Blockchain Meets the Cyber Kill Chain

SANS DFIR Summit
July 2021

Agenda

- Myth Busting
- Why Blockchain for DFIR?
- Case Studies
  - Prevention
  - Attribution Strategies
  - Investigation + Disruption
- Resources

Common Crypto Myths

DEBUNKED

✗ MYTH	✓ FACT
"Only criminals use cryptocurrency."	Economic activity in 2020 = ~$3T ...only 0.34% of that activity was criminal
"Cryptocurrency is anonymous and therefore untraceable."	Crypto is *pseudonymous* and transaction data is public. Blockchain analytics tools enable tracking and enrichment.
"Cryptocurrency doesn't touch my work."	Historically, financial data has not been available or easily navigable. Crypto is multidisciplinary and complements other indicators.

What is cryptocurrency used for?

Storing funds

Investing and exchanging

Mining

Buying/selling legal goods and services

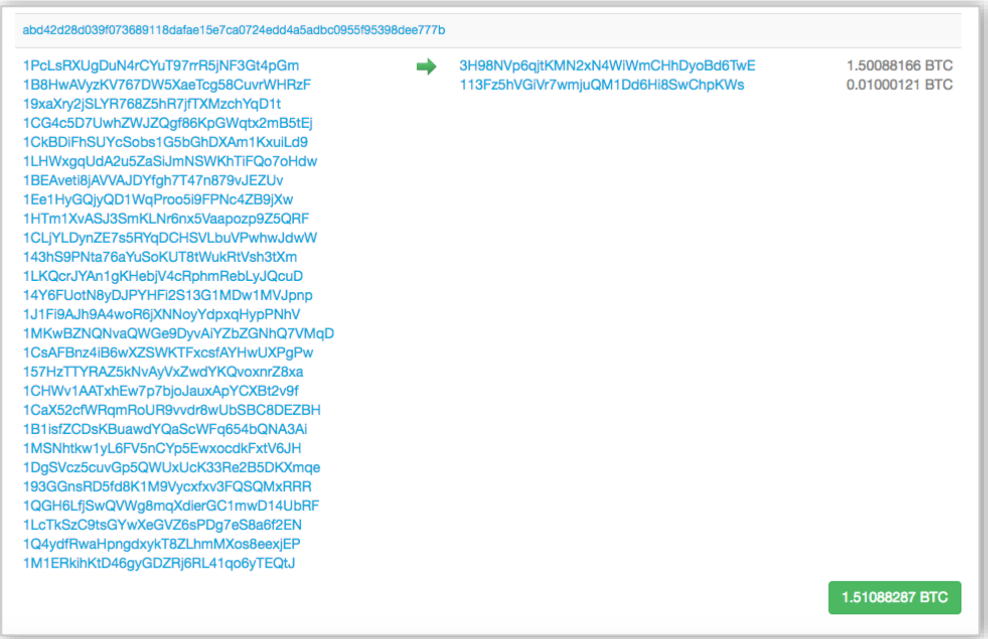
Stealing /scamming

Hiding trails (for privacy or money laundering)

Buying/selling illegal goods and services

Map addresses to real-world entities

What you see on the blockchain

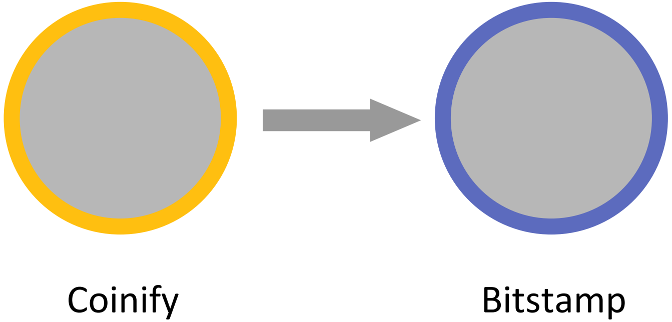


```
abd42d28d039f073689118dafae15e7ca0724edd4a5adbc0955f95398dee777b

1PcLsRXUgDuN4rCYuT97rrR5jNF3Gt4pGm     ➡   3H98NVp6qjtKMN2xN4WiWmCHhDyoBd6TwE    1.50088166 BTC
1B8HwAVyzKV767DW5XaeTcg58CuvrWHRzF         113Fz5hVGiVr7wmjuQM1Dd6Hi8SwChpKWs    0.01000121 BTC
19xaXry2jSLYR768Z5hR7jfTXMzchYqD1t
1CG4c5D7UwhZWJZQgf86KpGWqtx2mB5tEj
1CkBDiFhSUYcSobs1G5bGhDXAm1KxuiLd9
1LHWxgqUdA2u5ZaSiJmNSWKhTiFQo7oHdw
1BEAveti8jAVVAJDYfgh7T47n879vJEZUv
1Ee1HyGQjyQD1WqProo5i9FPNc4ZB9jXw
1HTm1XvASJ3SmKLNr6nx5Vaapozp9Z5QRF
1CLjYLDynZE7s5RYqDCHSVLbuVPwhwJdwW
143hS9PNta76aYuSoKUT8tWukRtVsh3tXm
1LKQcrJYAn1gKHebjV4cRphmRebLyJQcuD
14Y6FUotN8yDJPYHFi2S13G1MDw1MVJpnp
1J1Fi9AJh9A4woR6jXNNoyYdpxqHypPNhV
1MKwBZNQNvaQWGe9DyvAiYZbZGNhQ7VMqD
1CsAFBnz4iB6wXZSWKTFxcsfAYHwUXPgPw
157HzTTYRAZ5kNvAyVxZwdYKQvoxnrZ8xa
1CHWv1AATxhEw7p7bjoJauxApYCXBt2v9f
1CaX52cfWRqmRoUR9vvdr8wUbSBC8DEZBH
1B1isfZCDsKBuawdYQaScWFq654bQNA3Ai
1MSNhtkw1yL6FV5nCYp5EwxocdkFxtV6JH
1DgSVcz5cuvGp5QWUxUcK33Re2B5DKXmqe
193GGnsRD5fd8K1M9VycxfxV3FQSQMxRRR
1QGH6LfjSwQVWg8mqXdierGC1mwD14UbRF
1LcTkSzC9tsGYwXeGVZ6sPDg7eS8a6f2EN
1Q4ydfRwaHpngdxykT8ZLhmMXos8eexjEP
1M1ERkihKtD46gyGDZRj6RL41qo6yTEQtJ

                                                                                 1.51088287 BTC
```

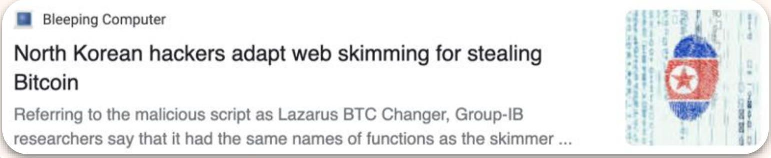
What you see in Chainalysis



Services can have thousands to tens of millions of addresses

Crypto-centric cybercrime is expanding

Cryptoskimming

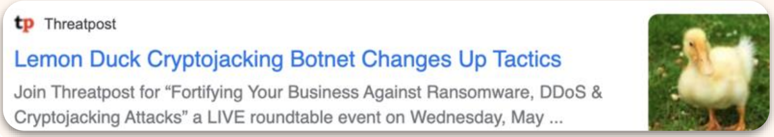


Bleeping Computer

North Korean hackers adapt web skimming for stealing Bitcoin

Referring to the malicious script as Lazarus BTC Changer, Group-IB researchers say that it had the same names of functions as the skimmer ...

