

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, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

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

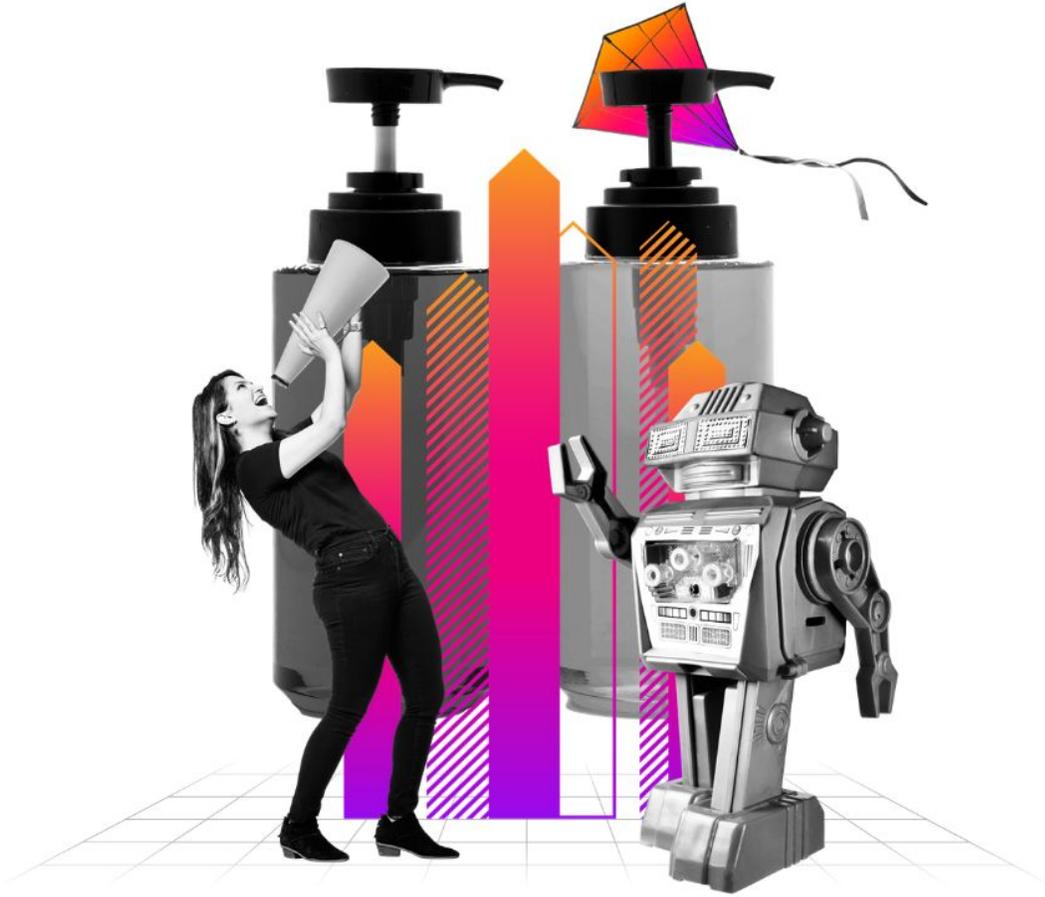
Global Staff Security Strategist
SURGe at Splunk

