationshins	T1588 006: Vulnerabilities	T1199 Trusted Relationshin	T1072: Software Deployment	T1137: Office Application	T1068: Exploitation for Privilege	T1564 007: VBA Stomping	Hooking	T1135: Network Share Discovery	Removable Media	Share
T1501.001: Determine Dhusies	11000.000. Vulliciubilitico	T1070. Valid Assounts	Taola	Chantum	Freeletion	T1574. Illical: Execution Flow	T105C 000: CIII Jacut Conture	T1040. Network Criffing	T1070: Cofficiente Depleument	T100
11591.001: Determine Physical		11078: Valid Accounts	10015	Startup	Escalation	11574: Hijack Execution Flow	11056.002: GOI Input Capture	11040: Network Snining	11072: Software Deployment	1102
Locations		T1078.004: Cloud Accounts	T1569: System Services	T1542: Pre-OS Boot	T1574: Hijack Execution Flow	T1562: Impair Defenses	T1056.001: Keylogging	T1201: Password Policy	Tools	Medi
T1591.003: Identify Business		T1078.001: Default Accounts	T1204: User Execution	T1053: Scheduled Task/Job	T1574.012: COB PROFILER	T1562.008: Disable Cloud Logs	T1056.003: Web Portal Capture	Discovery	T1080: Taint Shared Content	T107
Tempo		T1078 002: Domain Accounts	T1204 002: Malicious File	T1505: Server Software	T1574001: DLL Search Order	T1562 007: Disable or Modify Cloud Firewall	T1557: Man-in-the-Middle	T1120: Perinheral Device	T1550: Use Alternate	T1
T1C01.004. Identify Dalas	-	T1070.002. Domain Accounts	T1204.001. Malicious Link	Component	lie elie e	T1502.004. Disable of Modify Global Ticwall	T1557. Madifu Authentication	Discourse	Authentication Meterial	T 1
11591.004: Identity Roles	-	11078.003: Local Accounts	11204.001: Malicious Link	component	HIJACKING	11562.004: Disable or Modity System Firewall	11556: Modify Authentication	Discovery	Authentication Material	_ 11
T1598: Phishing for Information			T1047: Windows Management	T1205: Traffic Signaling	T1574.002: DLL Side-Loading	T1562.001: Disable or Modify Tools	Process	T1069: Permission Groups		St
T1597: Search Closed Sources			Instrumentation	T1078: Valid Accounts	T1574.004: Dylib Hijacking	T1562.002: Disable Windows Event Logging	T1040: Network Sniffing	Discovery		T111
T1506: Soarch Open Technical	-				T1574.005; Executable	T1562.002: Impair Command History Logging	T1002: 05 Crodential Dumping	T1060.002: Cloud Groups		T1
Detals and a search open reclinical					11074.000. EXecutable	T1502.000, Initiali Command History Edgging	T1003. 03 Credential Dumping	T1005.005. Cloud droups		
Databases	_				Installer File Permissions	11562.006: Indicator Blocking	11003.008: /etc/passwd and /	T1069.002: Domain Groups		RL
T1593: Search Open Websites/					Weakness	T1070: Indicator Removal on Host	etc/shadow	T1069.001: Local Groups		T1
Domains					T1574.006 I.D. PRELOAD	T1070 003: Clear Command History	T1003 005: Cached Domain	T1057: Process Discovery		Co
T1504: Soarch Victim Ownod	-				T1574.007: Path Interception	T1070.002: Cloar Linux or Mac System Logs	Credentials	T1012: Quory Pogistry		T1
11554. Search victim-Owned						T1070.002. Clear Linux or Mac System Logs	TI 000 000 DO0	T1012. Query negistry		11
wedsites	_				by PATH Environment variable	11070.001: Clear Windows Event Logs	11003.006: DCSync	11018: Remote System		- U
					T1574.008: Path Interception	T1070.004: File Deletion	T1003.004: LSA Secrets	Discovery		T105
					by Search Order Hijacking	T1070 005: Network Share Connection Removal	T1003 001: LSASS Memory	T1518: Software Discovery		T118
					T1574.000. Dath Intercention	T1070.000. Timestema	T1003.001. LONGO MCHIOLY	T1510.001. Convitu Coffman		T100
					11574.009: Path Interception	11070.006: Timestomp		11518.001: Security Software		1100
					by Unquoted Path	T1202: Indirect Command Execution	T1003.007: Proc Filesystem	Discovery		T111
					T1574.010: Services File	T1036: Masquerading	T1003.002: Security Account	T1082: System Information		T112
					Permissions Weakness	T1036 001: Invalid Code Signature	Manager	Discovery		
					T1574.011 0	T1000.001. Invalid Code Signature	TIFOO Ot al Analiantian Associa	TIOLO Outer Natural		
					11574.011: Services Registry	11036.004: Masquerade lask or Service	11528: Steal Application Access	11016: System Network		
					Permissions Weakness	T1036.005: Match Legitimate Name or Location	Token	Configuration Discovery		
					T1055: Process Injection	T1036.003: Bename System Utilities	T1558: Steal or Forge Kerberos	T1049: System Network		
					T1053: Scheduled Task/Job	T1036 002: Bight-to-Left Override	Tickets	Connections Discovery		
					T1033. Scheduled Hask/Job	T1000.002. high-to-ten overhoe	T1520, Cheel Web Cassier	T1022: Custom Ourses (lleas		
					11078: Valid Accounts	11036.006: Space alter Fliename	11539: Stear web Session	11033: System Owner/User		
						T1556: Modify Authentication Process	Cookie	Discovery		
						T1578: Modify Cloud Compute Infrastructure	T1111: Two-Factor	T1007: System Service		
						T1578 002: Create Cloud Instance	Authentication Interception	Discovery		
						T1570.001, Greate Chonshot	T1EE2: Upgagered Credentials	T1124: Sustan Time Discourse		
						1157 6.001: Create Shapshot	11552: Unsecured credentials	11124: System Time Discovery		
						11578.003: Delete Cloud Instance	11552.003: Bash History	11497: Virtualization/Sandbox		
						T1578.004: Revert Cloud Instance	T1552.005: Cloud Instance	Evasion		
						T1112: Modify Registry	Metadata API			
						T1601: Modify System Imago	T1552 001: Crodentiale In Files			
						T1500 Notes de Dela de Dela de	T1552.001: Credentials In Files			
						11599: Network Boundary Bridging	11552.002: Credentials in			
						T1027: Obfuscated Files or Information	Registry			
						T1542: Pre-OS Boot	T1552.006: Group Policy			
						T1055: Process Injection	Proforancos			
							TICICICIUCS			
						11207: Rogue Domain Controller	11552.004: Private Keys			
						T1014: Rootkit				
						T1218: Signed Binary Proxy Execution				
						T1216: Signed Script Provy Execution				
						TIERO, Orginou Jonipi i Toxy Excoulton				
						11555: SUDVERT ITUST CONTROLS				
						11221: Iemplate Injection				
						T1205: Traffic Signaling				
						T1127: Trusted Developer Utilities Provy Execution				
						T1525: Unused /Ungunported Cloud Degione				
						11555: Unused/Unsupported Cloud Regions				
						11550: Use Alternate Authentication Material				
						T1078: Valid Accounts				
						T1497: Virtualization/Sandhox Evasion				
						T1600: Wookon Encryption				
						T1000, Weaker Elici yption				
						11220: XSL Script Processing				

