Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf22

Understanding the Latest Ransomware Threats To Protect Your Organization

SEC1514B

Brett Stone-Gross, Ph.D.
Director of Threat Intelligence | Zscaler

Shannon Davis
Global Staff Security Strategist | Splunk

splunk> .conf22

Brett Stone-Gross, Ph.D.

Director of Threat Intelligence | Zscaler

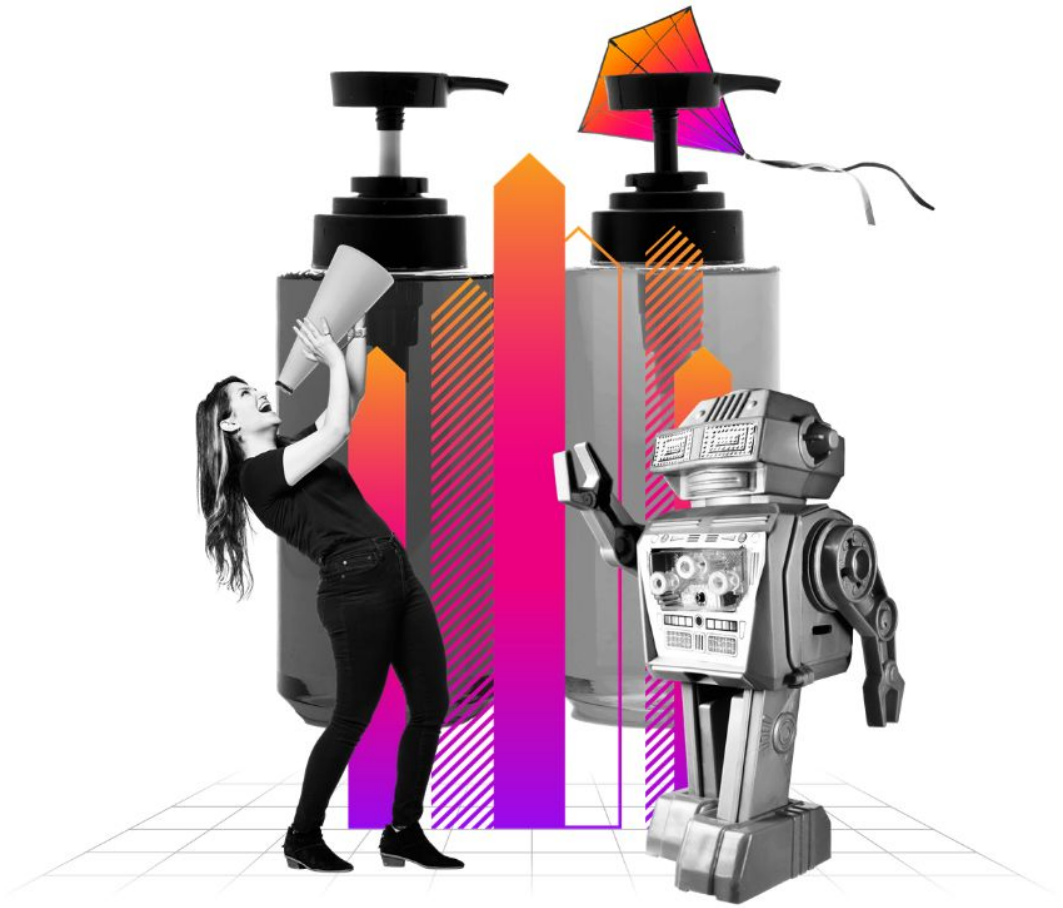
Shannon Davis

Global Staff Security Strategist
SURGe at Splunk

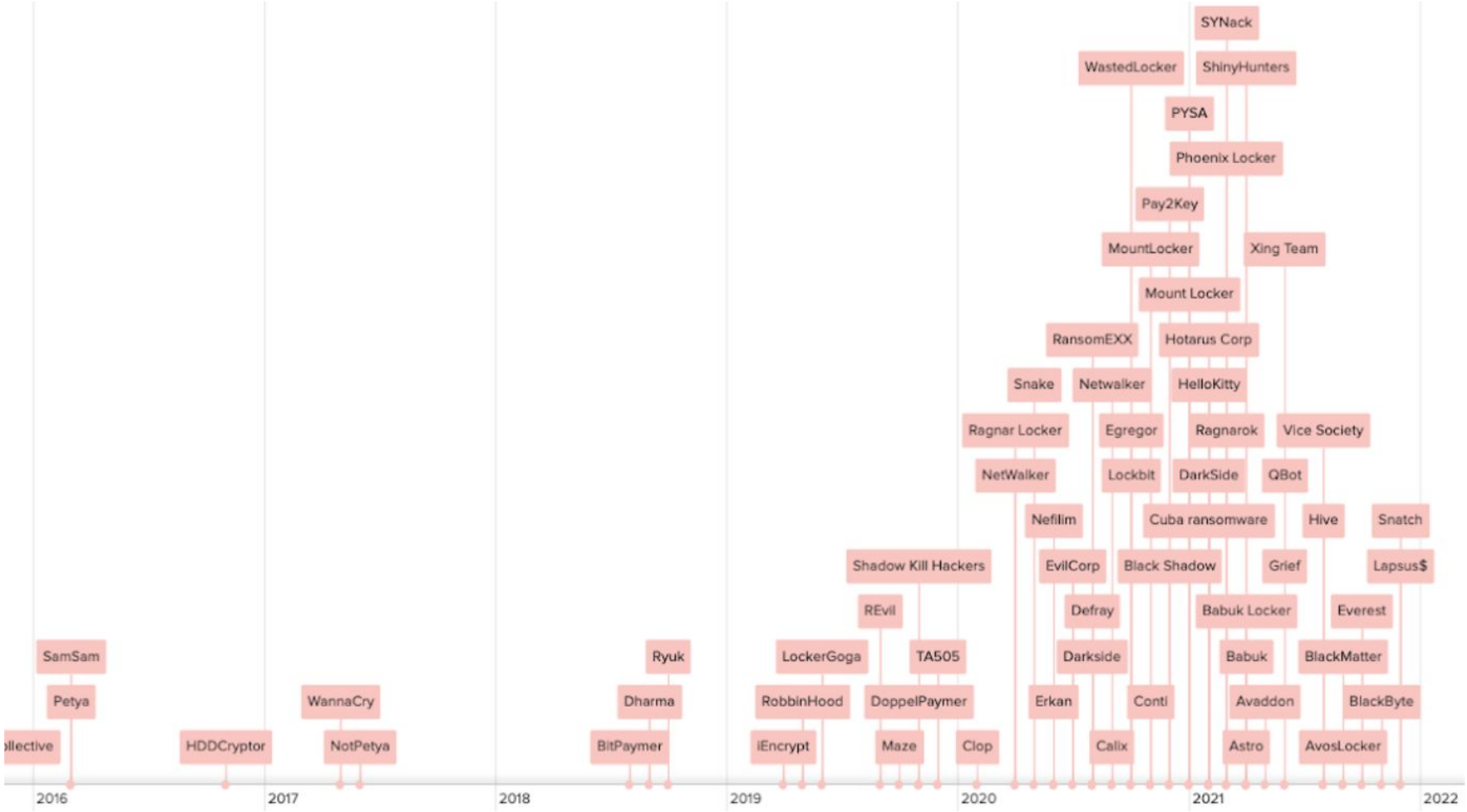
splunk> .conf22

Agenda

- Ransomware Today
- Ransomware Leaks
- Obfuscation, Evasion, Delivery
- Gone But Not Forgotten
- Helpful Advice



Ransomware Today



splunk> .conf22

High Profile Incidents

Increased scrutiny and pressure at the highest levels of government

- Darkside attack against Colonial Pipeline
- REvil attacks
  - Kaseya supply-chain attack
  - JBS meat processor

Nation-state “ransomware” attacks

- PartyTicket
  - Used in conjunction with HermeticWiper attacks at the beginning of the Ukraine invasion
  - Likely developed as a decoy

Ransomware is Fast!

Median time taken to encrypt 100K files

Family	Median Duration
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
Average of the median	**00:42:52**