Cryptojacking (mining)

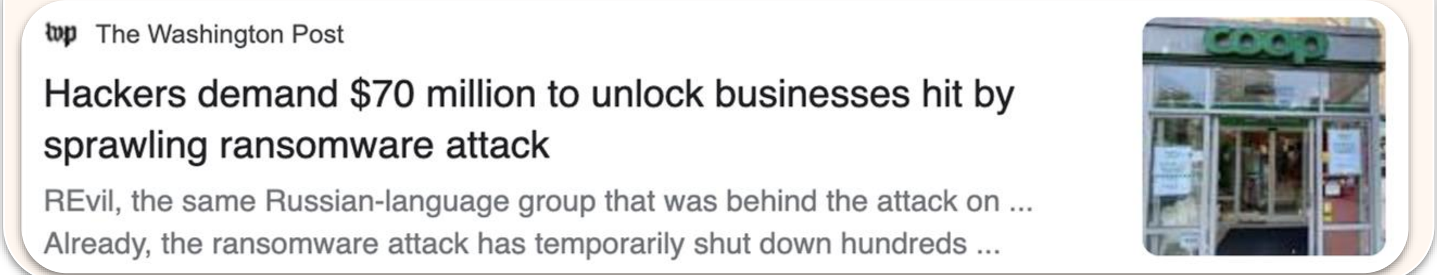


Threatpost

Lemon Duck Cryptojacking Botnet Changes Up Tactics

Join Threatpost for "Fortifying Your Business Against Ransomware, DDoS & Cryptojacking Attacks" a LIVE roundtable event on Wednesday, May ...

Ransomware

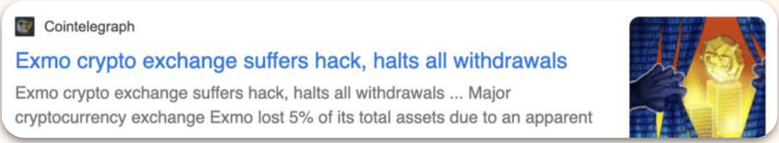


The Washington Post

Hackers demand $70 million to unlock businesses hit by sprawling ransomware attack

REvil, the same Russian-language group that was behind the attack on ... Already, the ransomware attack has temporarily shut down hundreds ...

Exchange hacks

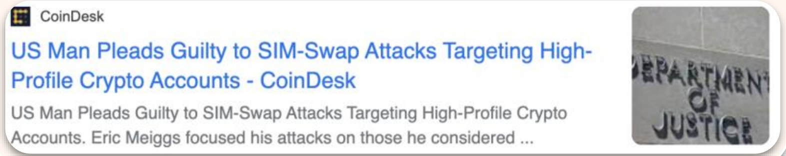


Cointelegraph

Exmo crypto exchange suffers hack, halts all withdrawals

Exmo crypto exchange suffers hack, halts all withdrawals ... Major cryptocurrency exchange Exmo lost 5% of its total assets due to an apparent

SIM-swapping



CoinDesk

US Man Pleads Guilty to SIM-Swap Attacks Targeting High-Profile Crypto Accounts - CoinDesk

US Man Pleads Guilty to SIM-Swap Attacks Targeting High-Profile Crypto Accounts. Eric Meiggs focused his attacks on those he considered ...

