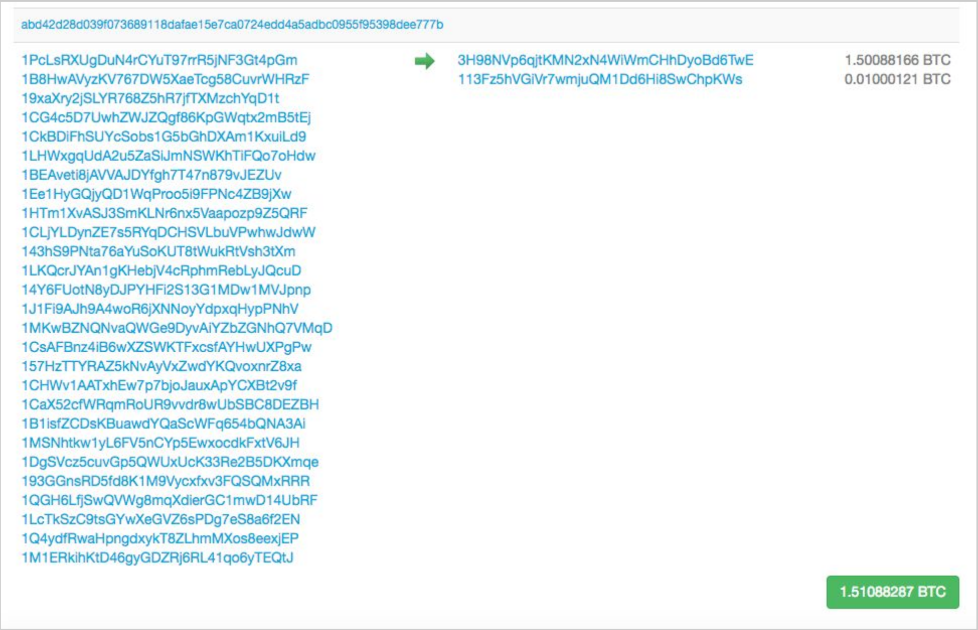
Chainalysis

Cryptocurrency Tracing

Workshop on Crime and Cryptocurrencies
November 17, 2021

Chainalysis maps addresses to entities

What you see on the blockchain

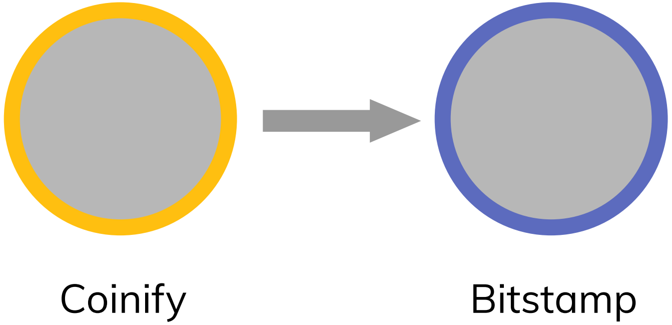


abd42d28d039f073689118dafae15e7ca0724edd4a5adbc0955f95398dee777b

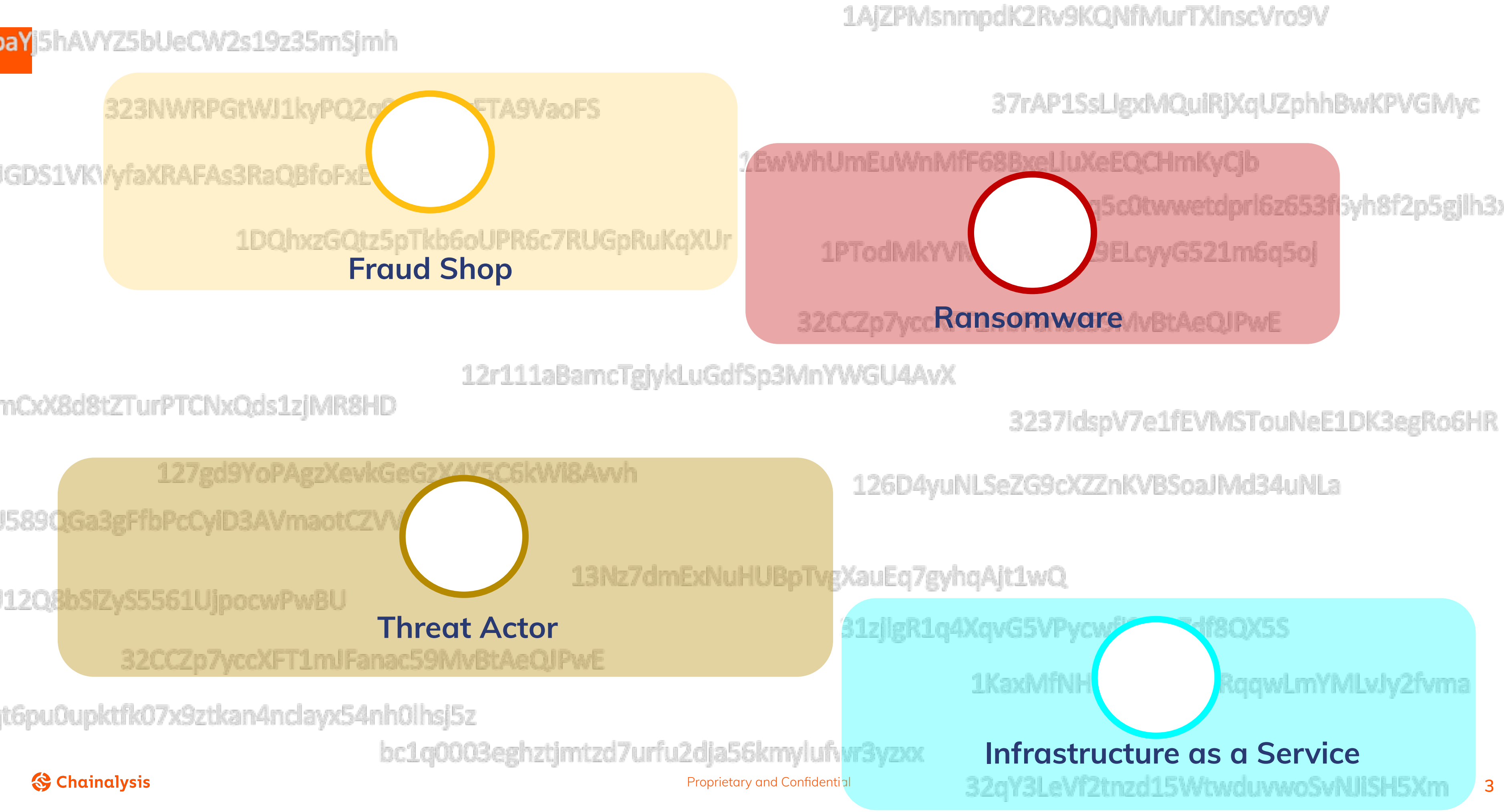
1PcLsRXUgDuN4rCYuT97rrR5jNF3Gt4pGm
1B8HwAVyzKV767DW5XaeTcg58CuvrWHRzF
19xaXry2jSLYR768Z5hR7jfTXMzchYqD1t
1CG4c5D7UwhZWJZQgf86KpGWqtx2mB5tEj
1CkBDiFhSUYcSobs1G5bGhDXAm1KxuiLd9
1LHWxgqUdA2u5ZaSiJmNSWKhTiFQo7oHdw
1BEAveti8jAVVAJDYfgh7T47n879vJEZUv
1Ee1HyGQjyQD1WqProo5i9FPNc4ZB9jXw