Ransomware Leaks

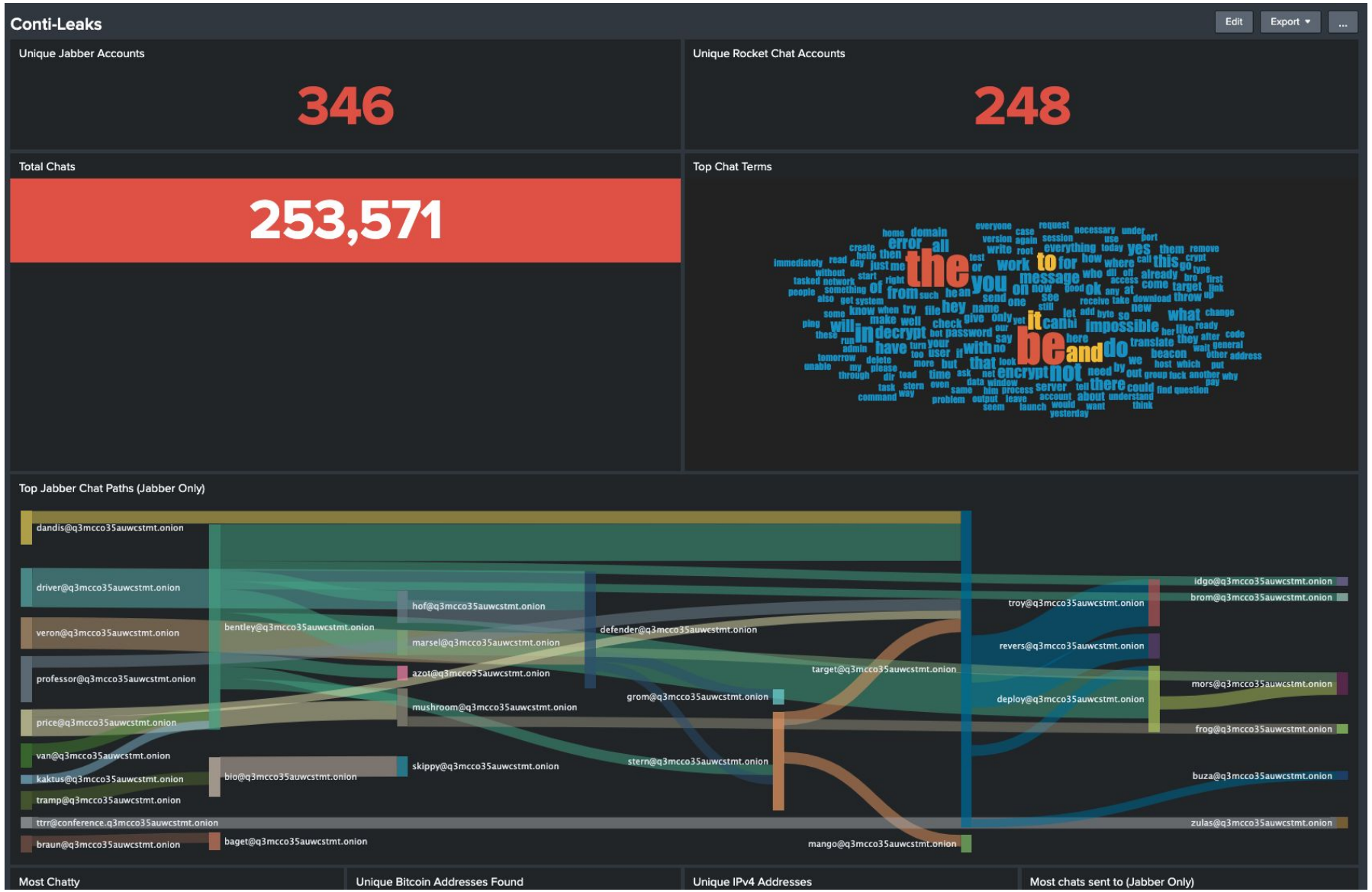
Conti Leaks

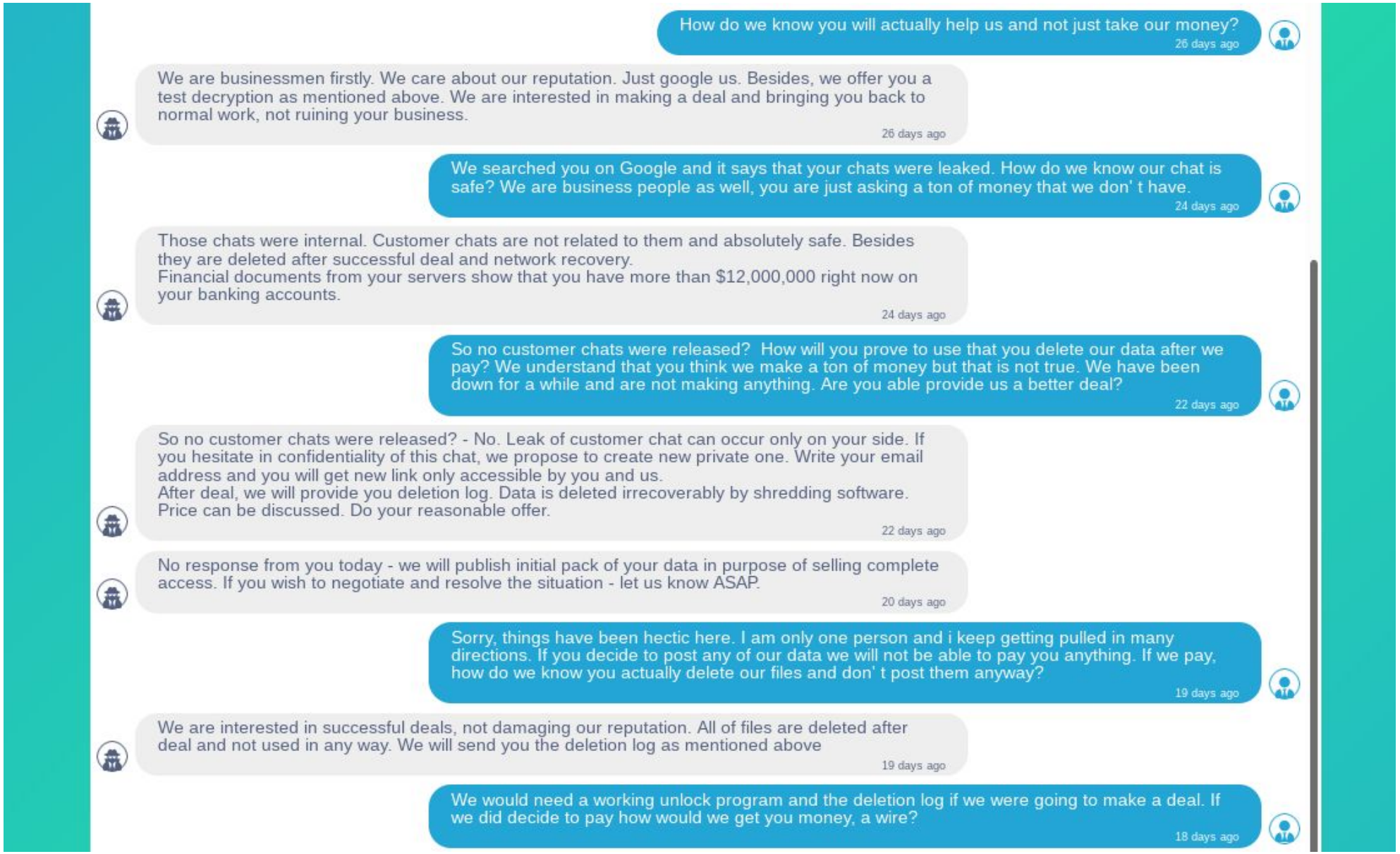
Chat leaks

- Nearly two years of internal communications leaked
  - June 2020 to March 2022
- Logs include a variety of information
  - Targeted U.S. hospitals in October 2020