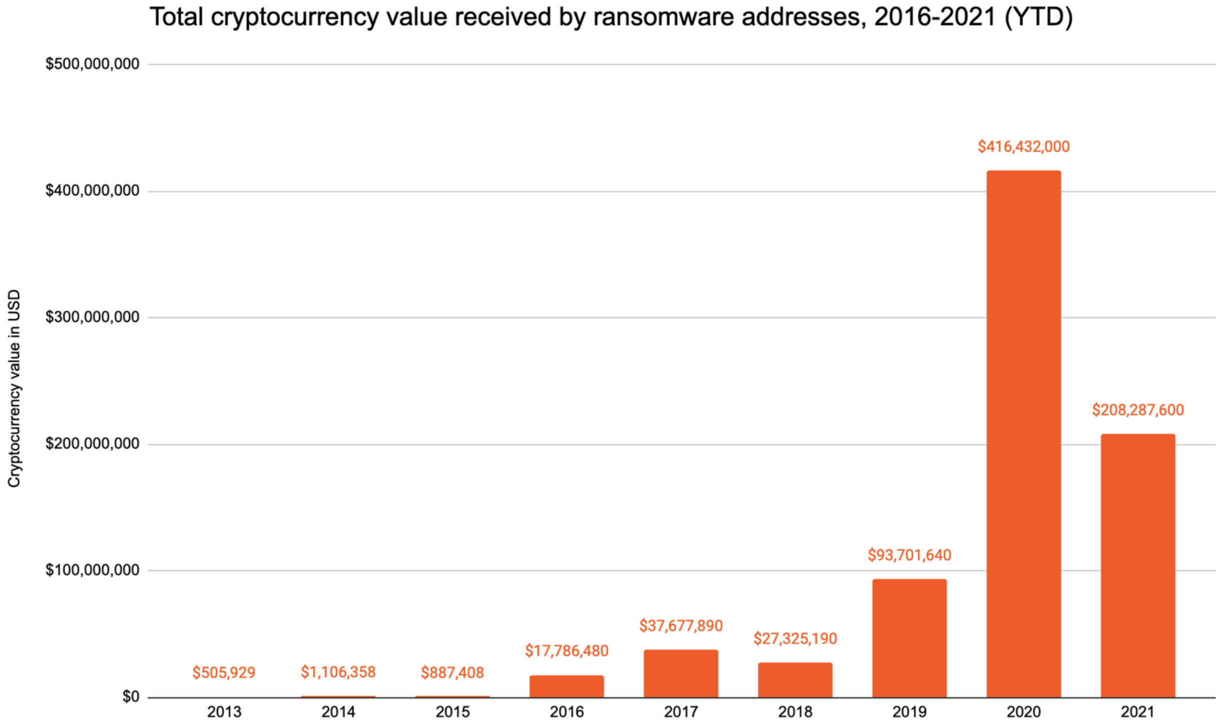
Ransomware Trends

Increase in overall Ransomware revenue

Increase in average ransom payment demanded

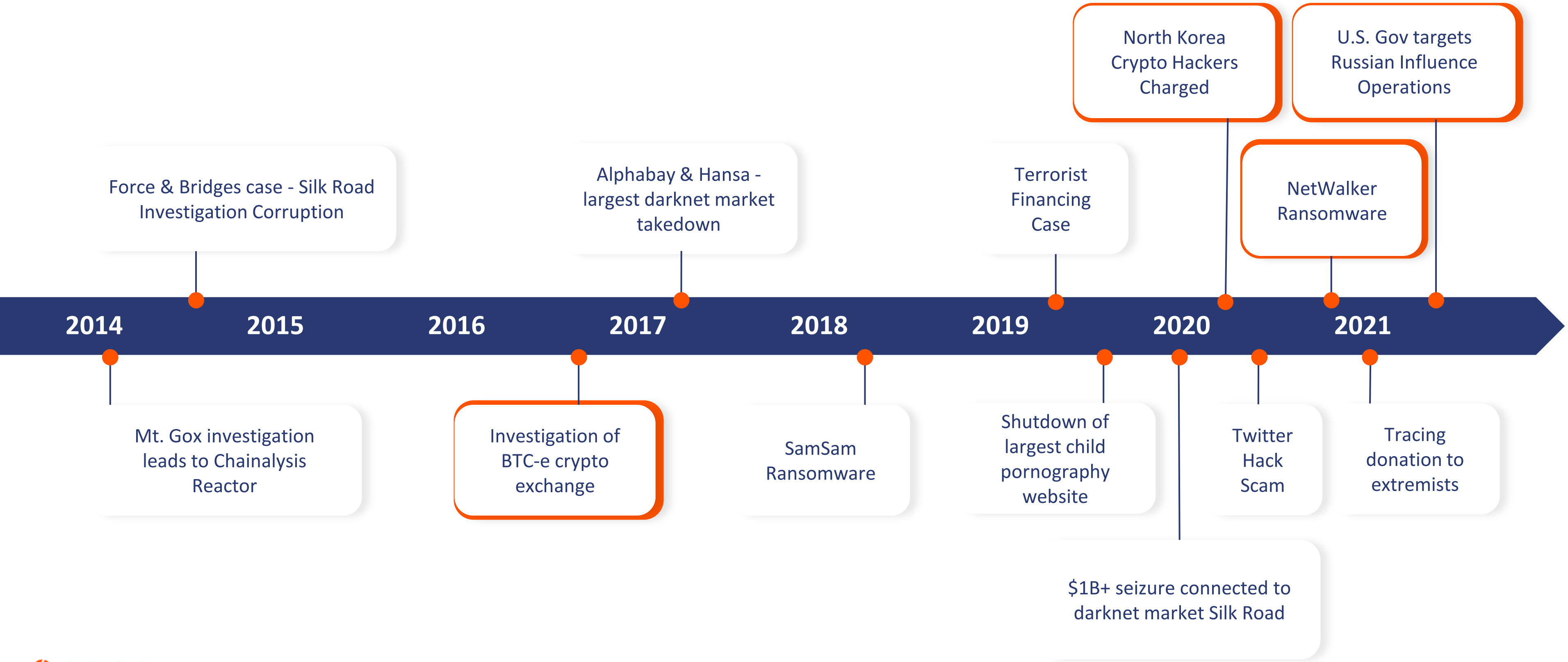
Increase in unique threat actors engaging in the ransomware ecosystem

Increase in ransomware group turnover



How does it work for DFIR investigations?

Attribution & Disruption in Action



2014

Mt. Gox investigation leads to Chainalysis Reactor

Force & Bridges case - Silk Road Investigation Corruption

2015

2016

Investigation of BTC-e crypto exchange

2017

Alphabay & Hansa - largest darknet market takedown

2018

SamSam Ransomware

Terrorist Financing Case

2019

Shutdown of largest child pornography website

2020

$1B+ seizure connected to darknet market Silk Road

North Korea Crypto Hackers Charged

Twitter Hack Scam

NetWalker Ransomware

2021

Tracing donation to extremists

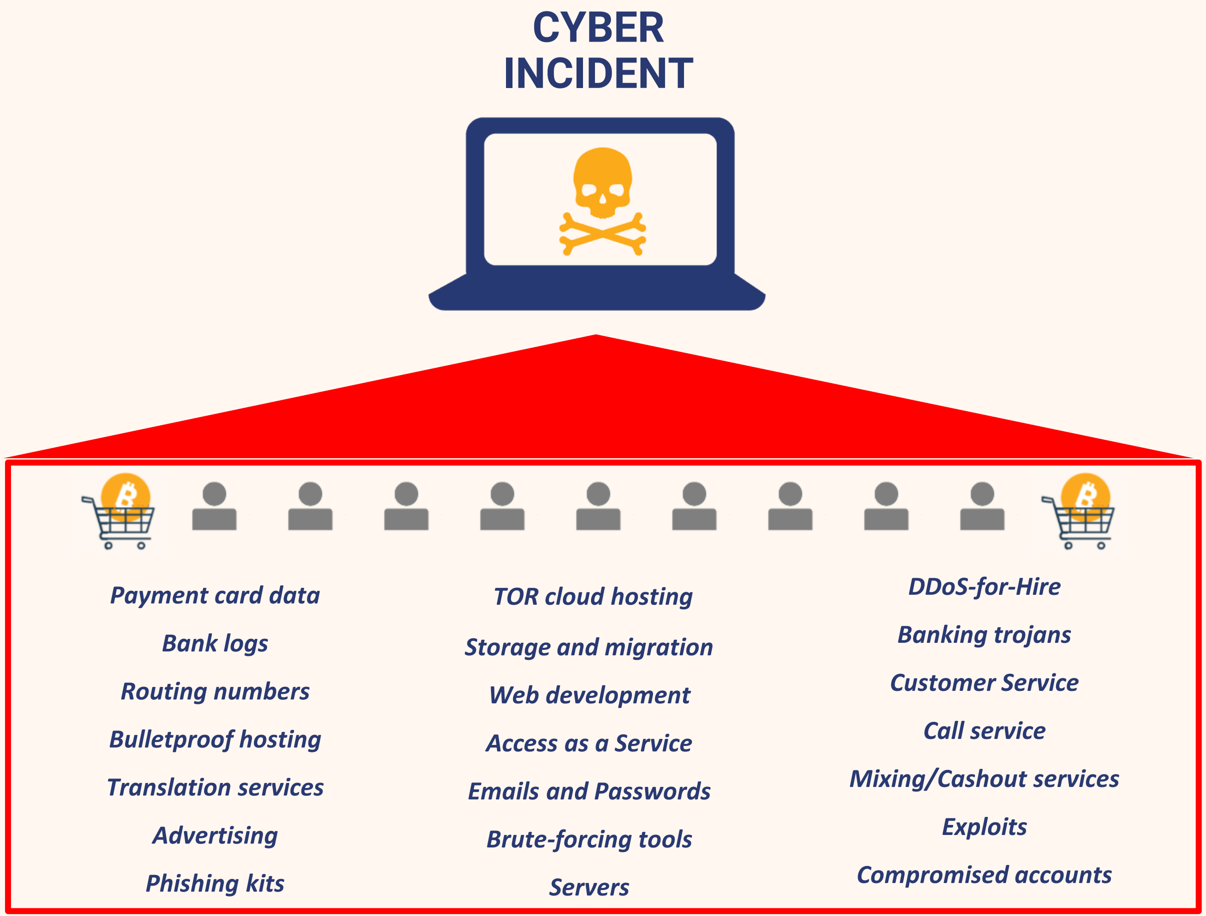
U.S. Gov targets Russian Influence Operations

