PROMIS

Professional Master in Information Security
Online Courses for Professionals in Security

BLEKINGE INSTITUTE OF TECHNOLOGY

"Indicator of compromise lifecycle and evaluation during threat hunting" –
By Oleksii Baranovskyi

Upcoming Security Seminars and Events
Send an email to **Nina Wennberg** **niw@bth.se** to subscribe to our mailing list and stay up to date for PROMIS talks and events!

PRO.M.IS
security built in

Visit PROMIS promisedu.se

PROMIS

BLEKINGE INSTITUTE OF TECHNOLOGY

Dr. Oleksii Baranovskyi, Ph.D.

Experienced cyber security expert with history in the academic as well as the financial and cybersecurity industry.

Certifications: CISSP, CISM, CCISO, CEH, SSCP, CHFI, ECSA, ECIH, CND, ISO 27001 Lead Auditor, etc.

Interests: Cloud Security and DevSecOps, Digital Forensic, Cyberwars.

I teach in these courses :

Penetration Testing and Ethical Hacking 3 credits

Advanced Forensic 7,5 credits

Web System Security, 7,5 credits

PRO.M.IS
security built in

What are Indicators of Compromise?

BLEKINGE INSTITUTE OF TECHNOLOGY

An Indicator of Compromise (IoC) is a clue that can be used to indicate an intrusion or compromise of a host in a network.

IoC can reveal:

- Tactics, Techniques and Procedures (TTP) used
- Severity of the incident
- Where to focus indident response and mitigation
- Who the threat actors are

IoC vs IoA

BLEKINGE INSTITUTE OF TECHNOLOGY

What happened?

What is happening and why?

MISP Perspective

BLEKINGE INSTITUTE OF TECHNOLOGY

Attribute Categories vs. Types

Category	Antivirus detection	Artifacts dropped	Attribution	External analysis	Financial fraud	Internal reference
AS				X		
aba-rtn					X	
anonymised	X	X	X	X	X	X
attachment	X	X		X		
authentihash		X				
bank-account-nr					X	
bic					X	
bin					X	
boolean						
bro				X		
btc					X	
campaign-id			X			
campaign-name			X			
cc-number					X	
cdhash		X				
chrome-extension-id						

- **hasshserver-md5**: hasshServer is a network fingerprinting standard which can be used to identify specific Server SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- **hex**: A value in hexadecimal format
- **hostname**: A full host/dnsname of an attacker
- **hostname|port**: Hostname and port number separated by a |
- **http-method**: HTTP method used by the malware (e.g. POST, GET, ...).
- **iban**: International Bank Account Number
- **identity-card-number**: Identity card number
- **impfuzzy**: A fuzzy hash of import table of Portable Executable format
- **imphash**: Import hash - a hash created based on the imports in the sample.
- **ip-dst**: A destination IP address of the attacker or C&C server
- **ip-dst|port**: IP destination and port number separated by a |
- **ip-src**: A source IP address of the attacker
- **ip-src|port**: IP source and port number separated by a |
- **issue-date-of-the-visa**: The date on which the visa was issued
- **ja3-fingerprint-md5**: JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.
- **jabber-id**: Jabber ID
- **jarm-fingerprint**: JARM is a method for creating SSL/TLS server fingerprints.
- **kusto-query**: Kusto query - Kusto from Microsoft Azure is a service for storing and running interactive analytics over Big Data.
- **last-name**: Last name of a natural person
- **link**: Link to an external information
- **mac-address**: Mac address
- **mac-eui-64**: Mac EUI-64 address
- **malware-sample**: Attachment containing encrypted malware sample
- **malware-type**:

Problem statement

BLEKINGE INSTITUTE OF TECHNOLOGY

The lifetime of the various available attributes are not homogeneous:

- IP addresses changes up
- IP addresses or domain names are traded and get used in different fashions over time
- File hashes usually tend not to vary over time, but a legitimate file can be embedded in a malware
- Etc.

Conclusions

BLEKINGE
INSTITUTE OF
TECHNOLOGY

1. Possible False Positives generation
2. Non-efficient storage and computational facilities using
3. Each attribute (IoC or IoA) has its own **DECAY** function

MISP approach

BLEKINGE INSTITUTE OF TECHNOLOGY

- Attributes should be evaluated
- The using should be based of evaluation
- The base score of an attribute should be a weighting of the **confidence** of its **source** and its linked taxonomies.
- The elapsed time an attribute was seen **first** and seen **last**.
- The end-time of an attribute represents the time at which the overall score should be 0.
- **The score should be reset upon a new sighting**.
- The **decay rate** represents the **speed** at which the overall score is decreasing over time.
    - The decay speed is variable over time: The decay rate of the IP should be low in the first hours, but should go faster the more time passes. The first time activities from this IP are sighted, the better chances are that the threat actors are still active or are executing follow up operations. When this IP address is shared among a community targeted by the threat actors, more and more members can take measures, such as blocking the IP address.