  - Potential connections with Russian law enforcement / intelligence
  - Attack methods and tools

Source code and documentation

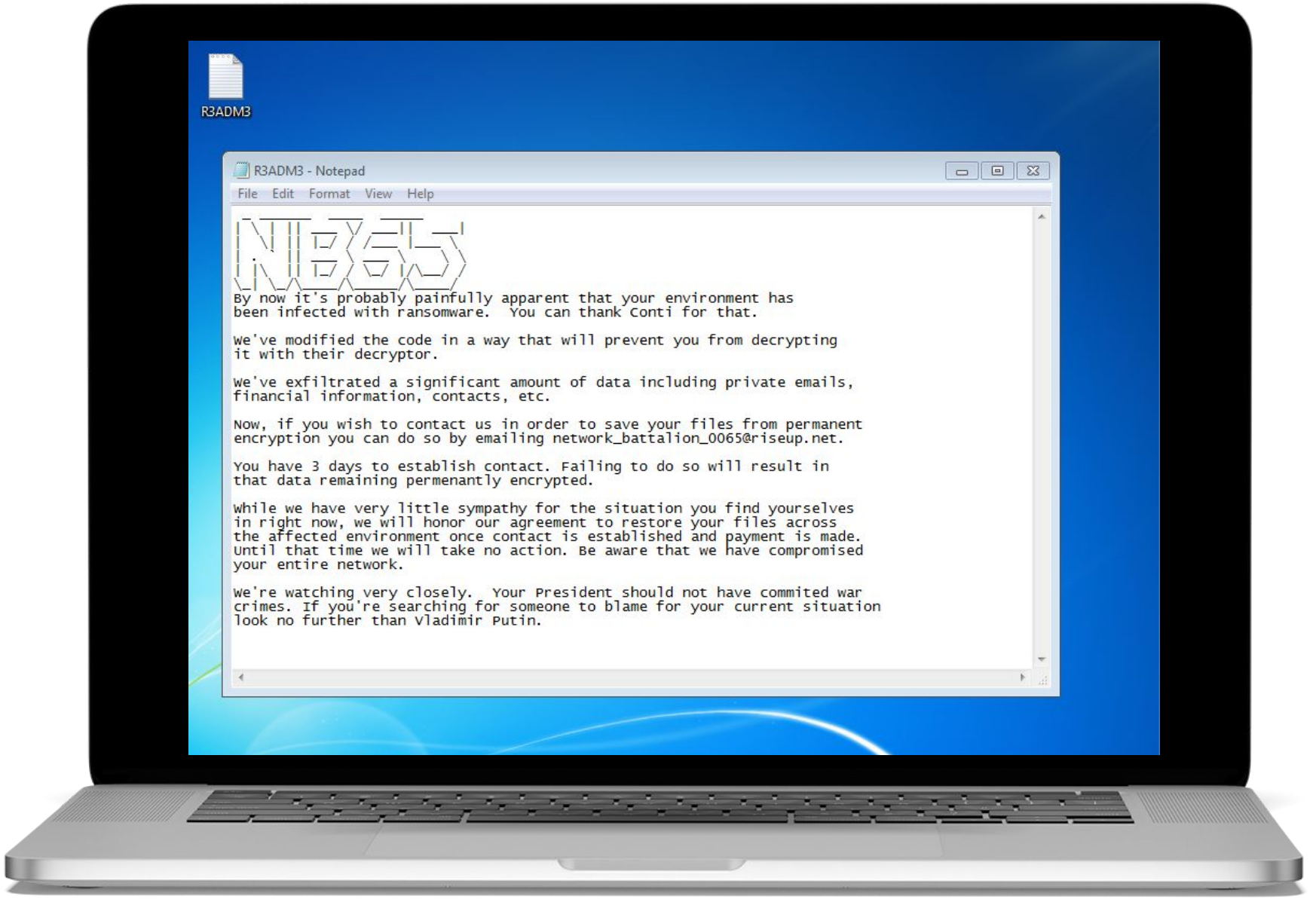
- Admin panels and screenshots
- Conti ransomware v2 and v3 leaked
  - A new version was released in January, but that source code has not been leaked