Thriving underground supply chain

- Incidents are not monolithic - threat actors outsource components of an attack to underground professionals

- Easy-to-deploy OOTB tools enable amateurs to leapfrog to sophistication

- Attackers scout for additional talent & tools to make illicit campaigns more devastating



CYBER INCIDENT

Payment card data

Bank logs

Routing numbers

Bulletproof hosting

Translation services

Advertising

Phishing kits

TOR cloud hosting

Storage and migration

Web development

Access as a Service

Emails and Passwords

Brute-forcing tools

Servers

DDoS-for-Hire

Banking trojans

Customer Service

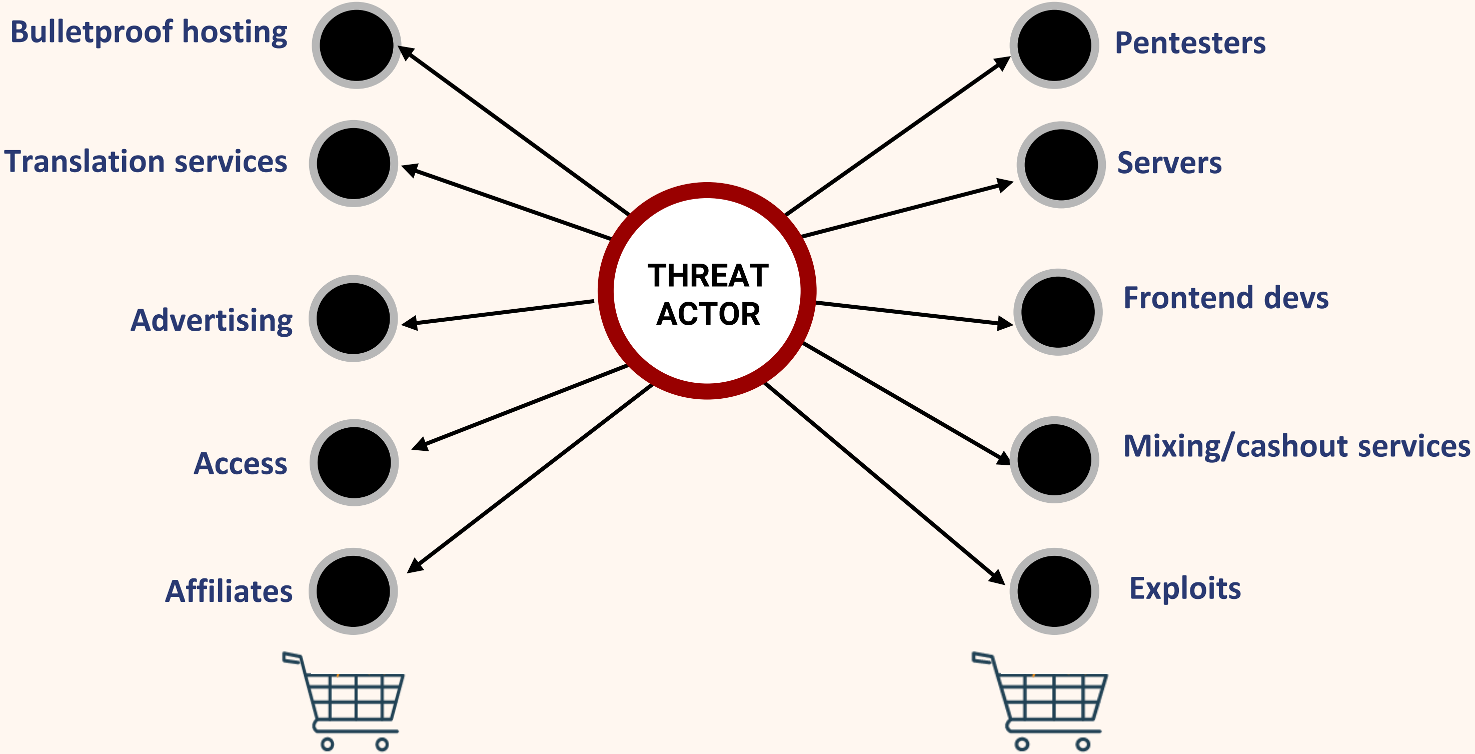
Call service

Mixing/Cashout services

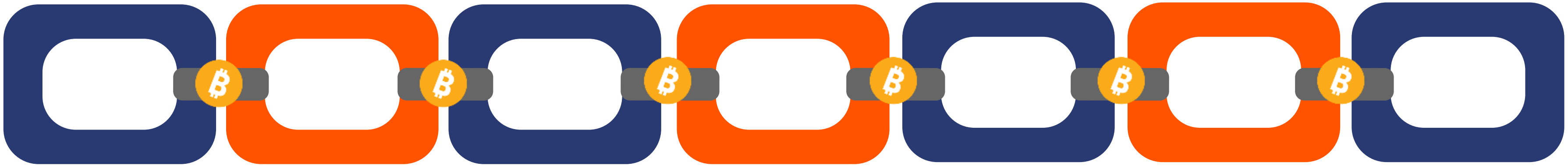
Exploits

Compromised accounts

A single attack relies on multiple people and tools



Cyber Kill Chain Meets Blockchain



RECONNAISSANCE	WEAPONIZATION	DELIVERY	EXPLOITATION	INSTALLATION	COMMAND & CONTROL	ACTIONS ON OBJECTIVES
Infostealer Network access Scanning Tools Pentesters	Botnets Exploit kits Malware	Phishing kits Affiliates Domains Bulletproof hosting	Exploits Brute forcing tools	RATS Tools (Cobalt Strike) Miners	C2 Infrastructure Stolen creds	Ransomware Cryptojacking Data encryption/ exfiltration Account takeover

Threat actors use cryptocurrency to propel cyber intrusions through each stage of the kill chain

Lockheed-Martin Cyber Kill Chain

Why Blockchain Analytics for DFIR?