Domain: Enterprise ATT&CK v8

Platforms: Linux*, macOS*, Windows*, Office 365*, Azure* AD, AWS*, GCP*, Azure*, SaaS, PRE, Network

thou source with the second se

2: Data from Configuration

sitory 3: Data from Information

IS: Data from montation sistories 1213.001: Confluence 1213.002: Sharepoint 15: Data from Local System 19: Data from Network ad Deire ed Drive 5: Data from Removable

4: Data Staged 1074.001: Local Data Staging 1074.002: Remote Data

taging **4: Email Collection** 1114.003: Email Forwarding

L114.001: Local Email llection 114.002: Remote Email

ollection 6: Input Capture 5: Man in the Browser 7: Man-in-the-Middle 3: Screen Capture 5: Video Capture

TA0009: Collection Carchive Collected Data 560.003: Archive via Custom Thomas Achive Via Cust Protocol T1092: Communication Thr 11092: Communication Thro Removable Media 11132: Data Encoding 11001: Data Obfuscation 11568: Dynamic Resolution 115673: Encrypted Channels 11008: Fallback Channels 11105: Ingress Tool Transfer 11104: Multi-Stage Channels 11095: Non-Application Laye Protocol 11095: Non-Application Laye Protocol 11571: Non-Standard Port 11572: Protocol Tunneling 11090: Proxy 11219: Remote Access Softw 11205: Traffic Signaling 11102: Web Service

ntrol	TA0010: Exfiltration
	T1020: Automated Exfiltration
	T1030: Data Transfer Size Limits
ough	T1048: Exfiltration Over
Ŭ	Alternative Protocol
	T1041: Exfiltration Over C2
	Channel
	T1011: Exfiltration Over Other
	Network Medium
	T1011.001: Exfiltration Over
r	Bluetooth
ls	T1052: Exfiltration Over Physical
er	Medium
	T1052.001: Exfiltration
	over USB
	T1567: Exfiltration Over Web
	Service
ware	T1567.002: Exfiltration to
	Cloud Storage
	T1567 001 · Exfiltration to Code

Repository T1029: Scheduled Transfer T1537: Transfer Data to Cloud ccount

TA0040: Impact tion T1531: Account Access Removal Limits T1485: Data Destruction T1486: Data Encrypted for Immact