1HTm1XvASJ3SmKLNr6nx5Vaapozp9Z5QRF
1CLjYLDynZE7s5RYqDCHSVLbuVPwhwJdwW
143hS9PNta76aYuSoKUT8tWukRtVsh3tXm
1LKQcrJYAn1gKHebjV4cRphmRebLyJQcuD
14Y6FUotN8yDJPYHFi2S13G1MDw1MVJpnp
1J1Fi9AJh9A4woR6jXNNoyYdpxqHypPNhV
1MKwBZNQNvaQWGe9DyvAiYZbZGNhQ7VMqD
1CsAFBnz4iB6wXZSWKTFxcsfAYHwUXPgPw
157HzTTYRAZ5kNvAyVxZwdYKQvoxnrZ8xa
1CHWv1AATxhEw7p7bjoJauxApYCXBt2v9f
1CaX52cfWRqmRoUR9vvdr8wUbSBC8DEZBH
1B1isfZCDsKBuawdYQaScWFq654bQNA3Ai
1MSNhtkw1yL6FV5nCYp5EwxocdkFxtV6JH
1DgSVcz5cuvGp5QWUxUcK33Re2B5DKXmqe
193GGnsRD5fd8K1M9Vycxfxv3FQSQMxRRR
1QGH6LfjSwQVWg8mqXdierGC1mwD14UbRF
1LcTkSzC9tsGYwXeGVZ6sPDg7eS8a6f2EN
1Q4ydfRwaHpngdxykT8ZLhmMXos8eexjEP
1M1ERkihKtD46gyGDZRj6RL41qo6yTEQtJ