Identify and map the entire attack supply chain, adversary infrastructure and associates

Programmatic prioritization and lead generation with integration and enhancement of existing datasets

Automated real-time alerts prompt quick disposition of risky activity
eg. OFAC SDN list, cryptocurrency activity in sanctioned or high risk jurisdictions

Enterprise-level access to a unique proprietary dataset used as evidence in court

Attribution of a specific threat actor or group with a single cryptocurrency address

Common operating picture with public and private sector fosters collaboration for intelligence sharing and coordinated disruption or asset recovery

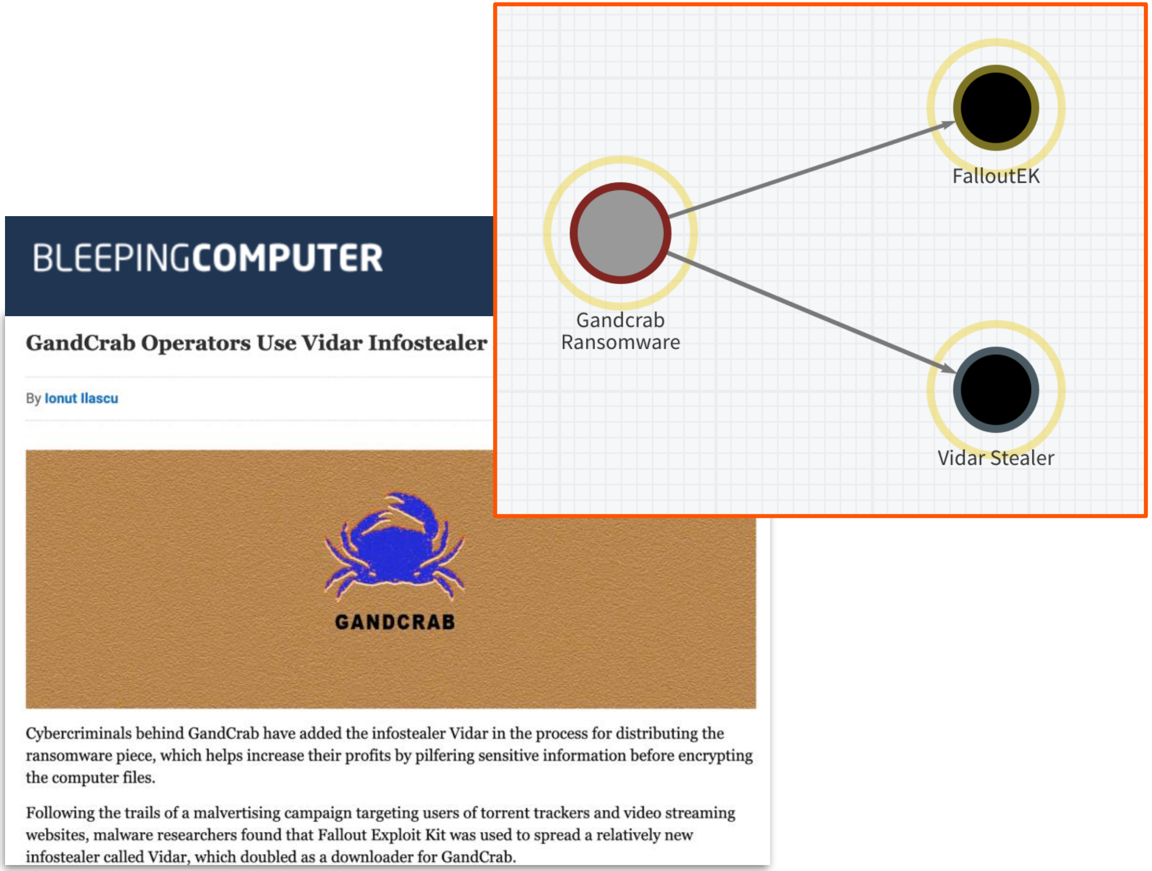
Enrichment, Attribution, Disruption, Recovery

Case Studies

Prevention: Stay ahead of the threat

(and the news)

- ***Prioritize appropriate measures (such as patching)***
- ***Eliminate vulnerabilities before an attack even takes place***



BLEEPINGCOMPUTER

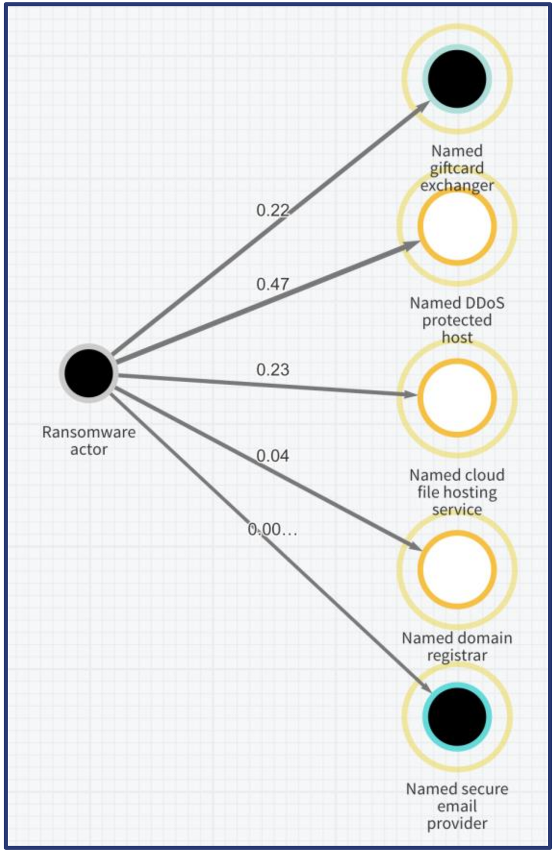
GandCrab Operators Use Vidar Infostealer