- Impact T1565: Data Manipulation T1565:003: Runtime Data Manipulation T1565.001: Stored Data

- T1565.001: Stored Data Manipulation T1565.002: Transmitted Data Manipulation T1491: Defacement T1561.001: Disk Content Wipe T1561.002: Disk Structure Wine
- Wipe T1499: Endpoint Denial of
- 11499: Endpoint Denial of Service 11495: Firmware Corruption 11490: Inhibit System Recovery 11498: Network Denial of Service 11496: Resource Hijacking 11498: Service Stop 11529: System Shutdown/ Reboot

- Reboot

Targeted Intrusions

Domain: Enternrise ATT&CK v8

Platforms: Linux® macOS® Windows® Office 365® Azure® AD JaaS SaaS PRF Network

iui gotou ii				Domain: Enterprise Al	TACK VO	Fiduorins: Linux , ind		00 , AZUTE AD, 1885, 5885,	, FRE, NELWOIK				
TA0042: Deconnoisconco	TA0042: Becourse Development	TADOO1, Initial Access	TA0002: Execution	TA0002: Devoietoneo	TAGOOA: Drivilago Eccelation	TADADE: Defense Evenion	TADDOG: Cradential Access		TADDOR: Lateral Movement	TAGOOD: Collection	TAGG11: Command and Control	TA0010, Exfiltration	TA0040, Impact
T1595: Active Scanning	T1583: Acquire Infrastructure	T1189: Drive-by Compromise	T1059: Command and Scripting	T1098: Account Manipulation	T1548: Abuse Elevation Control	T1548: Abuse Elevation Control Mechanism	TAUUUS: Credential Access	T1087: Account Discovery	T1210: Exploitation of Remote	T1560: Archive Collected Data	TAUGEL: Command and Control	T1020: Automated Exfiltration	T1531: Account Access Removal
T1592: Gather Victim Host	T1586: Compromise Accounts	T1190: Exploit Public-Facing	Interpreter	T1098.003: Add Office 365	Mechanism	T1548.002: Bypass User Account Control	T1110.004: Credential Stuffing	T1087.004: Cloud Account	Services	T1560.003: Archive via Custom	Protocol	T1030: Data Transfer Size Limits	T1485: Data Destruction
Information T1589: Gather Victim Identity	T1584: Compromise	Application T1133: External Remote	T1059.002: AppleScript	Global Administrator Role	T1134: Access Token Manipulation	T1548.004: Elevated Execution with Prompt	T1110.002: Password Cracking T1110.001: Password	T1087.002: Domain Account	T1534: Internal Spearphishing	Method T1560.002: Archive via Library	T1071.004: DNS T1071.002: File Transfer	T1048: Exfiltration Over	T1486: Data Encrypted for
Information	T1587: Develop Capabilities	Services	T1059.008: Network Device CLI	Credentials	T1134.002: Create Process	T1548.003: Sudo and Sudo Caching	Guessing	T1087.001: Local Account	T1563: Remote Service Session	T1560.001: Archive via Utility	Protocols	T1041: Exfiltration Over C2	T1565: Data Manipulation
T1590: Gather Victim Network	T1587.002: Code Signing	T1200: Hardware Additions	T1059.001: PowerShell	T1098.002: Exchange Email	with Token	T1134: Access Token Manipulation	T1110.003: Password Spraying	T1010: Application Window	Hijacking	T1123: Audio Capture	T1071.003: Mail Protocols	Channel T1011: Evfiltration Over Other	T1565.003: Runtime Data
T1591: Gather Victim Org	T1587.003: Digital Certificates	T1566.001: Spearphishing	T1059.004: Unix Shell	T1098.004: SSH Authorized	Impersonate Token	T1140: Deobfuscate/Decode Files or Information	Password Stores	T1217: Browser Bookmark	T1021.003: Distributed	T1115: Clipboard Data	T1092: Communication Through	Network Medium	T1565.001: Stored Data
Information	T1587.004: Exploits	Attachment	T1059.005: Visual Basic	Keys	T1134.004: Parent PID	T1006: Direct Volume Access	T1555.003: Credentials from	Discovery	Component Object Model	T1602: Data from Configuration	Removable Media	T1052: Exfiltration Over Physical	Manipulation
Relationships	T1587.001: Malware	T1566.002: Spearphishing Link	Command Shell	T1547: Boot or Logon Autostart	T1134.005: SID-History	T1480: Execution Guardrails	T1555.001: Kevchain	T1538: Cloud Service Dashboard	Protocol	T1213: Data from Information	T1132: Data Encoding T1132.002: Non-Standard	T1567: Exfiltration Over Web	Manipulation
T1591.001: Determine Physical	T1588: Obtain Capabilities	via Service	T1203: Exploitation for Client	Execution	Injection	T1211: Exploitation for Defense Evasion	T1555.002: Securityd Memory	T1482: Domain Trust Discovery	T1021.002: SMB/Windows	Repositories	Encoding	Service	T1491: Defacement