3H98NVp6qjtKMN2xN4WiWmCHhDyoBd6TwE 1.50088166 BTC
113Fz5hVGiVr7wmjuQM1Dd6Hi8SwChpKWs 0.01000121 BTC

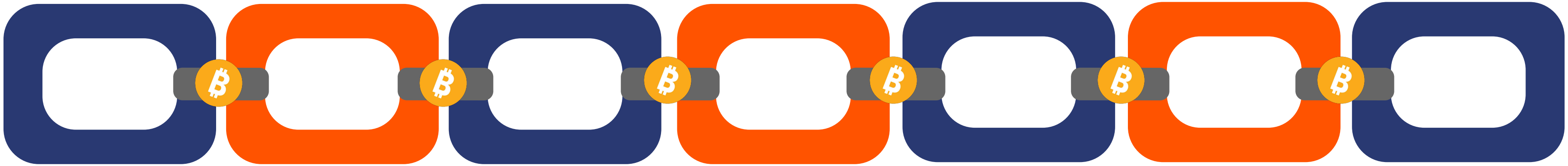
What you see in Chainalysis



Services can have thousands to tens of millions of addresses


Fraud Shop
Ransomware
Threat Actor
Infrastructure as a Service
1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V
37rAP1SsLJgxMQuiRjXqUZphhBwKPVGMyc
12r111aBamcTgjykLuGdfSp3MnYWGU4AvX
3237idspV7e1fEVMSTouNeE1DK3egRo6HR
126D4yuNLSeZG9cXZZnKVBSoaJMd34uNLa
13Nz7dmExNuHUBpTvgXauEq7gyhqAjt1wQ
32CCZp7yccXFT1mJFanac59MvBtAeQJPwE
1DQhxzGQtz5pTkb6oUPR6c7RUGpRuKqXUr
bc1q0003eghztjmtzd7urfu2dja56kmylufwr3yzxx
32qY3LeVf2tnzd15WtwduvwoSvNJiSH5Xm

Blockchain Meets Cyber Kill Chain



RECONNAISSANCE
- Infostealer
- Network access
- Scanning Tools
- Pentesters

WEAPONIZATION
- Botnets
- Exploit kits
- Malware

DELIVERY
- Phishing kits
- Affiliates
- Domains
- Bulletproof hosting

EXPLOITATION
- Exploits
- Brute forcing tools

INSTALLATION
- RATs
- Tools (Cobalt Strike)
- Miners

COMMAND & CONTROL
- C2 Infrastructure
- Stolen creds

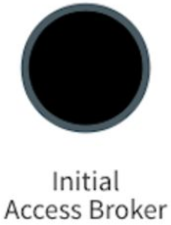
ACTIONS ON OBJECTIVES
- Ransomware
- Cryptojacking
- Data encryption/ exfiltration
- Account takeover