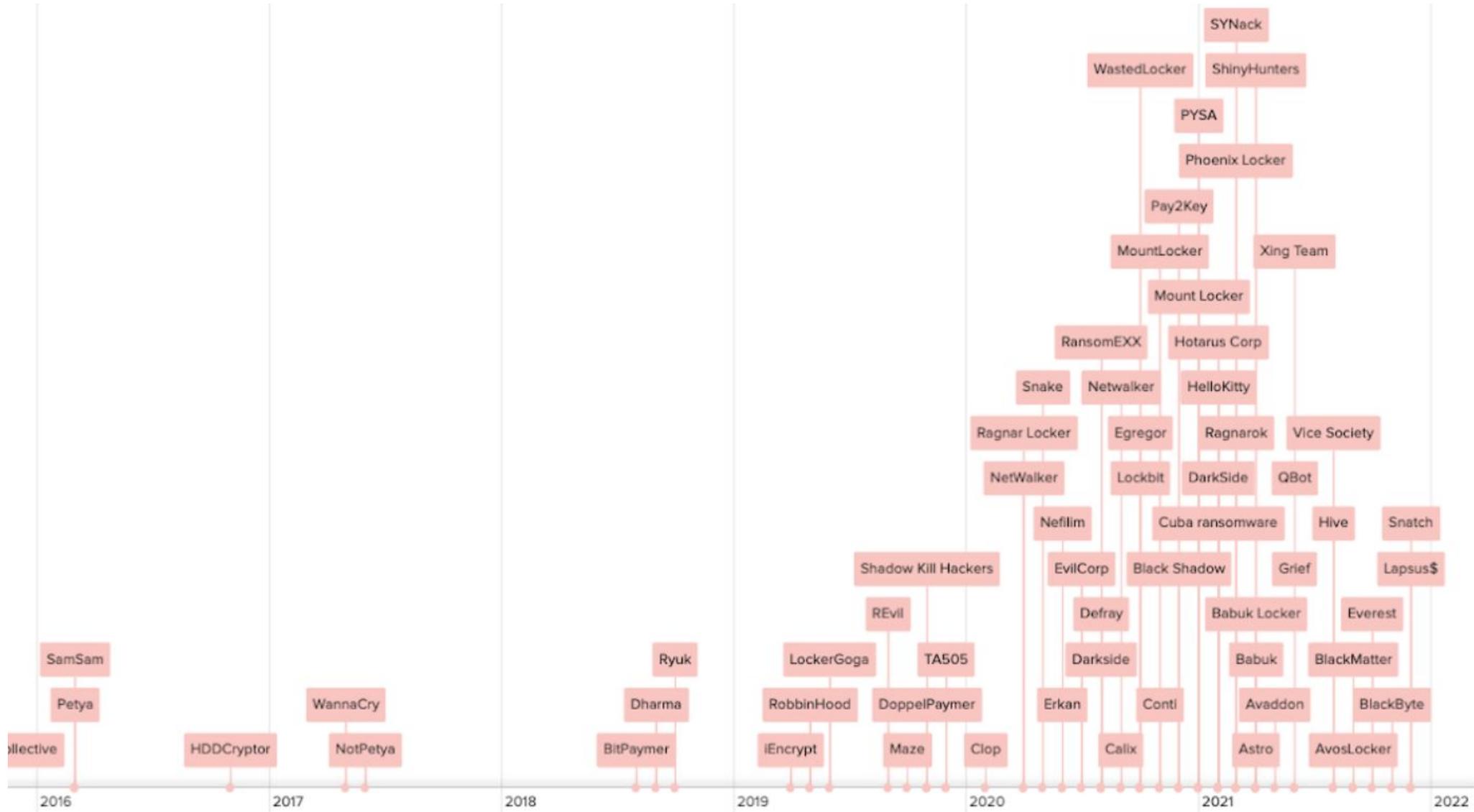
Agenda

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



Ransomware Today





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



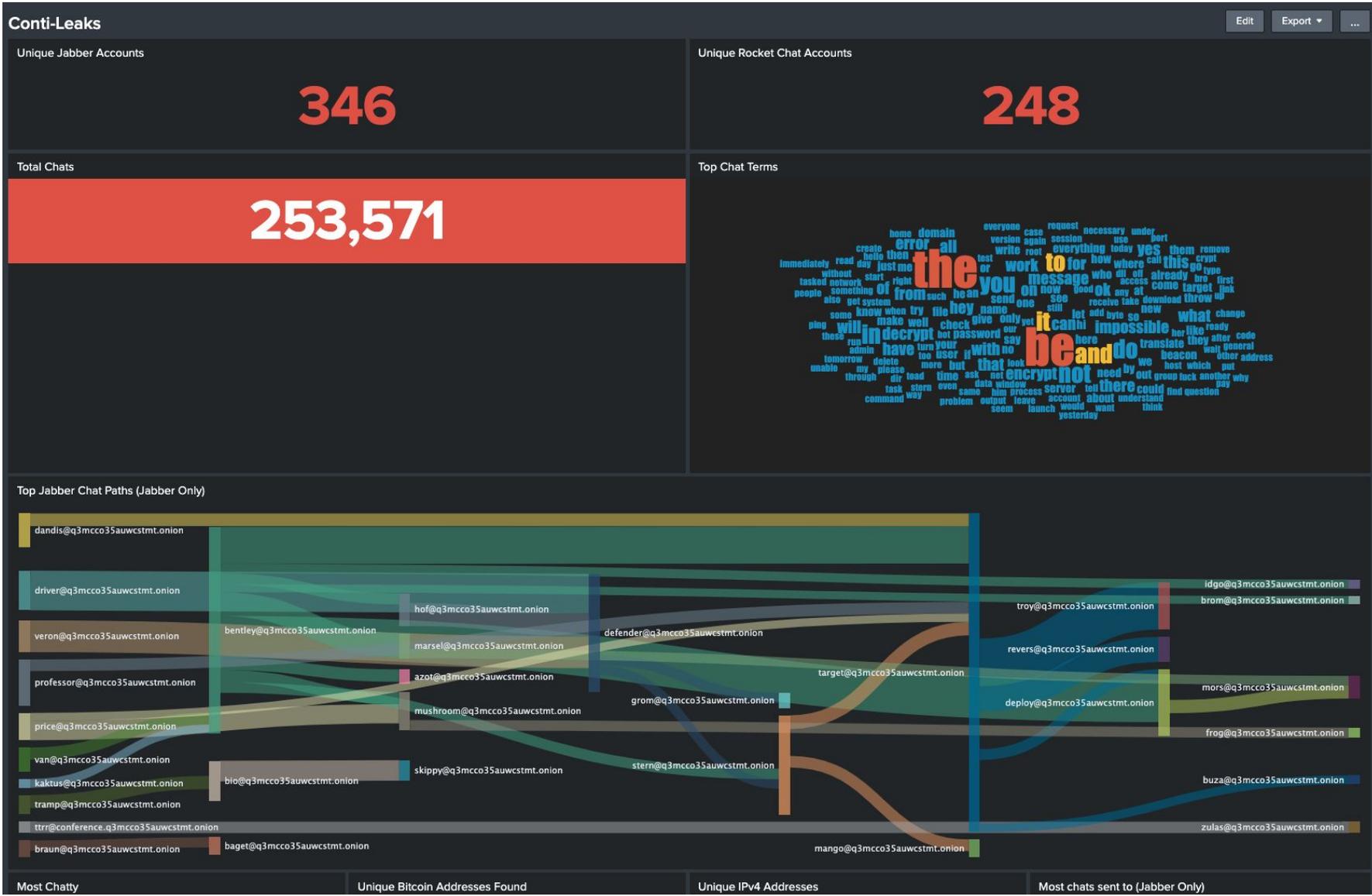
Conti Leaks

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



How do we know you will actually help us and not just take our money?

26 days ago



We are businessmen firstly. We care about our reputation. Just google us. Besides, we offer you a test decryption as mentioned above. We are interested in making a deal and bringing you back to normal work, not ruining your business.

26 days ago



We searched you on Google and it says that your chats were leaked. How do we know our chat is safe? We are business people as well, you are just asking a ton of money that we don't have.

24 days ago



Those chats were internal. Customer chats are not related to them and absolutely safe. Besides they are deleted after successful deal and network recovery. Financial documents from your servers show that you have more than \$12,000,000 right now on your banking accounts.

24 days ago



So no customer chats were released? How will you prove to use that you delete our data after we pay? We understand that you think we make a ton of money but that is not true. We have been down for a while and are not making anything. Are you able provide us a better deal?

22 days ago



So no customer chats were released? - No. Leak of customer chat can occur only on your side. If you hesitate in confidentiality of this chat, we propose to create new private one. Write your email address and you will get new link only accessible by you and us. After deal, we will provide you deletion log. Data is deleted irrecoverably by shredding software. Price can be discussed. Do your reasonable offer.

22 days ago



No response from you today - we will publish initial pack of your data in purpose of selling complete access. If you wish to negotiate and resolve the situation - let us know ASAP.

20 days ago



Sorry, things have been hectic here. I am only one person and i keep getting pulled in many directions. If you decide to post any of our data we will not be able to pay you anything. If we pay, how do we know you actually delete our files and don't post them anyway?

19 days ago



We are interested in successful deals, not damaging our reputation. All of files are deleted after deal and not used in any way. We will send you the deletion log as mentioned above

19 days ago

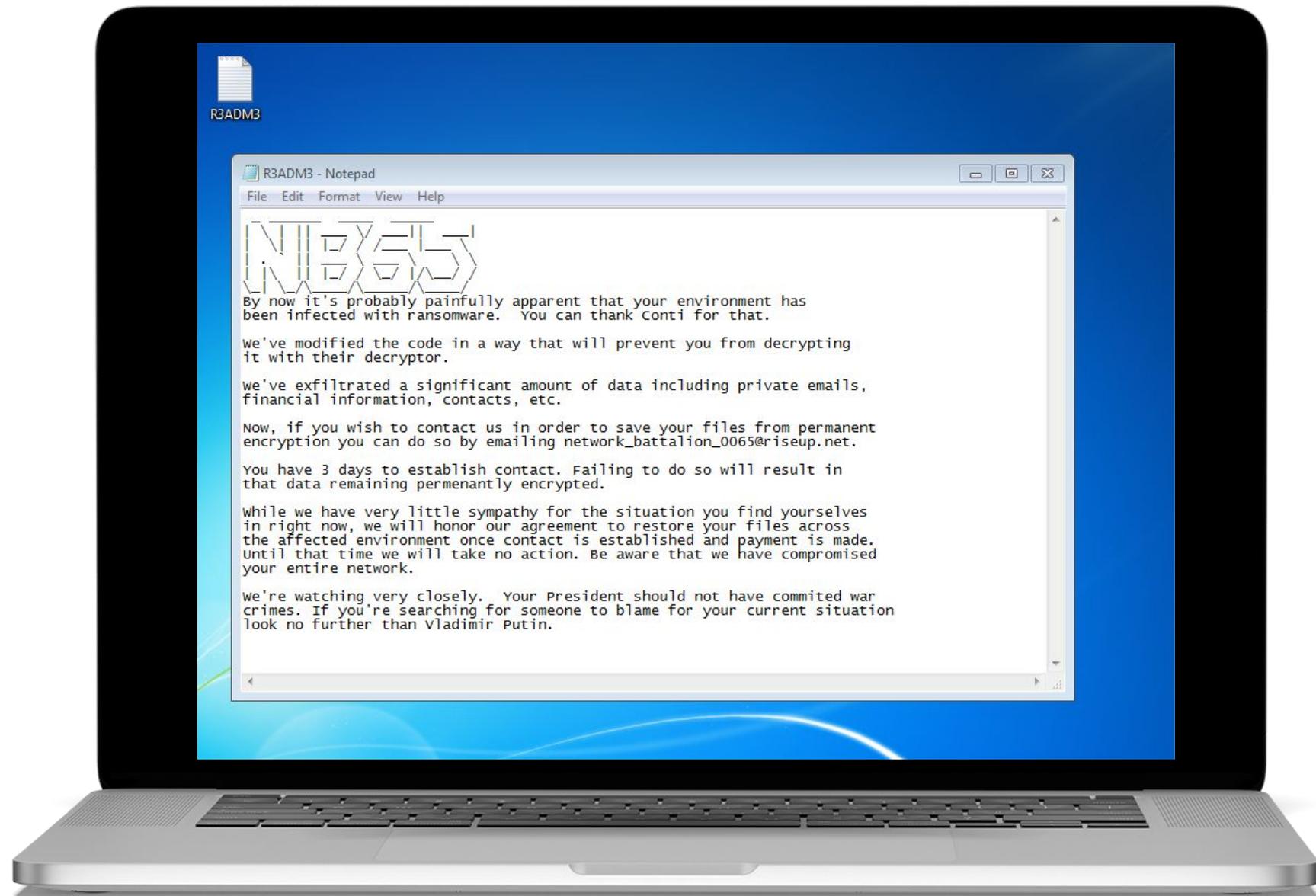


We would need a working unlock program and the deletion log if we were going to make a deal. If we did decide to pay how would we get you money, a wire?