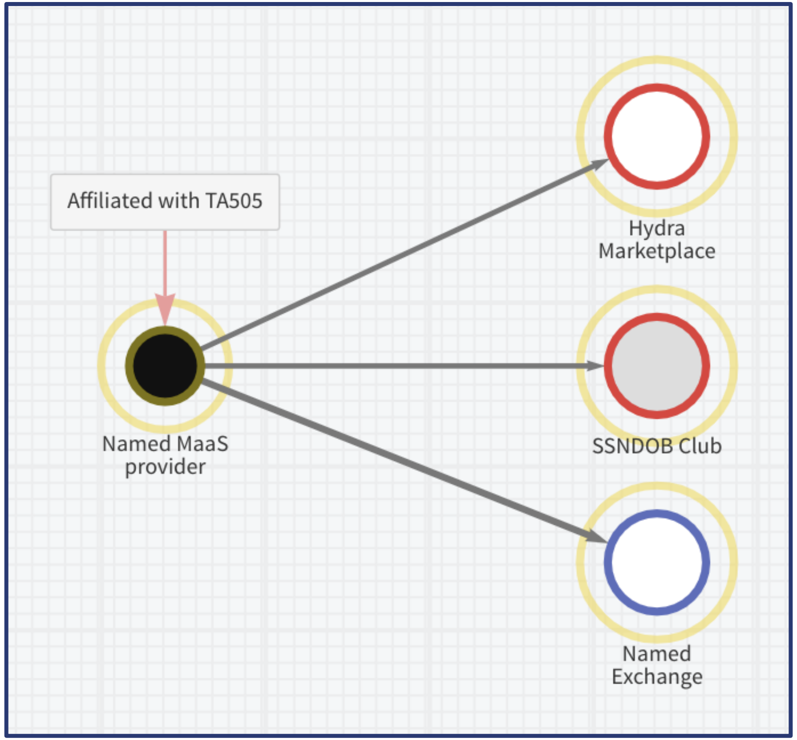
By Ionut Ilascu

Cybercriminals behind GandCrab have added the infostealer Vidar in the process for distributing the ransomware piece, which helps increase their profits by pilfering sensitive information before encrypting the computer files.

Following the trails of a malvertising campaign targeting users of torrent trackers and video streaming websites, malware researchers found that Fallout Exploit Kit was used to spread a relatively new infostealer called Vidar, which doubled as a downloader for GandCrab.

Insight into adversary infrastructure & capabilities


Named giftcard exchanger
0.22
0.47
Named DDoS protected host
0.23
Ransomware actor
Named cloud file hosting service
0.04
0.00…
Named domain registrar
Named secure email provider

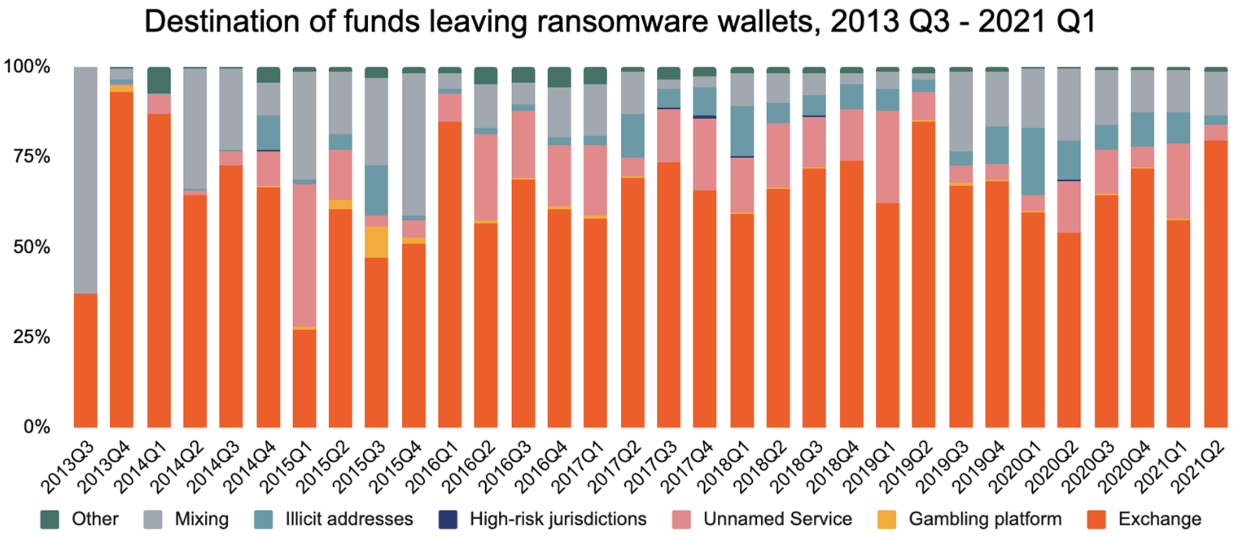


Role of Exchanges

Cyber criminals eventually need to move their crypto into fiat currency.

This means that, more than likely, they must interact with **an exchange**.

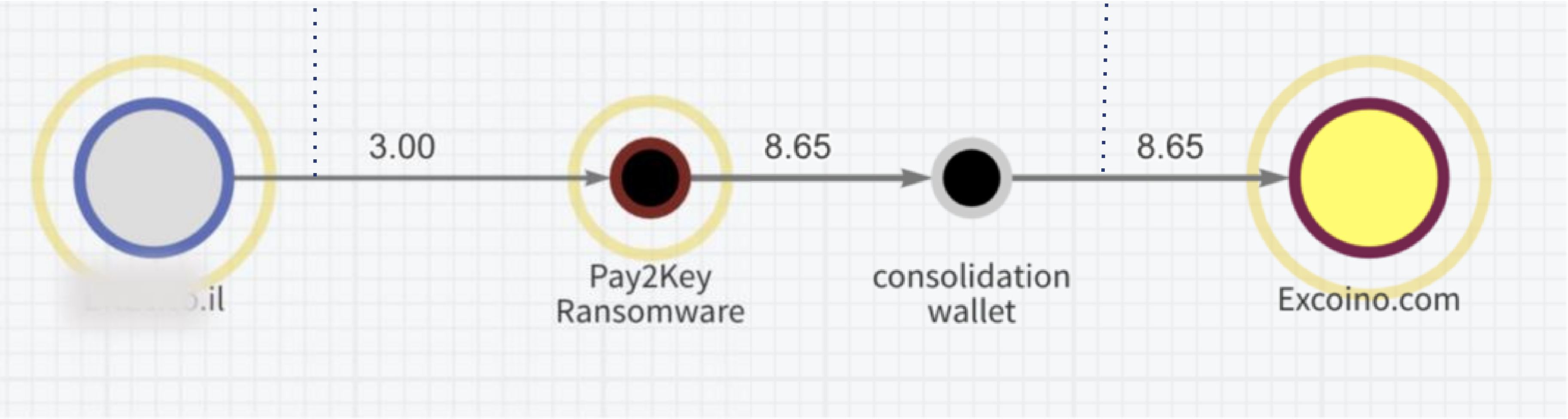
Exchanges are cryptocurrency services that play vital roles in attributing and disrupting ransomware actors.



Attribution Legal & Regulatory issues

In October 2020, Israeli victims were targeted by a new ransomware variant, “Pay2Key”.

