FALCON
Fighting Corruption & Organised Crime

SafeHorizon

Anticipate Ransomware Strategies

The role of tracking cryptocurrency patterns in a Crime-as-a-Service landscape

Francesco Zola, Mikel Gorricho*, Jon Ander Medina*, Lander Segurola*, Raúl Orduna**

** Vicomtech, Basque Reseaech and Technology Alliance*

What is the current landscape?

Criminal networks are leveling up by using the Crime-as-a-Service (CaaS) model, boosting collaboration among cybercriminals and amplifying the impact of their attacks. In this scenario, **Ransomware** is no longer just a threat to individuals, it is now targeting governments, banks, and even hospitals, generating significant economic gains for attackers.

What is the issue?

The CaaS model has enabled the mass production of Ransomware, allowing different strains to use similar tactics for ransom collection, fund movement, and money laundering. Furthermore, with the rise of cryptocurrencies (like Bitcoin and Monero) that promote decentralised operations and anonymity, Ransomware has found a perfect platform for growth.

What have we done?

We analyzed Ransomware strains and their financial movements in the Bitcoin network, uncovering common payment patterns and connections between them. Using advanced graph analysis, we explored how different strains might be linked, uncovering the modus operandi of the same (potential) attacker.

What we found.

Our research reveals that some Ransomware strains have been active in the Bitcoin network for years, using similar tactics. These findings could help law enforcement predict and track attackers more effectively. A step forward in understanding Ransomware cosystem.

This Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 870610 and grant agreement No 101168562.

vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE