Chainalysis builds trust in cryptocurrency

Growing partner network: 500+ customers across 60 countries

CRYPTOCURRENCY BUSINESSES

LAW ENFORCEMENT & REGULATORS

FINANCIAL INSTITUTIONS
Chainalysis maps addresses to entities

What you see on the blockchain

What you see in Chainalysis

Services can have thousands to tens of millions of addresses
Attribution & Disruption in Action

- Force & Bridges case - Silk Road Investigation Corruption
- Alphabay & Hansa - largest darknet market takedown
- Terrorist Financing Case
- Netwalker Ransomware Takedown
- North Korea Crypto Hackers Charged
- U.S. Gov targets Russian Influence Operations
- Mt. Gox investigation leads to Chainalysis Reactor
- Investigation of BTC-e crypto exchange
- SamSam Ransomware
- Shutdown of largest child pornography website
- Twitter Hack Scam
- Tracing donation to extremists
- $1B+ seizure connected to darknet market Silk Road
- U.S. sanctions Russian exchange laundering ransomware proceeds

Proprietary and Confidential
Ransomware Trends

**Increase** in overall Ransomware revenue

**Increase** in average ransom payment demanded

**Increase** in unique threat actors engaging in the ransomware ecosystem
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
Blockchain Meets Cyber Kill Chain

**Threat actors use cryptocurrency to propel cyber intrusions through each stage of the kill chain**
Prevention: Stay ahead of the threat (and the news)

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

Bulletproof hosting (BPHS)
- Reported as Makop Ransomware (0.04)
- Reported as Medusa Locker Ransomware (0.02)
- Reported as Globelmimposter Ransomware (0.08)
- Reported as Mamba Ransomware

MaaS and Exploit Kits
- Reported as Doppelpaymer Ransomware (0.05)
- Reported as STOP (DJVU) Ransomware (1.75)
- Reported as Philadelphia Ransomware (0.04)
- Reported as Bitpaymer Ransomware
Initial Access Brokers

- Conti Ransomware
- Egregor Ransomware
- Initial Access Broker
- NotWalker Affiliate
- Business Email Compromise actor
- Vice Society Ransomware

Paired 3/18/2021
Access pass derived through Exchange vuln

- Exchange 1
- Victim
- Black Kingdom Ransomware

P2P

Exchange 2
Affiliates’ divided loyalty

- Receiving Exposure
  - Lockbit ransomware
  - Reported as Doppelpaymer Ransomware
  - NetWalker...
  - Reported as Crysis-Dharma Ransomware

- Conti Ransomware
  - Affiliate I

- Vice Society Ransomware
  - Affiliate II

- NetWalker - Mailto Ransomware
  - Affiliate III

- Darkside Ransomware
Mixers & Monero

Admin panel:
- Full ajax, no page reloads. Convenient notifications about everything.
- Automatic generation of builds.
- Automatic issuance of decryters.
- Knock out bots with detailed statistics on the company’s performance.
- Sub-accounts with access control by 9 parameters.
- Live chat and support.
- Calls at our expense.

Leak site:
- A blog that is actually visited. Stable visits and media coverage.
- Hidden publications.
- Phased publication of target data.
- and many other functionalities.

Screenshot of the DarkSide admin’s Exploit.in forum post seeking affiliates for DarkSide 2.0

Screenshot of a REvil /Sodinokibi ransom note demanding payment in Monero
Identify the ‘Who’ and ‘How’

**Selling Access**

- Initial Access Broker

**Buyer Identified**

- Ransomware Operator
- Initial Access Broker

**TTPs of Buyer**

- Bulletproof hosting
- Threat actor selling logs
- Exploit Kit
- Ransomware Operator
- Stealer malware
- Cloud storage and file hosting
- Domain registrar
How does it work?

Take an address 13AM4VW2dhx...

What other addresses does it control? Where does the wallet send or source its funds?

What about the “Who”?

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

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.
Case Study
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
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

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