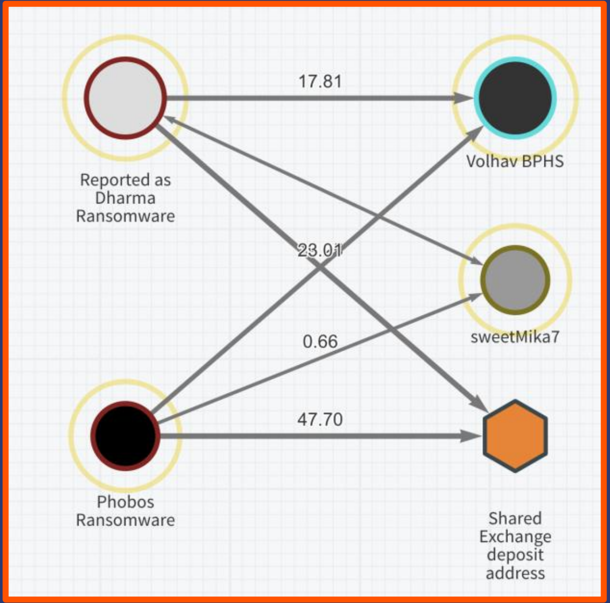
Funds from multiple victim payments were consolidated and ultimately cashed out an Iranian exchange.



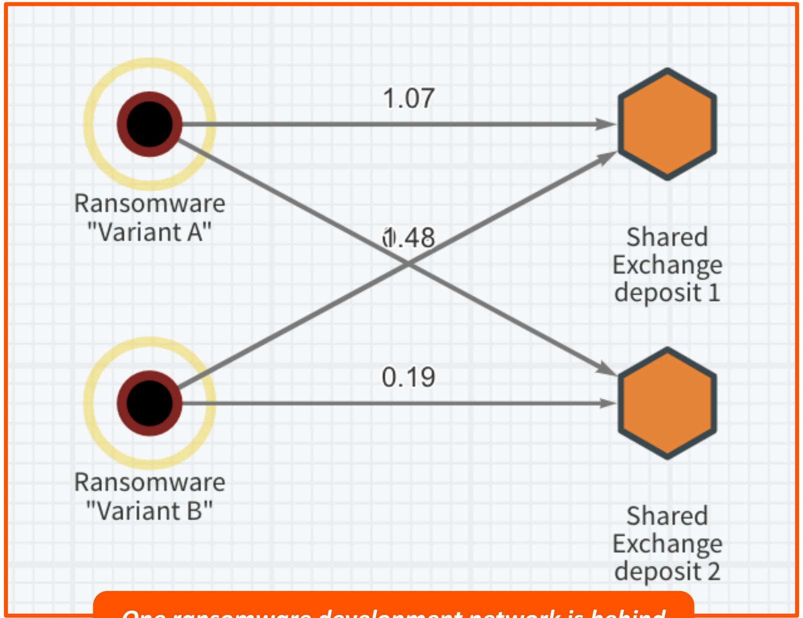
> *“ Using Chainalysis proprietary sources, we identified the root BTC address affiliated with the wallet… according to the public ledger this Bitcoin cluster received direct payments from multiple underground criminal sources, including ransomware operators tied to the Phobos and CrySiS (Dharma) strains. Operators likely used volhav as their preferred method of bulletproof hosting for component of their malicious infrastructure. The INFOSEC community has historically reported on technical and operational similarities between two, separate strains of ransomware, Phobos and CrySiS (Dharma) leading to speculation that operations of the malware were working together in some capacity. The co-hosting strengthens this theory. ”*

Recorded Future

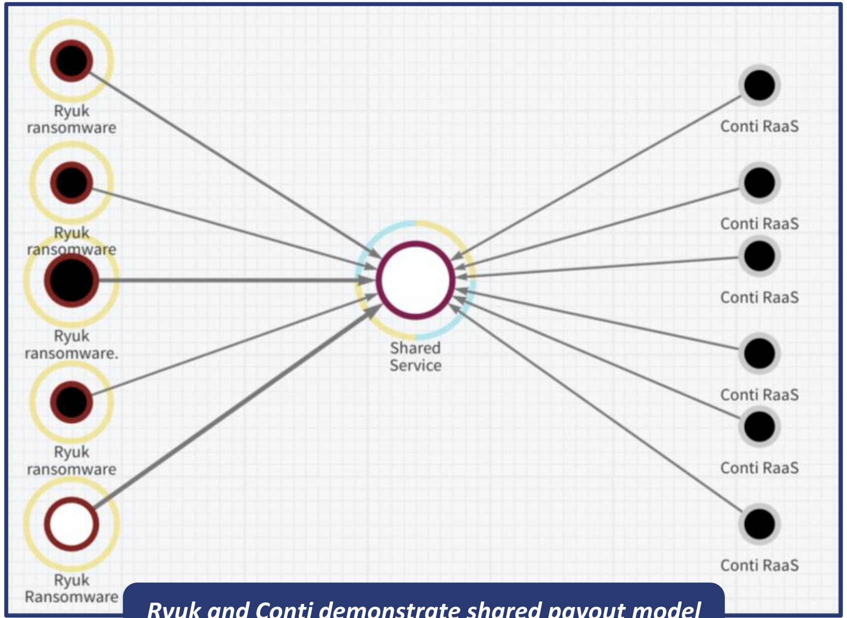
Threat Resolution


17.81
Reported as Dharma Ransomware
Volhav BPHS
23.01
sweetMika7
0.66
47.70
Phobos Ransomware
Shared Exchange deposit address