18 days ago



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)

4 / 61

4 security vendors and no sandboxes flagged this file as malicious

534f5fbb7669803812781e43c30083e9197d03f97f0d860ae7d9a59c0484ace4
SidAaCyp.txt

1.31 MB Size | 2022-03-14 05:02:06 UTC 29 days ago

64bits direct-cpu-clock-access idle invalid-signature overlay peexe runtime-modules signed

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR CONTENT SUBMISSIONS COMMUNITY 2

Crowdsourced YARA Rules

Matches rule **INDICATOR_KB_CERT_02fa994d660de659ee9037ecb437d766** by ditekshen from ruleset indicator_knownbad_certs at <https://github.com/ditekshen/detection>
↳ Detects executables signed with stolen, revoked or invalid certificates

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 2 MEDIUM 0 LOW 32

1 match for rule **Execution File Type Other Than .exe** by Max Altgelt from Sigma Integrated Rule Set (GitHub)
Checks whether the image specified in a process creation event doesn't refer to an .exe file (caused by process ghosting or other unorthodox methods to start a process)

1 match for rule **Execution Of Not Existing File** by Max Altgelt from Sigma Integrated Rule Set (GitHub)
Checks whether the image specified in a process creation event is not a full, absolute path (caused by process ghosting or other unorthodox methods to start a process)

32 matches for rule **Stop Windows Service** by Jakob Weinzettl, oscd.community from Sigma Integrated Rule Set (GitHub)
↳ Detects a windows service to be stopped

Security vendors' analysis on 2022-03-14T05:02:06 UTC

Cynet	Malicious (score: 100)	ESET-NOD32	A Variant Of WinGo/Packed/Oblfuscated....
SecureAge APEX	Malicious	Trapmine	Malicious.moderate.ml.score
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected

New Delivery Techniques

Exploitation of public vulnerabilities

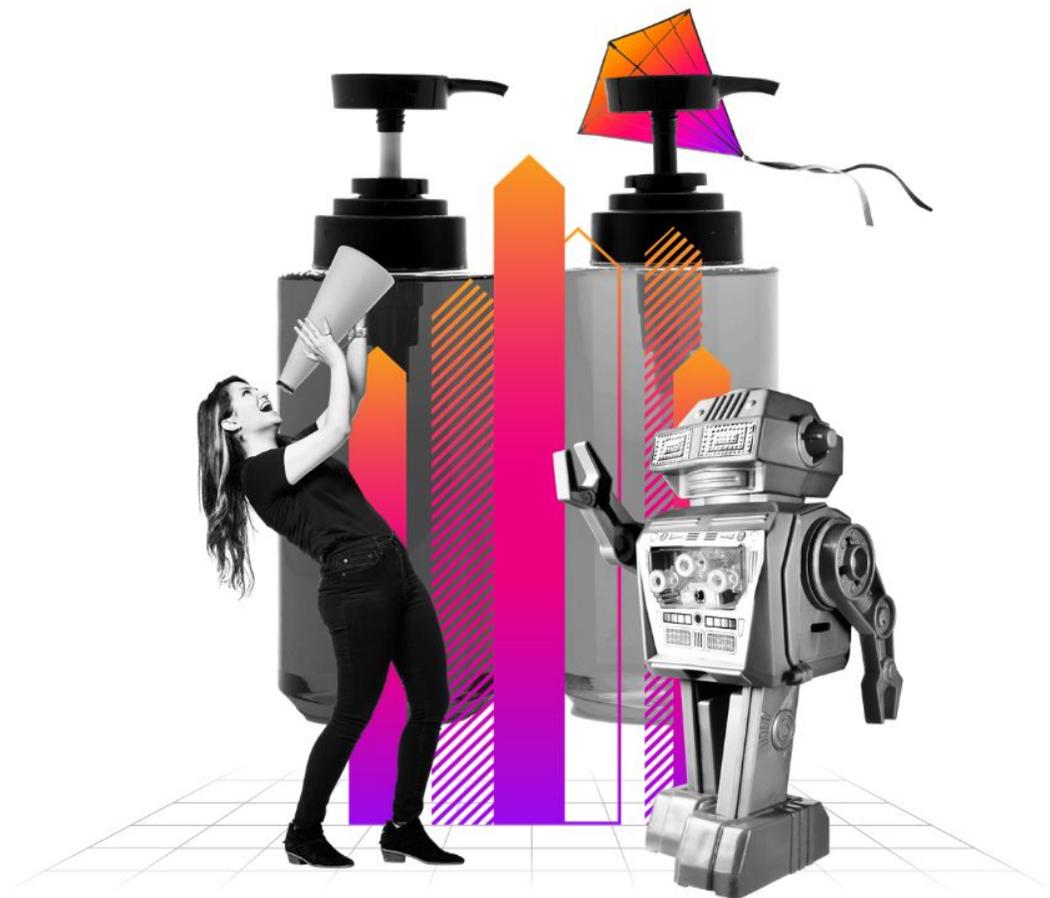
- Atlassian Confluence RCE vulnerability (CVE-2021-26084)
- Log4Shell attacks against applications that utilize Log4J
- Microsoft Exchange ProxyLogon vulnerabilities
- PrintNightmare