T1591.003: Identify Business	Certificates	Removable Media	T1559: Inter-Process	Initialization Scripts	III34.001: loken	T1222: File and Directory Permissions Modification T1222.002: Linux and Mac File and Directory Permissions	Credential Access	Discovery	Admin Snares T1021.004: SSH	T1005: Data from Local System T1039: Data from Network	T1001: Data Obfuscation	11029: Scheduled Transfer	T1499: Endpoint Denial of
Tempo	T1588.004: Digital Certificates	T1195: Supply Chain	Communication	T1176: Browser Extensions	T1547: Boot or Logon Autostart	Modification	T1187: Forced Authentication	T1046: Network Service	T1021.005: VNC	Shared Drive	T1001.001: Junk Data		Service
T1591.004: Identity Roles	T1588.005: Exploits T1588.001: Malware	T1195.003: Compromise	T1053: Scheduled Task/Job	Software Binary	T1547.002: Authentication	T1222.001: Windows File and Directory Permissions Modification T1564: Hide Artifacts	T1606.002: SAML Tokens	T1135: Network Share Discovery	Management	Media	Indersonation		T1495: Firmware corruption T1490: Inhibit System Recovery
T1597: Search Closed Sources	T1588.002: Tool	Hardware Supply Chain	T1129: Shared Modules	T1136: Create Account	Package	T1564.005: Hidden File System	T1606.001: Web Cookies	T1040: Network Sniffing	T1091: Replication Through	T1074: Data Staged	T1001.002: Steganography		T1498: Network Denial of
Databases	11588.006: Vuineradilities	Software Dependencies and	Tools	T1136.003: Cloud Account T1136.002: Domain Account	and Extensions	T1564.002: Hidden Users	T1056: Input Capture T1056.004: Credential API	Discovery	T1072: Software Deployment	T1074.001: Local Data Staging T1074.002: Remote Data	T1568: Dynamic Resolution T1568.003: DNS Calculation		Service T1496: Resource Hijacking
T1593: Search Open Websites/		Development Tools	T1569: System Services	T1136.001: Local Account	T1547.008: LSASS Driver	T1564.003: Hidden Window	Hooking	T1120: Peripheral Device	Tools	Staging	T1568.002: Domain Generation		T1489: Service Stop
T1594: Search Victim-Owned		Software Supply Chain	T1569.001: Launchett T1569.002: Service Execution	Process	T1547.011: Plist Modification T1547.010: Port Monitors	T1564.006: Run Virtual Instance	T1056.002: GUI Input Capture	T1069: Permission Groups	T1550: Use Alternate	T1114: Email Collection T1114.003: Email Forwarding	T1568.001: Fast Flux DNS		Reboot
Websites		T1199: Trusted Relationship	T1204: User Execution	T1546: Event Triggered	T1547.012: Print Processors	T1564.007: VBA Stomping	T1056.003: Web Portal Capture	Discovery	Authentication Material	Rule	T1573: Encrypted Channel		
		T1078: Valid Accounts T1078.004: Cloud Accounts	T1204.002: Malicious File	T1546.004: .bash profile and	Applications	T1574: HIJACK EXECUTION FIOW T1574.012: COR PROFILER	T1557: Man-In-the-Middle	T1069.003: Cloud Groups T1069.002: Domain Groups		Collection	Cryptography		
		T1078.001: Default Accounts	T1047: Windows Management	.bashrc	T1547.001: Registry Run Keys	T1574.001: DLL Search Order Hijacking	Process	T1069.001: Local Groups		T1114.002: Remote Email	T1573.001: Symmetric		
		T1078.002: Domain Accounts	Instrumentation	Features	7 Startup Folder T1547.005: Security Support	T1574.002: DLL Side-Loading T1574.004: Dvlib Hijacking	T1040: Network Sniming T1003: OS Credential Dumping	T1057: Process Discovery T1012: Query Registry		T1056: Input Capture	T1008: Fallback Channels		
			-	T1546.009: AppCert DLLs	Provider	T1574.005: Executable Installer File Permissions Weakness	T1003.008: /etc/passwd and /	T1018: Remote System		T1185: Man in the Browser	T1105: Ingress Tool Transfer		
				T1546.010: Applnit DLLs T1546.011: Application	11547.009: Shortcut Modification	T1574.006: LD_PRELOAD T1574.007: Path Interception by PATH Environment Variable	tc/shadow T1003.005: Cached Domain	Discovery T1518: Software Discovery		T1113: Screen Capture	11104: Multi-Stage Channels T1095: Non-Application Laver		
				Shimming	T1547.003: Time Providers	T1574.008: Path Interception by Search Order Hijacking	Credentials	T1518.001: Security Software		T1125: Video Capture	Protocol		
				11546.001: Change Detault File Association	i 1547.004: Winlogon Helper DLL	11574.009: Path Interception by Unquoted Path T1574.010: Services File Permissions Weakness	T1003.006: DCSync T1003.004: LSA Secrets	T1082: System Information			T15/1: Non-Standard Port T1572: Protocol Tunneling		
				T1546.015: Component Object	T1037: Boot or Logon	T1574.011: Services Registry Permissions Weakness	T1003.001: LSASS Memory	Discovery			T1090: Proxy		