splunk> .conf22

Conti Forks

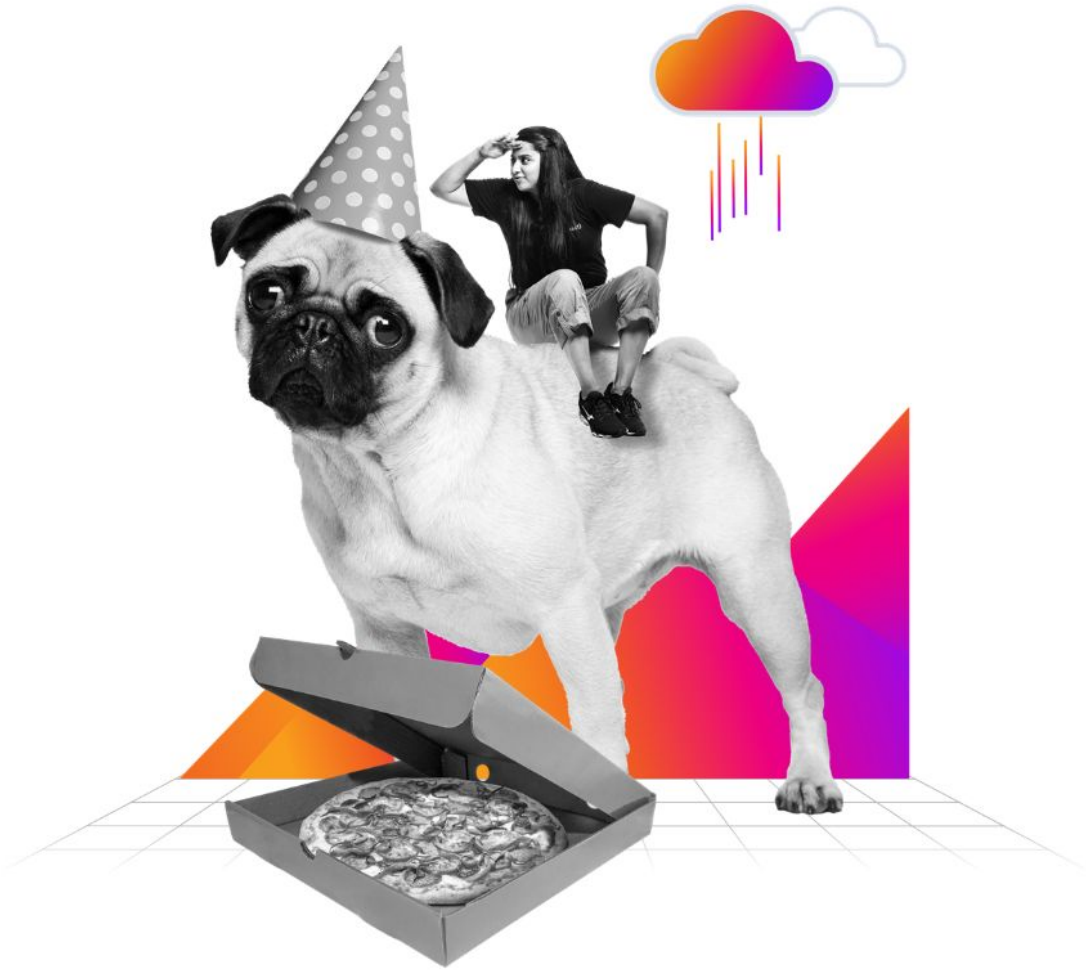


Babuk Leak

The leaked source code was forked

- Modified encryption algorithms (ECC Curve25519 to RSA)
- Rebranding
  - Rook
  - NightSky
  - Pandora
- Added complex packing and obfuscation