A little math ☺

BLEKINGE INSTITUTE OF TECHNOLOGY

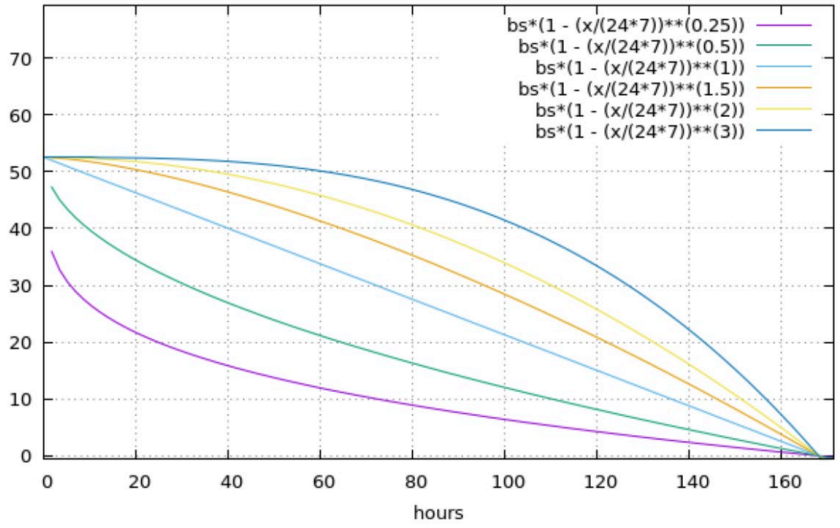
$$base\_score_a = weight_x \cdot tags + \omega_{sc} \cdot source\_confidence$$

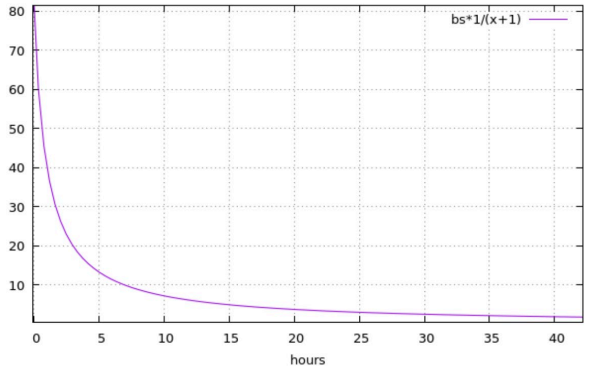
$$tags = \frac{\sum_{j=1}^{j=G} \sum_{i=1}^{i=T} taxonomy_i \cdot weight_i}{\sum_{j=1}^{j=G} \sum_{i=1}^{i=T} 100 \cdot weight_i}$$

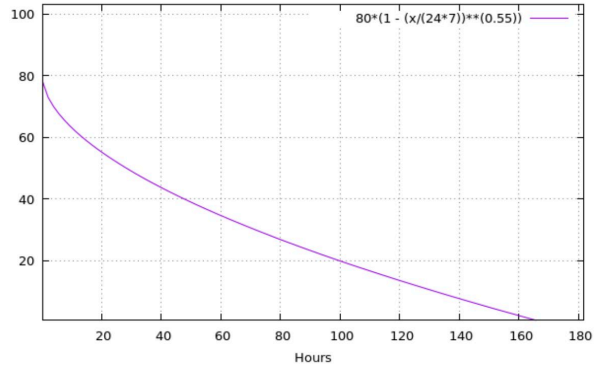
$$\mathtt{score}_a = \mathtt{base\_score} - \delta_a (T_t - T_{t-1})$$

$$\mathtt{score}_a = base\_score_a \cdot e^{-\delta_a \cdot t}$$

$$\mathtt{score}_a = \mathtt{base\_score} \cdot \left(1 - \left(\frac{t}{\tau_a}\right)^{\frac{1}{\delta_a}}\right)$$







Questions and Point of contentions

BLEKINGE INSTITUTE OF TECHNOLOGY

- Source confidence
  - Platform decision
  - Likes and reviews
  - Consensus **(in research)**
- Reporters activities

Lifecycle Management for Effective Threat Intelligence and Response

BLEKINGE INSTITUTE OF TECHNOLOGY

The lifecycle management of indicators is an essential element during incident response preparation, as it will influence decisions and actions against attackers. It's a continuous process of IoC and IoA to guarantee the information you work with is (and remains) valid and useful.