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

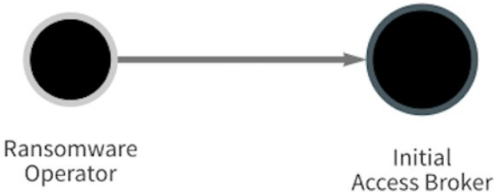
Lockheed-Martin
Cyber Kill Chain

Identify the ‘Who’ and ‘How’

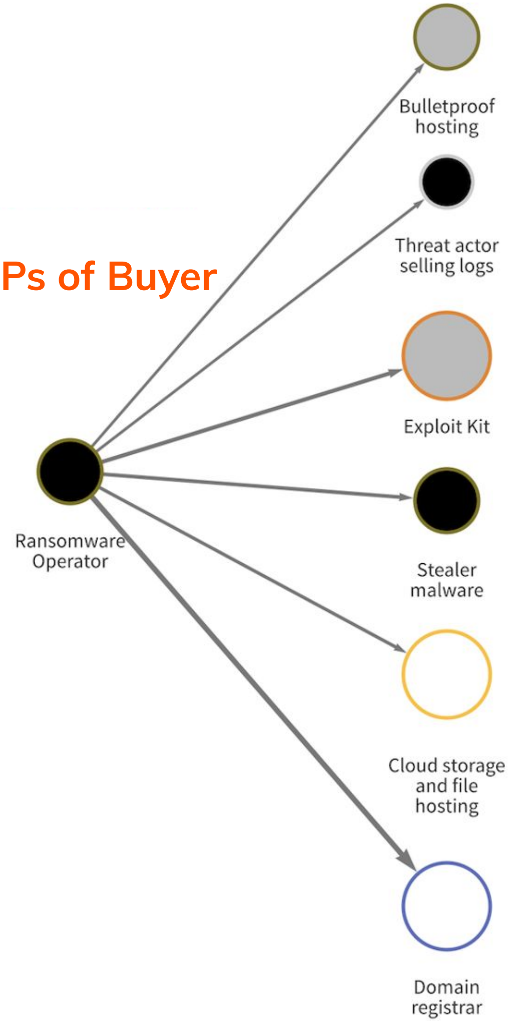
Selling Access



Buyer Identified



TTPs of Buyer

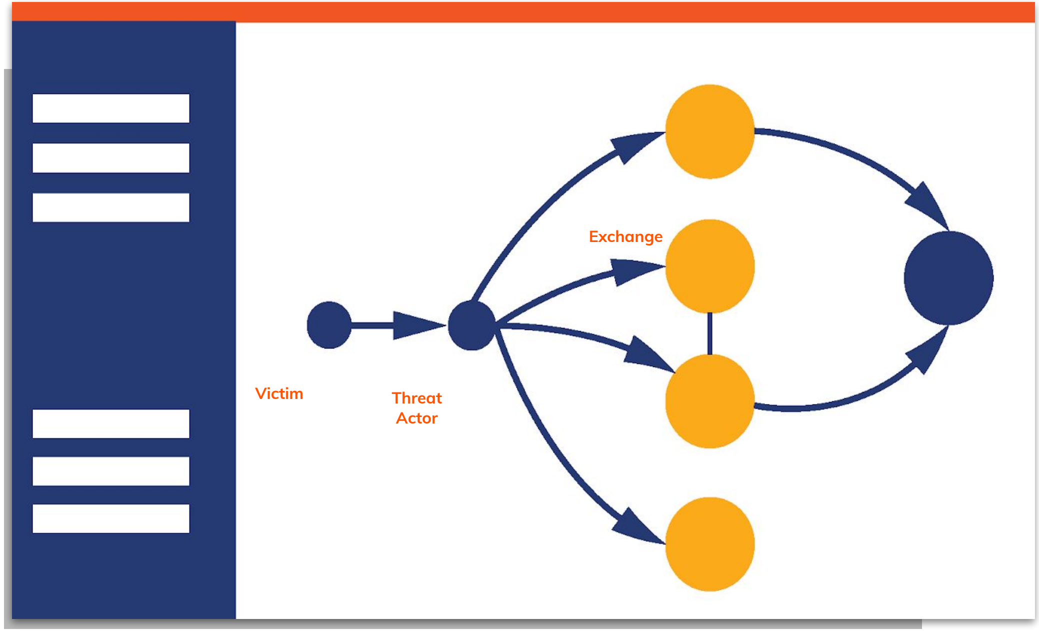


Role of Exchanges