				Model Hijacking T1546.014: Emond	Initialization Scripts T1543: Create or Modify System	T1562.004: Disable or Modify System Firewall	11003.003: NTDS T1003.007: Proc Filesystem	Configuration Discovery			11090.004: Domain Fronting T1090.002: External Proxy		
				T1546.012: Image File	Process	T1562.001: Disable or Modify Tools	T1003.002: Security Account	T1049: System Network			T1090.001: Internal Proxy		
				Execution Options Injection T1546.006: LC_LOAD_DYLIB	T1543.001: Launch Agent T1543.004: Launch Daemon	T1562.002: Disable Windows Event Logging T1562.003: Impair Command History Logging	Manager T1528: Steal Application Access	Connections Discovery T1033: System Owner/User			T1219: Remote Access Software		
				Addition	T1543.002: Systemd Service	T1562.006: Indicator Blocking	Token	Discovery			T1205: Traffic Signaling		
				T1546.007: Netsn Helper DLL T1546.013: PowerShell Profile	T1484: Domain Policy	T1070: Indicator Removal on Host T1070.003: Clear Command History	Tickets	Discovery			11102: Web Service		
				T1546.002: Screensaver	Modification	T1070.002: Clear Linux or Mac System Logs	T1558.004: AS-REP Roasting	T1124: System Time Discovery					
				T1546.005: Irap T1546.003: Windows	Modification	T1070.001: Clear Windows Event Logs T1070.004: File Deletion	T1558.001: Golden Ticket T1558.003: Kerberoasting	Evasion					
				Management Instrumentation	T1484.001: Group Policy	T1070.005: Network Share Connection Removal	T1558.002: Silver Ticket						
				T1133: External Remote	T1546: Event Triggered	T1202: Indirect Command Execution	Cookie						
				Services	Execution	T1036: Masquerading	T1111: Two-Factor						
				T1137: Office Application	Escalation	T1036.004: Masquerade Task or Service	T1552: Unsecured Credentials						
				Startup	T1574: Hijack Execution Flow	T1036.005: Match Legitimate Name or Location	T1552.003: Bash History						
				T1053: Scheduled Task/Job	T1055.004: Asynchronous	T1036.002: Right-to-Left Override	T1552.001: Credentials in Files						
				T1505: Server Software	Procedure Call	T1036.006: Space after Filename	Registry						
				T1505.001: SQL Stored	Library Injection	T1112: Modify Registry	Preferences						
				Procedures	T1055.011: Extra Window	T1601: Modify System Image	T1552.004: Private Keys						
				T1505.002: Web Shell	T1055.002: Portable	T1027: Obfuscated Files or Information							
				T1205: Traffic Signaling	Executable Injection T1055.009: Proc Memory	T1027.001: Binary Padding T1027.004: Compile After Delivery							
					T1055.013: Process	T1027.005: Indicator Removal from Tools							
					Doppelgänging T1055.012: Process Hollowing	T1027.002: Software Packing T1027.003: Steganography							
					T1055.008: Ptrace System	T1522: Pre-OS Boot							
					Calls T1055.003: Thread Execution	11055: Process Injection T1207: Roque Domain Controller							
					Hijacking	T1014: Rootkit							
					11055.005: Thread Local Storage	T1218: Signed Binary Proxy Execution T1218.003: CMSTP							
					T1055.014: VDSO Hijacking	T1218.001: Compiled HTML File							
					T1053: Scheduled Task/Job T1053.001: At (Linux)	T1218.002: Control Panel T1218.004: InstallUtil							
					T1053.002: At (Windows)	T1218.005: Mshta							
					11053.003: Cron T1053.004: Launchd	11218.007: Msiexec T1218.008: Odbcconf							
					T1053.005: Scheduled Task	T1218.009: Regsvcs/Regasm							
					T1053.006: Systemd Timers T1078: Valid Accounts	11218.010: Kegsvr32 T1218.011: Rundll32							
						T1218.012: Verclsid							
						11216: Signed Script Proxy Execution T1553: Subvert Trust Controls							
						T1553.002: Code Signing							
						11553.001: Gatekeeper Bypass T1553.004: Install Root Certificate							
						T1553.003: SIP and Trust Provider Hijacking							
						11221: Iemplate Injection T1205: Traffic Signaling							
						T1127: Trusted Developer Utilities Proxy Execution							
						T1550.001: Application Access Token							
						T1550.002: Pass the Hash							
						T1550.004: Web Session Cookie							
						T1078: Valid Accounts							
						T1497: VII (Ualization/Sanubox Evasion T1497.001: System Checks							
						T1497.003: Time Based Evasion							
						T1600: Weaken Encryption							
						T1220: XSL Script Processing							