In general, save you a money!

Passive actions of DoD

BLEKINGE INSTITUTE OF TECHNOLOGY

Discover: The discover action is a "historical look at the data." This action heavily relies on your capability to store logs for a reasonable amount of time and have them accessible for searching. Typically, this type of action is applied against SIEM or stored network data. The goal is to determine whether you have seen a specific indicator in the past.

Detect: The other passive action is setting up detection rules of an indicator for future traffic. These actions are most often executed via an IDS or a specific logging rule on your firewall or application. It can also be configured as an alert in a SIEM when a specific condition is triggered.

U.S. Department of Defense. Joint Publication 3-13 Information Operations, February 2006. URL http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.

Active Actions by DoD

BLEKINGE
INSTITUTE OF
TECHNOLOGY

Deny: The deny action prevents the event from taking place. Common examples include a firewall block or a proxy filter.

Disrupt: Disruption makes the event fail as it is occurring. Examples include quarantining or memory protection measures.

Degrade: Degrading will not immediately fail an event, but it will slow down the further actions of the attacker. This tactic allows you to catch up during an incident response process, but you have to consider that the attackers may eventually succeed in achieving their objectives. Throttling bandwidth is one way to degrade an intrusion.

Deceive: Deception allows you to learn more about the intentions of the attacker by making them think the action was successful. One way to do this is to put a honeypot in place and redirect the traffic, based on an indicator, towards the honeypot.

Destroy: The destroy action is rarely for “usual” defenders, as this is an offensive action against the attacker. These actions, including physical destructive actions and arresting the attackers, are usually left to law enforcement agencies.

Example from Lokhid Martin

BLEKINGE INSTITUTE OF TECHNOLOGY

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

How to Feed Your Threat Intelligence Process

BLEKINGE
INSTITUTE OF
TECHNOLOGY

There's not a single rule, but 7 main steps:

1. Insert the indicator into your own intelligence platform.
2. Evaluate the **quality** of the indicator: Is it relevant to your organization? How likely is it to cause false positives? Do you have the capabilities to consume the indicator?
3. Apply the "discover" passive action by searching for past events matching the indicator. Typically, this is done using your SIEM solution and going through your logs and network data, searching for events that match the indicator.
4. Apply the "detect" passive action. Update your intrusion detection system (IDS) rule set and proxy logging to trigger an alert when the indicator is observed.
5. Apply both "discover" and "detect" actions to determine whether the indicator has been seen in your organization. If it has, then you'll have to analyze events related to that hit and search for additional indicators. These indicators will have to go through the same validation process.
6. Weigh the benefits of each active action to determine which is best for your organization, and then see that one through.
7. Share the validated and verified indicators extracted from this process with your threat intelligence community.

BLEKINGE
INSTITUTE OF
TECHNOLOGY

Security Readiness Shift Left

Upcoming Courses

BLEKINGE INSTITUTE OF TECHNOLOGY

Application Open for Autumn 2022 Courses – visit promisedu.se

[Development Security Applications (DevSecOps) 7,5 credits]

[Security Inventory for Software Development 3 credits]

[Applied Cryptography 5 credits]

[Security for Critical Infrastructure (Operational Technology) 7,5 credits]

[Web System Security, 7,5 credits]

All courses are:
- Designed for professionals
- Given Online and flexible
- App 25% Study Pace
- Free of charge, University credits

Questions about Application?

Contact Nina Wennberg niw@bth.se or Anna Eriksson aes@bth.se

PRO.M.IS
security built in


AXIS
COMMUNICATIONS


advenica


addalot


factor10


IBM


SWEDSOFT


BALLOU


Handelsbanken


Nordea


sast
SWEDISH ASSOCIATION FOR SOFTWARE TESTING


BIL Sweden


DXC.technology


Orange Cyberdefense


TRUESEC


BorgWarner


CYBERCOM
GROUP


BLEKINGE TEKNISKA HÖGSKOLA
BTH

Polisen


ERICSSON


FKG

MaxKompetens


citynetwork


telenor


2Secure


SAAB
TECHNOLOGIES

SAAB

Thank you!


IT&Telekomföretagen


IKEA


SIREN
Swedish Requirements Engineering Research Network


TOLPAGORNI
product management


Knowledge Foundation


PRO.M.IS
security built in