Obfuscation, Evasion, Delivery



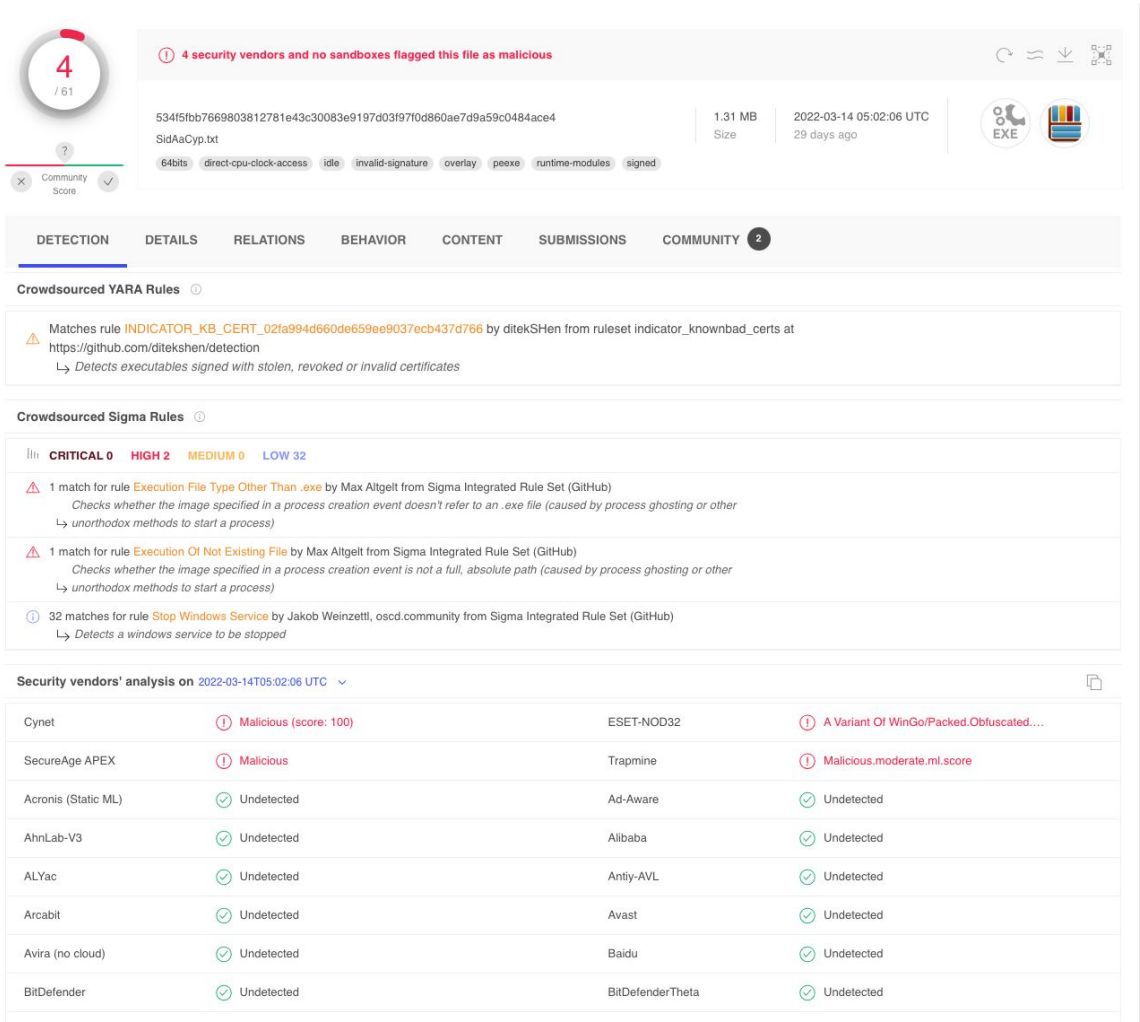
Complex Malware Obfuscation Techniques

Packers
- VMProtect

String obfuscation
- ADVObfuscator

Control flow obfuscation
- LLVM

Antivirus Evasion (BlackByte)



splunk> .conf22

New Delivery Techniques

Exploitation of public vulnerabilities

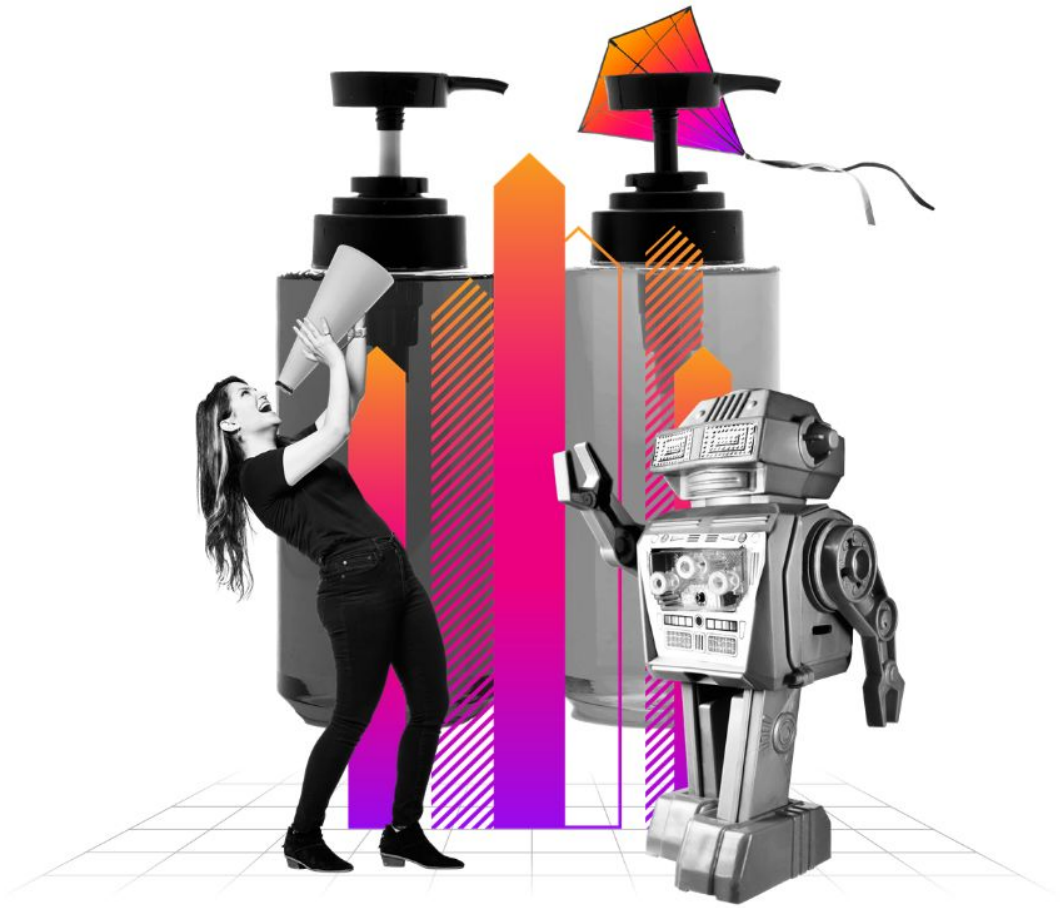
- Atlassian Confluence RCE vulnerability (CVE-2021-26084)
- Log4Shell attacks against applications that utilize Log4J
- Microsoft Exchange ProxyLogon vulnerabilities
- PrintNightmare