APPENDIX H Unmapped ATT&CK (Sub-)Techniques to CIS Safeguards Within an Attack Pattern

The following are ATT&CK (sub-)techniques that were used within an attack pattern, and assigned to an ATT&CK mitigation, but could not be defended against by a CIS Safeguard in the master mapping.

ATTACK TYPE	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	ATTACK TYPE	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME
Malware	T1583	Acquire Infrastructure	Ransomware	T1592	Gather Victim Host Information
Malware	T1583.005	Botnet	Ransomware	T1592.004	Client Configurations
Malware	T1584	Compromise Infrastructure	Web App Hacking	T1583.006	Web Services
Malware	T1584.001	Domains	Web App Hacking	T1584.006	Web Services
Malware	T1586.002	Email Accounts	Web App Hacking	T1596.005	Scan Databases
Malware	T1587	Develop Capabilities	Insider and Privilege Misuse	T1587.001	Malware
Malware	T1587.003	Digital Certificates	Insider and Privilege Misuse	T1588.001	Malware
Malware	T1588.004	Digital Certificates	Insider and Privilege Misuse	T1589	Gather Victim Identity Informa
Malware	T1592	Gather Victim Host Information	Insider and Privilege Misuse	T1589.001	Credentials
Malware	T1592.002	Software	Insider and Privilege Misuse	T1591	Gather Victim Org Information
Ransomware	T1480	Execution Guardrails	Insider and Privilege Misuse	T1591.002	Business Relationships
Ransomware	T1583	Acquire Infrastructure	Insider and Privilege Misuse	T1592	Gather Victim Host Informatio
Ransomware	T1583.005	Botnet	Insider and Privilege Misuse	T1592.001	Hardware
Ransomware	T1584	Compromise Infrastructure	Insider and Privilege Misuse	T1592.002	Software
Ransomware	T1585	Establish Accounts	Insider and Privilege Misuse	T1592.003	Firmware
Ransomware	T1587.001	Malware	Insider and Privilege Misuse	T1592.004	Client Configurations
Ransomware	T1587.002	Code Signing Certificates	Targeted Intrusions	T1480	Execution Guardrails
Ransomware	T1588.001	Malware	Targeted Intrusions	T1587	Develop Capabilities
Ransomware	T1588.002	Tool	Targeted Intrusions	T1587.001	Malware
Ransomware	T1588.003	Code Signing Certificates	Targeted Intrusions	T1588	Obtain Capabilities
Ransomware	T1588.004	Digital Certificates	Targeted Intrusions	T1588.001	Malware
Ransomware	T1588.005	Exploits	Targeted Intrusions	T1591	Gather Victim Org Information
Ransomware	T1589.001	Credentials	Targeted Intrusions	T1591.001	Determine Physical Locations
Ransomware	T1589.003	Employee Names	Targeted Intrusions	T1592	Gather Victim Host Informatio

ATT&CK (Sub-)Techniques With No ATT&CK Mitigation Mapped Within an Attack Pattern

The following are ATT&CK (sub-)techniques that had no assignment to an ATT&CK mitigation (and therefore, were not mapped to a CIS Safeguard); however, they were used within an attack pattern.