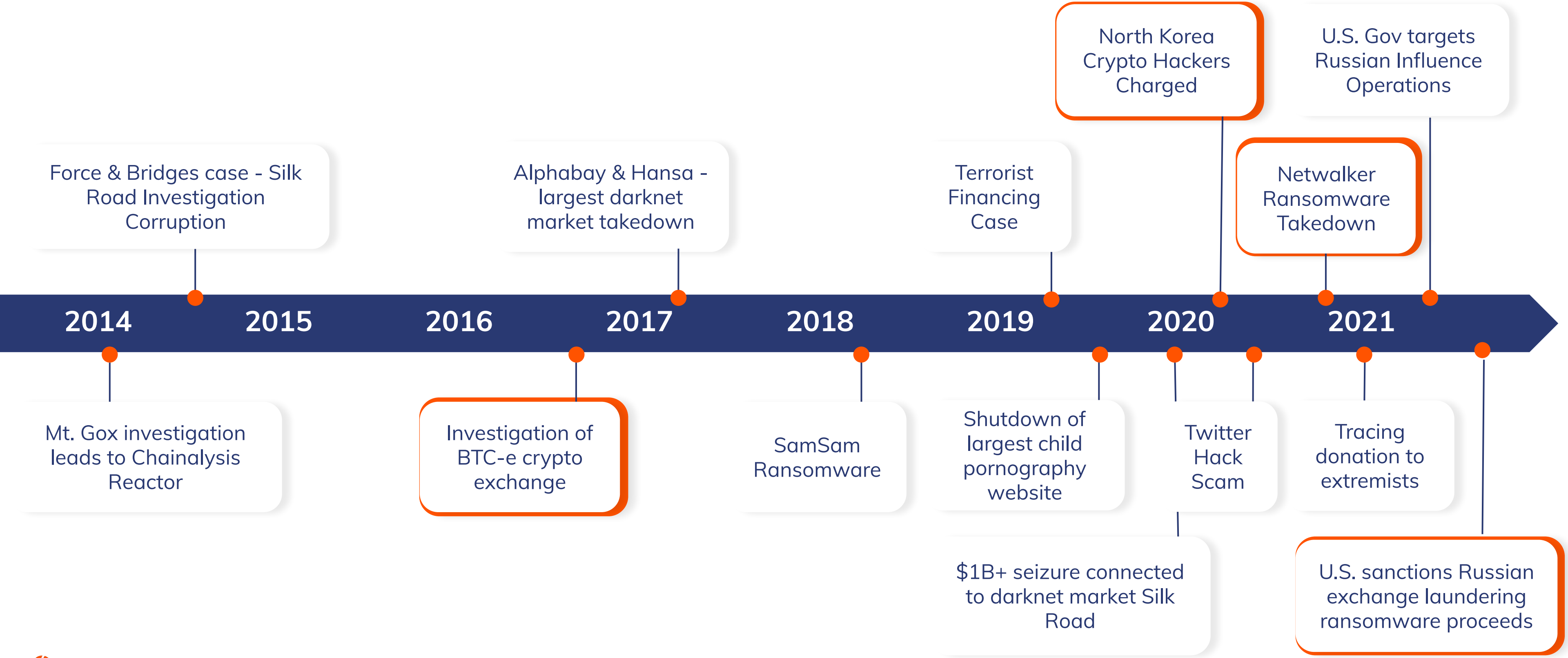
Financially-motivated cyber criminals eventually need to move their crypto into fiat currency.

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

Exchanges are cryptocurrency services that play vital roles in attributing and disrupting the ransomware supply chain.