Misconfigured / poorly configured devices

- QNAP Network Attached Storage (NAS) devices

Packages containing malicious USB devices

- BadUSB / Bad Beetle USB



Gone But Not Forgotten

splunk> .conf22

Law Enforcement Actions

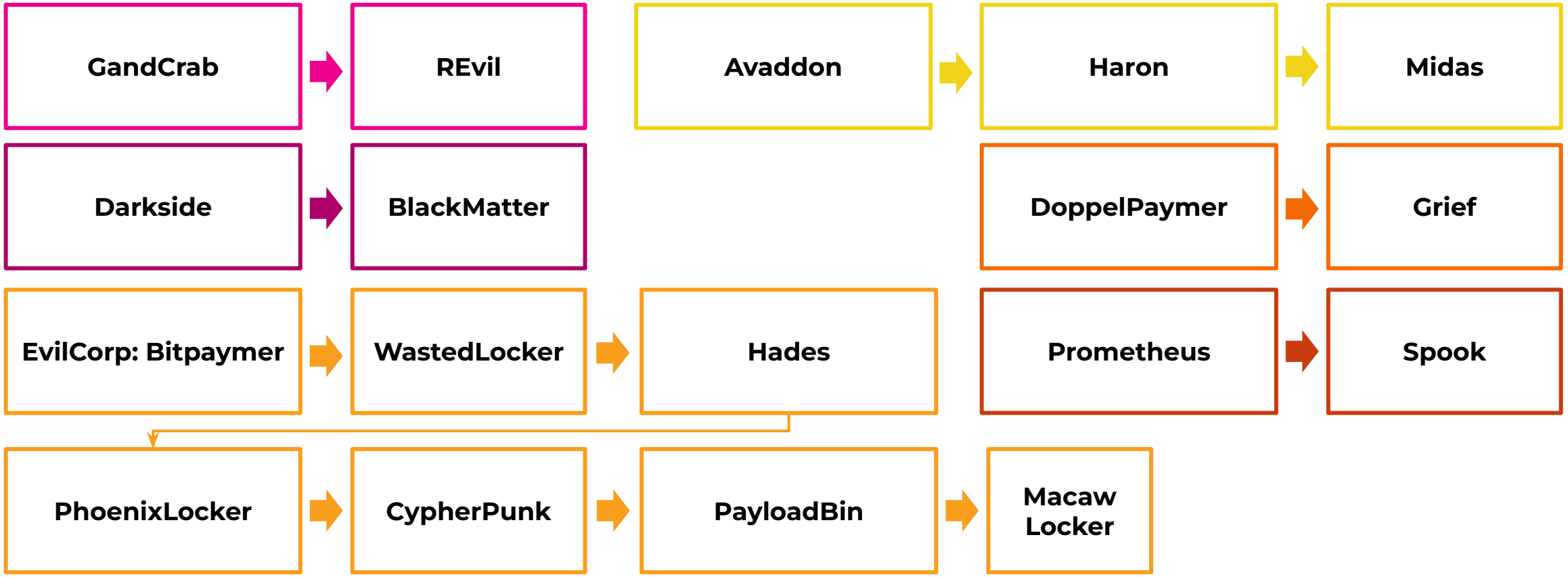
Arrests
- Maze/Egregor
- Netwalker
- REvil