ATTACK TYPE	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME	ATTACK TYPE	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE NAME
Malware	T1005	Data from Local System	Malware	T1564	Hide Artifacts
Malware	T1007	System Service Discovery	Malware	T1564.001	Hidden Files and Directories
Malware	T1012	Query Registry	Malware	T1568.001	Fast Flux DNS
Malware	T1016	System Network Config. Discovery	Ransomware	T1005	Data from Local System
Malware	T1018	Remote System Discovery	Ransomware	T1007	System Service Discovery
Malware	T1027.001	Binary Padding	Ransomware	T1012	Query Registry
Malware	T1027.003	Steganography	Ransomware	T1016	System Network Config. Discovery
Malware	T1027.004	Compile After Delivery	Ransomware	T1018	Remote System Discovery
Malware	T1027.005	Indicator Removal from Tools	Ransomware	T1020	Automated Exfiltration
Malware	T1033	System Owner/User Discovery	Ransomware	T1027.001	Binary Padding
Malware	T1036.004	Masquerade Task or Service	Ransomware	T1027.003	Steganography
Malware	T1039	Data from Network Shared Drive	Ransomware	T1027.004	Compile After Delivery
Malware	T1049	System Network Conn. Discovery	Ransomware	T1027.005	Indicator Removal from Tools
Malware	T1056	Input Capture	Ransomware	T1036.002	Right-to-Left Override
Malware	T1056.001	Keylogging	Ransomware	T1036.004	Masquerade Task or Service
Malware	T1056.004	Credential API Hooking	Ransomware	T1039	Data from Network Shared Drive
Malware	T1057	Process Discovery	Ransomware	T1049	System Network Conn. Discovery
Malware	T1069	Permission Groups Discovery	Ransomware	T1056	Input Capture
Malware	T1069.001	Local Groups	Ransomware	T1056.001	Keylogging
Malware	T1069.002	Domain Groups	Ransomware	T1057	Process Discovery
Malware	T1070.004	File Deletion	Ransomware	T1069.002	Domain Groups
Malware	T1070.005	Network Share Conn. Removal	Ransomware	T1070.004	File Deletion
Malware	T1074	Data Staged	Ransomware	T1082	System Information Discovery
Malware	T1074.001	Local Data Staging	Ransomware	T1083	File and Directory Discovery
Malware	T1082	System Information Discovery	Ransomware	T1113	Screen Capture
Malware	T1083	File and Directory Discovery	Ransomware	T1120	Peripheral Device Discovery
Malware	T1087.003	Email Account	Ransomware	T1123	Audio Capture
Malware	T1113	Screen Capture	Ransomware	T1124	System Time Discovery
Malware	T1115	Clipboard Data	Ransomware	T1134.004	Parent PID Spoofing
Malware	T1124	System Time Discovery	Ransomware	T1140	Deobfuscate/Decode Files or Info.
Malware	T1125	Video Capture	Ransomware	T1202	Indirect Command Execution
Malware	T1140	Deobfuscate/Decode Files or Info.	Ransomware	T1497	Virtualization/Sandbox Evasion
Malware	T1202	Indirect Command Execution	Ransomware	T1497.001	System Checks
Malware	T1496	Resource Hijacking	Ransomware	T1497.002	User Activity Based Checks
Malware	T1497	Virtualization/Sandbox Evasion	Ransomware	T1497.003	Time Based Evasion
Malware	T1505.003	Web Shell	Ransomware	T1518	Software Discovery
Malware	T1518	Software Discovery	Ransomware	T1518.001	Security Software Discovery
Malware	T1518.001	Security Software Discovery	Ransomware	T1529	System Shutdown/Reboot
Malware	T1529	System Shutdown/Reboot	Ransomware	T1534	Internal Spearphishing
Malware	T1531	Account Access Removal	Ransomware	T1546.015	Comp. Object Model Hijacking
Malware	T1546	Event Triggered Execution	Ransomware	T1547	Boot or Logon Autostart Exec.
Malware	T1547	Boot or Logon Autostart Exec.	Ransomware	T1547.001	Registry Run Keys/Startup Folder
Malware	T1547.001	Registry Run Keys/Startup Folder	Ransomware	T1553.002	Code Signing
Malware	T1553.002	Code Signing	Ransomware	T1555.002	Securityd Memory