Attribution | Impersonators & Chameleons



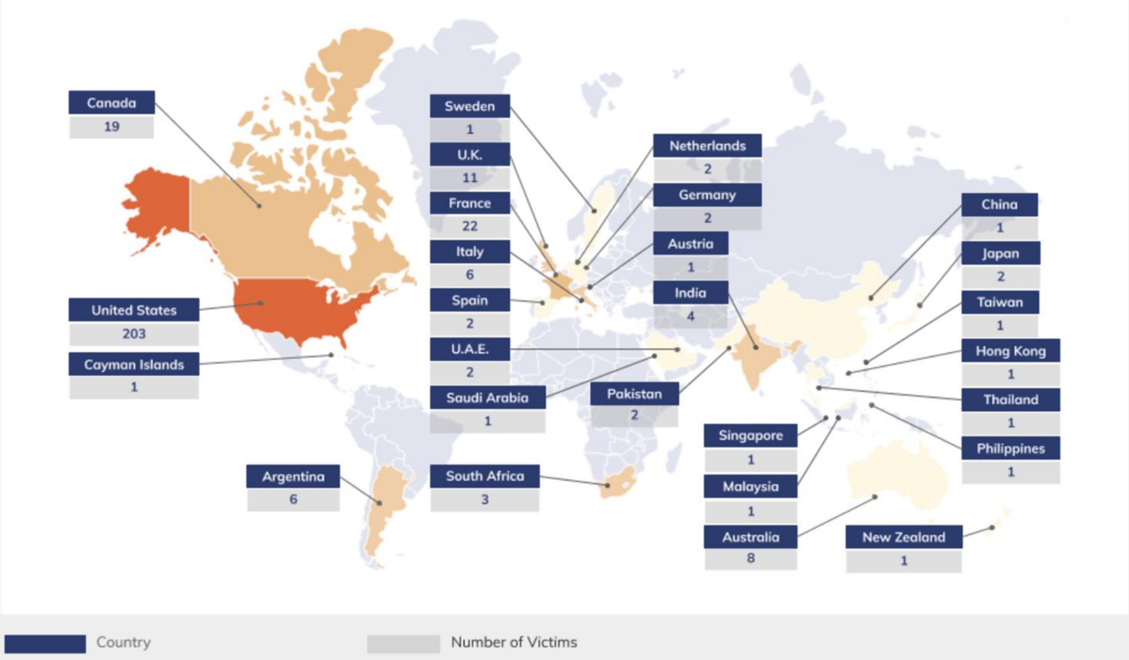
One ransomware development network is behind multiple ransomware strains



Ryuk and Conti demonstrate shared payout model as well as creators and operators

NetWalker Ransomware

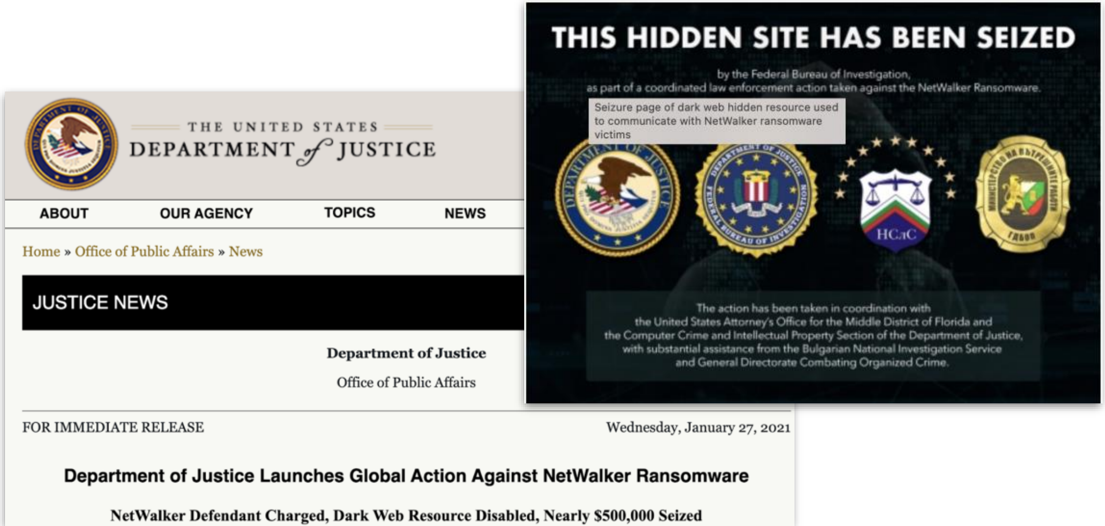
- Operated as a Ransomware- as-a-Service (RaaS) model
- Garnered at least $78 million in ransom proceeds since becoming active in August 2019
- Impacted at least 305 victims from 27 countries, including 203 in the U.S.
- While NetWalker publicly claimed not to target hospitals, they've attacked healthcare facilities in Philadelphia, Atlanta, and Canada



Investigation & Disruption

NetWalker ransomware affiliate and Canadian national Vachon-Desjardins arrested and charged in January 2021

- Allegedly responsible for at least 91 attacks, and received $14 million worth of bitcoin at the time of receipt
- Nearly $500,000 seized



THE UNITED STATES DEPARTMENT of JUSTICE

ABOUT | OUR AGENCY | TOPICS | NEWS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Wednesday, January 27, 2021

Department of Justice Launches Global Action Against NetWalker Ransomware

NetWalker Defendant Charged, Dark Web Resource Disabled, Nearly $500,000 Seized

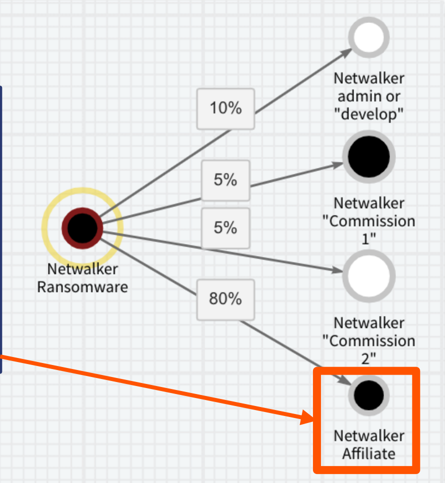
THIS HIDDEN SITE HAS BEEN SEIZED

by the Federal Bureau of Investigation, as part of a coordinated law enforcement action taken against the NetWalker Ransomware.

Seizure page of dark web hidden resource used to communicate with NetWalker ransomware victims

The action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice, with substantial assistance from the Bulgarian National Investigation Service and General Directorate Combating Organized Crime.

Affiliates like Vachon-Desjardins were responsible for obtaining access to victim networks and ultimately deploying the ransomware. Hence, affiliates receive the lion's share of the profits--typically 76-80% commissions for NetWalker affiliates as shown in Chainalysis Reactor.



Resources

Visit Chainalysis.com

Research Reports

The 2021 Crypto Crime Report

Everything you need to know about ransomware, darknet markets, and more

February 2021

Webinars

Training

Cryptocurrency Fundamentals Certification

Investigation Specialist Certification

Intelligence Briefs & Blogs

Bulletproof Hosting Provider Black Host Linked to North Korea Cryptocurrency Exchange Hackers

Black Host is a **bulletproof hosting provider**, which is a type of web hosting provider that lets customers use its services anonymously and is generally lenient on the content it will allow them to host. Firms like Black Host fit into a wider category of anonymity services that allow users to maintain a web presence without compromising their privacy. Other examples include virtual SIM card providers, VPN providers, and anonymous email providers.

- Case Studies
- Money Laundering
- Scams
- Ransomware
- Darknet Markets
- Mixing
- Terrorism and Extremism Financing
- Market Trends
- APTs
- Anonymity Services
- Geographic Intelligence
- Sanctions
- **and more!**

Thank you

jackie@chainalysis.com

Twitter @jburnskoven