Infrastructure disruption / seizures / takedowns
- DarkSide
- REvil

Sanctions
- EvilCorp

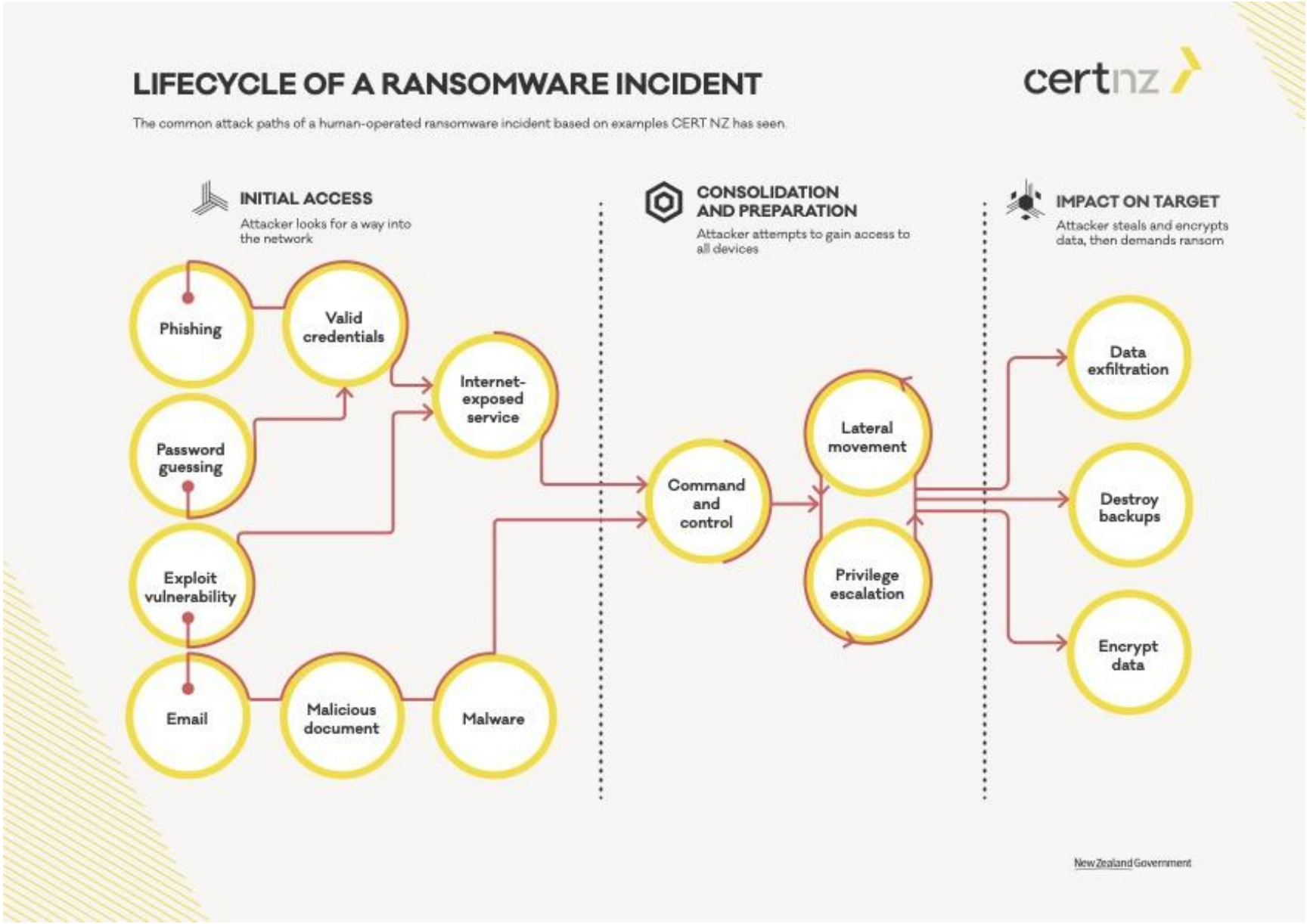
Law Enforcement Action Response

Ransomware “rebranding”



Helpful Advice

splunk> .conf22



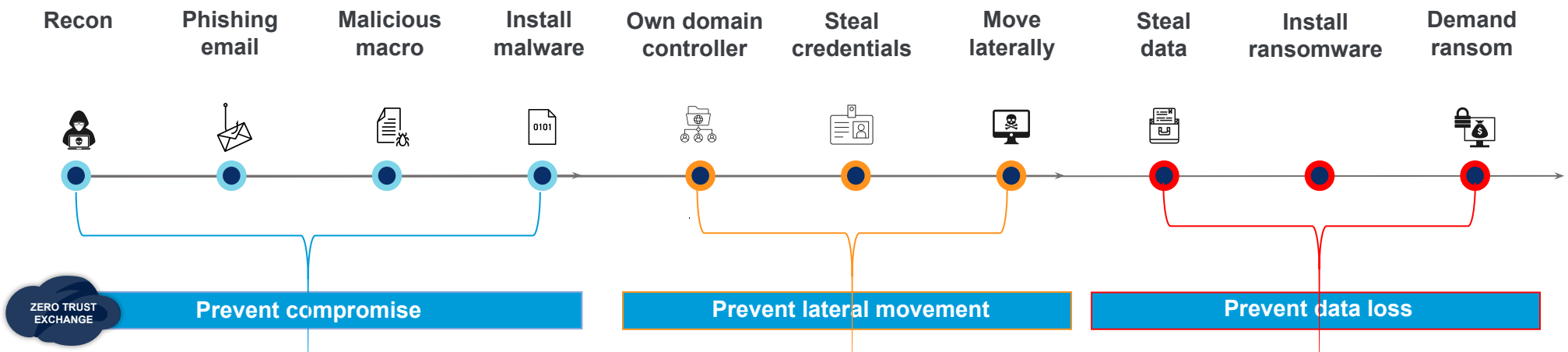
https://research.splunk.com/

ransomware

170+ Results Found

Zscaler Zero Trust Exchange

Designed to offer comprehensive protection against sophisticated attacks



Block threats before they reach you

Eliminate the attack surface
Private apps are invisible to the internet, can't be discovered and attacked

Inline content inspection (SSL)
Proprietary proxy architecture, sophisticated content inspection engine with AI-powered cloud-effect

Protect public cloud data
Fix misconfigurations to prevent unauthorized access to cloud resources

Stop the spread of infection (LAN/WAN)

User to app segmentation
Connects an authenticated user and device to an authorized app without bringing the user on the network

Workload to workload segmentation
Uses software identity to allow or block workload communications in hybrid and multi-cloud environments

Prevent data loss to the internet

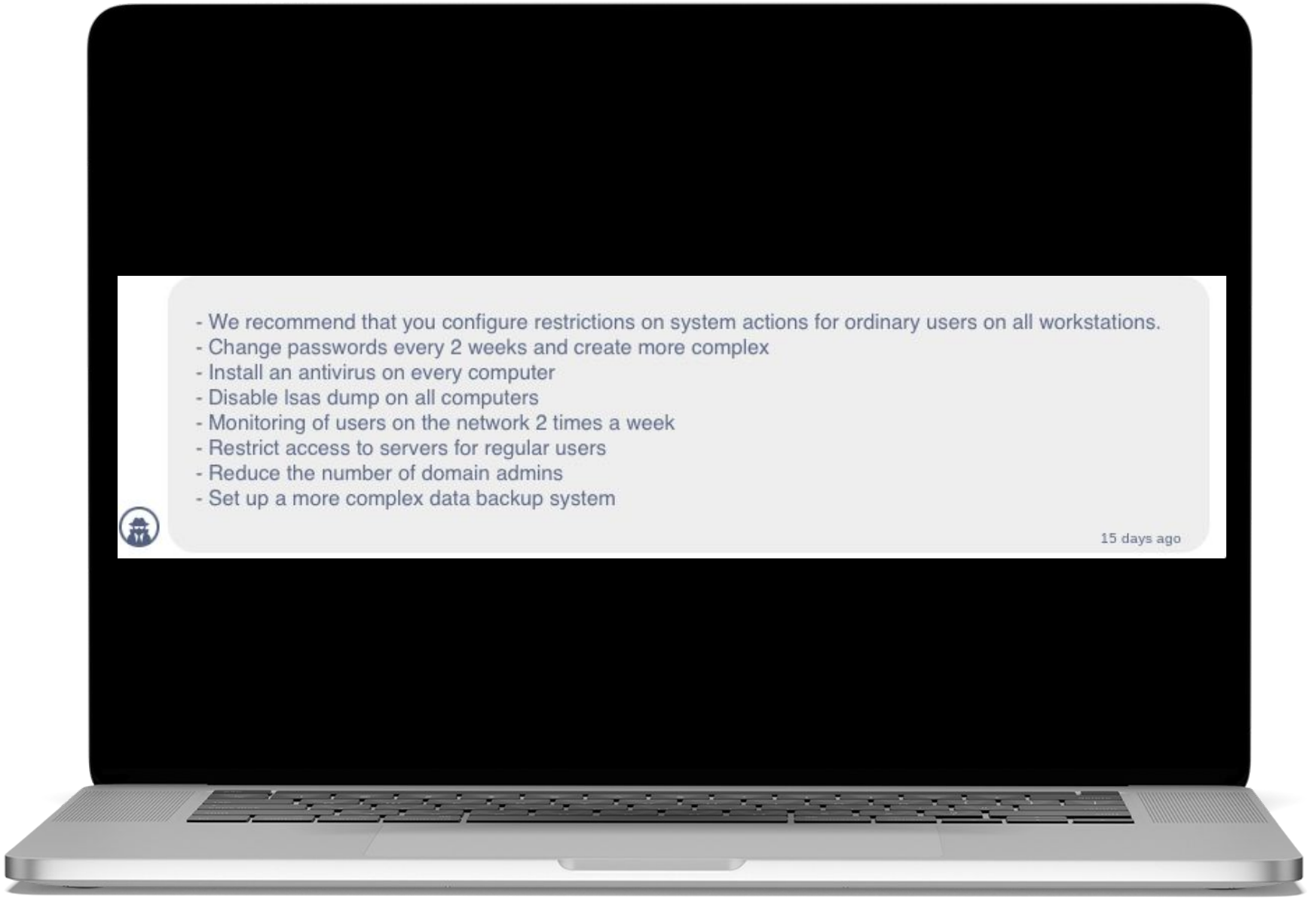
Inline content inspection (SSL)
Proprietary proxy architecture with Inline DLP policies for users, servers, workloads, IoT and OT Systems