ATTACK TYPE	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE Name	ATTACK TYPE	ATT&CK (SUB-) Technique ID	ATT&CK (SUB-)TECHNIQUE Name
Ransomware	T1560.002	Archive via Library	Insider and Privilege Misuse	T1115	Clipboard Data
Ransomware	T1560.003	Archive via Custom Method	Insider and Privilege Misuse	T1120	Peripheral Device Discovery
Ransomware	T1564.001	Hidden Files and Directories	Insider and Privilege Misuse	T1123	Audio Capture
Ransomware	T1600	Weaken Encryption	Insider and Privilege Misuse	T1125	Video Capture
Ransomware	T1600.002	Disable Crypto Hardware	Insider and Privilege Misuse	T1518	Software Discovery
Web App Hacking	T1007	System Service Discovery	Insider and Privilege Misuse	T1518.001	Security Software Discovery
Web App Hacking	T1016	System Network Config. Discovery	Insider and Privilege Misuse	T1560.002	Archive via Library
Web App Hacking	T1018	Remote System Discovery	Insider and Privilege Misuse	T1560.003	Archive via Custom Method
Web App Hacking	T1033	System Owner/User Discovery	Insider and Privilege Misuse	T1564	Hide Artifacts
Web App Hacking	T1036.006	Space after Filename	Insider and Privilege Misuse	T1564.001	Hidden Files and Directories
Web App Hacking	T1056	Input Capture	Insider and Privilege Misuse	T1564.005	Hidden File System
Web App Hacking	T1056.004	Credential API Hooking	Targeted Intrusions	T1005	Data from Local System
Web App Hacking	T1057	Process Discovery	Targeted Intrusions	T1007	System Service Discovery
Web App Hacking	T1069	Permission Groups Discovery	Targeted Intrusions	T1012	Query Registry
Web App Hacking	T1082	System Information Discovery	Targeted Intrusions	T1016	System Network Config. Discovery
Web App Hacking	T1083	File and Directory Discovery	Targeted Intrusions	T1018	Remote System Discovery
Web App Hacking	T1120	Peripheral Device Discovery	Targeted Intrusions	T1027.003	Steganography
Web App Hacking	T1124	System Time Discovery	Targeted Intrusions	T1027.004	Compile After Delivery
Web App Hacking	T1134.004	Parent PID Spoofing	Targeted Intrusions	T1027.005	Indicator Removal from Tools
Web App Hacking	T1202	Indirect Command Execution	Targeted Intrusions	T1033	System Owner/User Discovery
Web App Hacking	T1497	Virtualization/Sandbox Evasion	Targeted Intrusions	T1036.004	Masquerade Task or Service
Web App Hacking	T1505.003	Web Shell	Targeted Intrusions	T1039	Data from Network Shared Drive
Web App Hacking	T1542.002	Component Firmware	Targeted Intrusions	T1049	System Network Conn. Discovery
Web App Hacking	T1546.005	Trap	Targeted Intrusions	T1056	Input Capture
Web App Hacking	T1546.012	Image File Exec. Options Injection	Targeted Intrusions	T1056.001	Keylogging
Web App Hacking	T1546.015	Comp. Object Model Hijacking	Targeted Intrusions	T1057	Process Discovery
Web App Hacking	T1547.010	Port Monitors	Targeted Intrusions	T1069	Permission Groups Discovery
Web App Hacking	T1564.001	Hidden Files and Directories	Targeted Intrusions	T1069.001	Local Groups
Insider and Privilege Misuse	T1005	Data from Local System	Targeted Intrusions	T1069.002	Domain Groups
Insider and Privilege Misuse	T1007	System Service Discovery	Targeted Intrusions	T1070.004	File Deletion
Insider and Privilege Misuse	T1012	Query Registry	Targeted Intrusions	T1070.005	Network Share Conn. Removal
Insider and Privilege Misuse	T1014	Rootkit	Targeted Intrusions	T1070.006	Timestomp
Insider and Privilege Misuse	T1016	System Network Config. Discovery	Targeted Intrusions	T1074	Data Staged
Insider and Privilege Misuse	T1018	Remote System Discovery	Targeted Intrusions	T1074.001	Local Data Staging
Insider and Privilege Misuse	T1020	Automated Exfiltration	Targeted Intrusions	T1074.002	Remote Data Staging
Insider and Privilege Misuse	T1025	Data from Removable Media	Targeted Intrusions	T1082	System Information Discovery
Insider and Privilege Misuse	T1033	System Owner/User Discovery	Targeted Intrusions	T1083	File and Directory Discovery
Insider and Privilege Misuse	T1039	Data from Network Shared Drive	Targeted Intrusions	T1113	Screen Capture
Insider and Privilege Misuse	T1056	Input Capture	Targeted Intrusions	T1124	System Time Discovery
Insider and Privilege Misuse	T1056.001	Keylogging	Targeted Intrusions	T1134.004	Parent PID Spoofing
Insider and Privilege Misuse	T1056.004	Credential API Hooking	Targeted Intrusions	T1140	Deobfuscate/Decode Files or Info.
Insider and Privilege Misuse	T1057	Process Discovery	Targeted Intrusions	T1207	Rogue Domain Controller
Insider and Privilege Misuse	T1069	Permission Groups Discovery	Targeted Intrusions	T1497.001	System Checks
Insider and Privilege Misuse	T1069.001	Local Groups	Targeted Intrusions	T1497.003	Time Based Evasion
Insider and Privilege Misuse	T1069.002	Domain Groups	Targeted Intrusions	T1505.003	Web Shell
Insider and Privilege Misuse	T1069.003	Cloud Groups	Targeted Intrusions	T1518	Software Discovery
Insider and Privilege Misuse	T1070.004	File Deletion	Targeted Intrusions	T1518.001	Security Software Discovery
Insider and Privilege Misuse	T1074	Data Staged	Targeted Intrusions	T1529	System Shutdown/Reboot
Insider and Privilege Misuse	T1074.001	Local Data Staging	Targeted Intrusions	T1546	Event Triggered Execution
Insider and Privilege Misuse	T1074.002	Remote Data Staging	Targeted Intrusions	T1546.012	Image File Exec. Options Injection
Insider and Privilege Misuse	T1082	System Information Discovery	Targeted Intrusions	T1547	Boot or Logon Autostart Exec.
Insider and Privilege Misuse	T1083	File and Directory Discovery	Targeted Intrusions	T1547.001	Registry Run Keys/Startup Folder
Insider and Privilege Misuse	T1087.003	Email Account	Targeted Intrusions	T1553.002	Code Signing
Insider and Privilege Misuse	T1113	Screen Capture	Targeted Intrusions	T1564	Hide Artifacts





The Center for Internet Security, Inc. (CIS[®]) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls[®] and CIS Benchmarks[™], globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images[®] provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center[®] (MS-ISAC[®]), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center[®] (EI-ISAC[®]), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

- 💮 cisecurity.org
- 🖾 info@cisecurity.org
- 518-266-3460
- in Center for Internet Security
- 🥑 @CISecurity
- TheCISecurity
- cisecurity