Attribution & Disruption in Action



2014 2015 2016 2017 2018 2019 2020 2021

Mt. Gox investigation leads to Chainalysis Reactor

Force & Bridges case - Silk Road Investigation Corruption

Investigation of BTC-e crypto exchange

Alphabay & Hansa - largest darknet market takedown

SamSam Ransomware

Terrorist Financing Case

Shutdown of largest child pornography website

North Korea Crypto Hackers Charged

$1B+ seizure connected to darknet market Silk Road

Twitter Hack Scam

Netwalker Ransomware Takedown

Tracing donation to extremists

U.S. Gov targets Russian Influence Operations

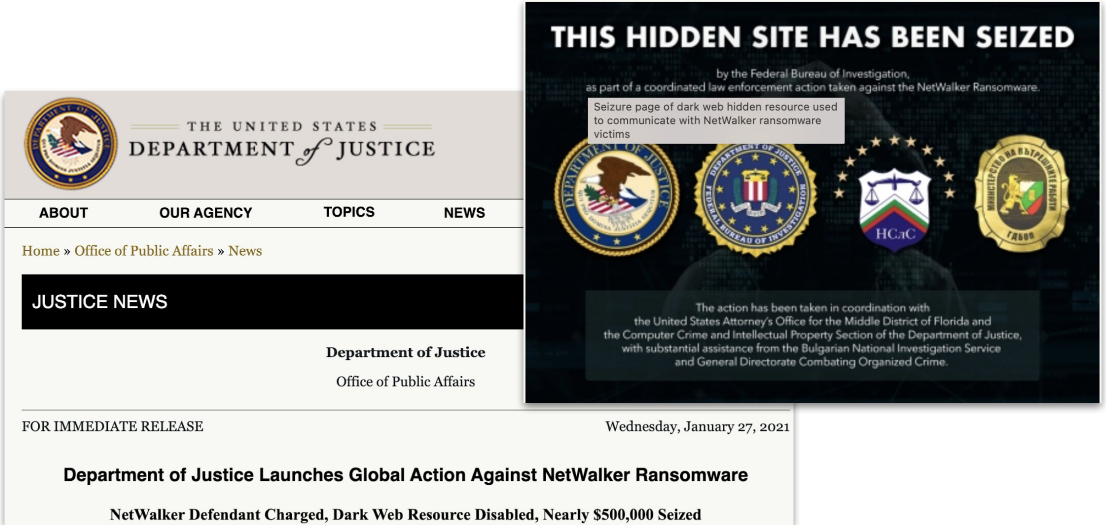
U.S. sanctions Russian exchange laundering ransomware proceeds

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

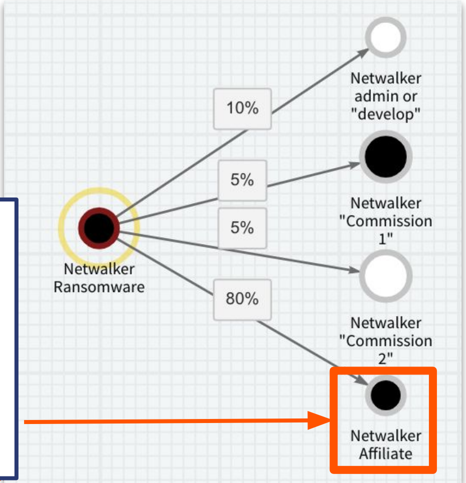
THIS HIDDEN SITE HAS BEEN SEIZED

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 are responsible for finding 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.



During a ransomware event

Payment Made

A ransomware payment is made by or on behalf of a victim in response to an attack

Tracked by investigators

Professional investigators follow the money and track attempted laundering

Criminal attempts to cash out

The threat actor moves funds to an exchange we work with regularly

Chainalysis alerts exchange

Chainalysis representative alerts exchange that a live ransomware payment has landed in their system to stop the movement of funds

Compliance actions taken

The compliance team takes whatever actions their compliance team deems correct. OFAC guidance is to contact law enforcement immediately and report to OFAC.

Ransomware disincentivized

The profitability of ransomware schemes is reduced. We make it much more difficult for criminals to launder their ill gotten gains.

Thank you!
Questions?

Chainalysis.com

brian.carter@chainalysis.com