Innovative data classification engine
with advanced exact data match, document fingerprinting capabilities

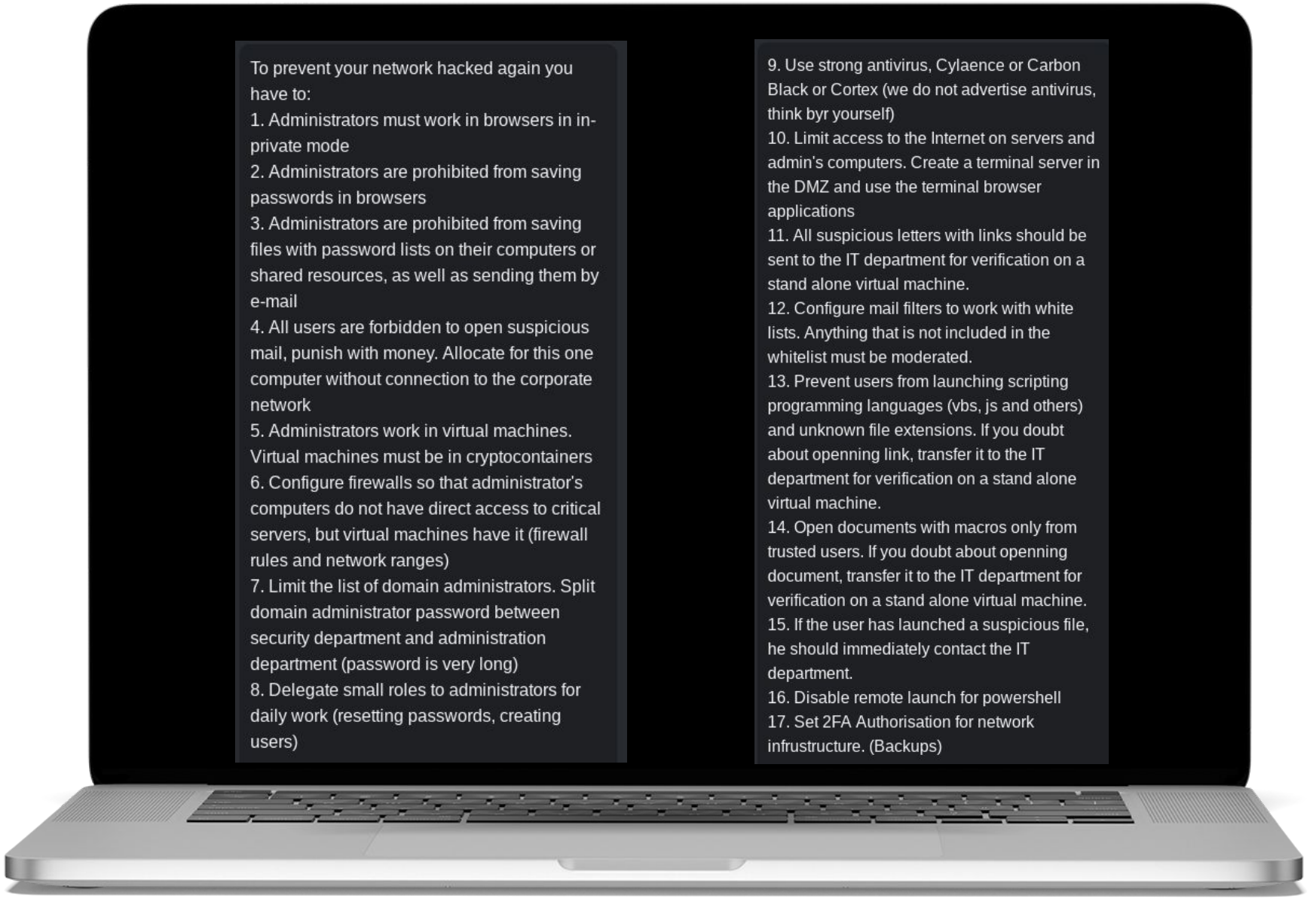
Secure SaaS data (CASB)
Prevent oversharing and discover sensitive data at rest

splunk> .conf22

Advice From Conti



Advice From the DarkSide



Shannon Davis
@DrShannon2000
shannon@splunk.com

Brett Stone-Gross
@pushecx
bstonegross@zscaler.com

splunk> .conf22

Thank You

splunk> .conf22