Misconfigured / poorly configured devices

- QNAP Network Attached Storage (NAS) devices

Packages containing malicious USB devices

- BadUSB / Bad Beetle USB



Gone But Not Forgotten

Law Enforcement Actions

Arrests

- Maze/Egregor
- Netwalker
- REvil

Infrastructure disruption / seizures / takedowns

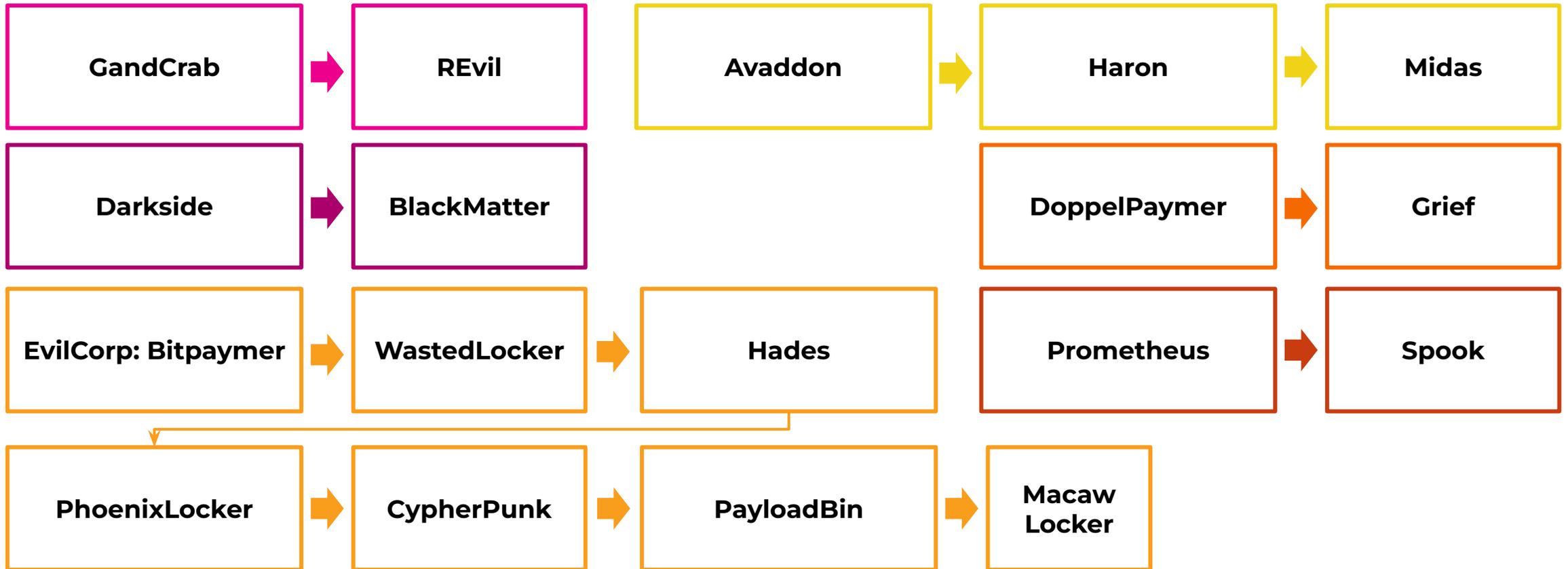
- DarkSide
- REvil

Sanctions

- EvilCorp

Law Enforcement Action Response

Ransomware “rebranding”



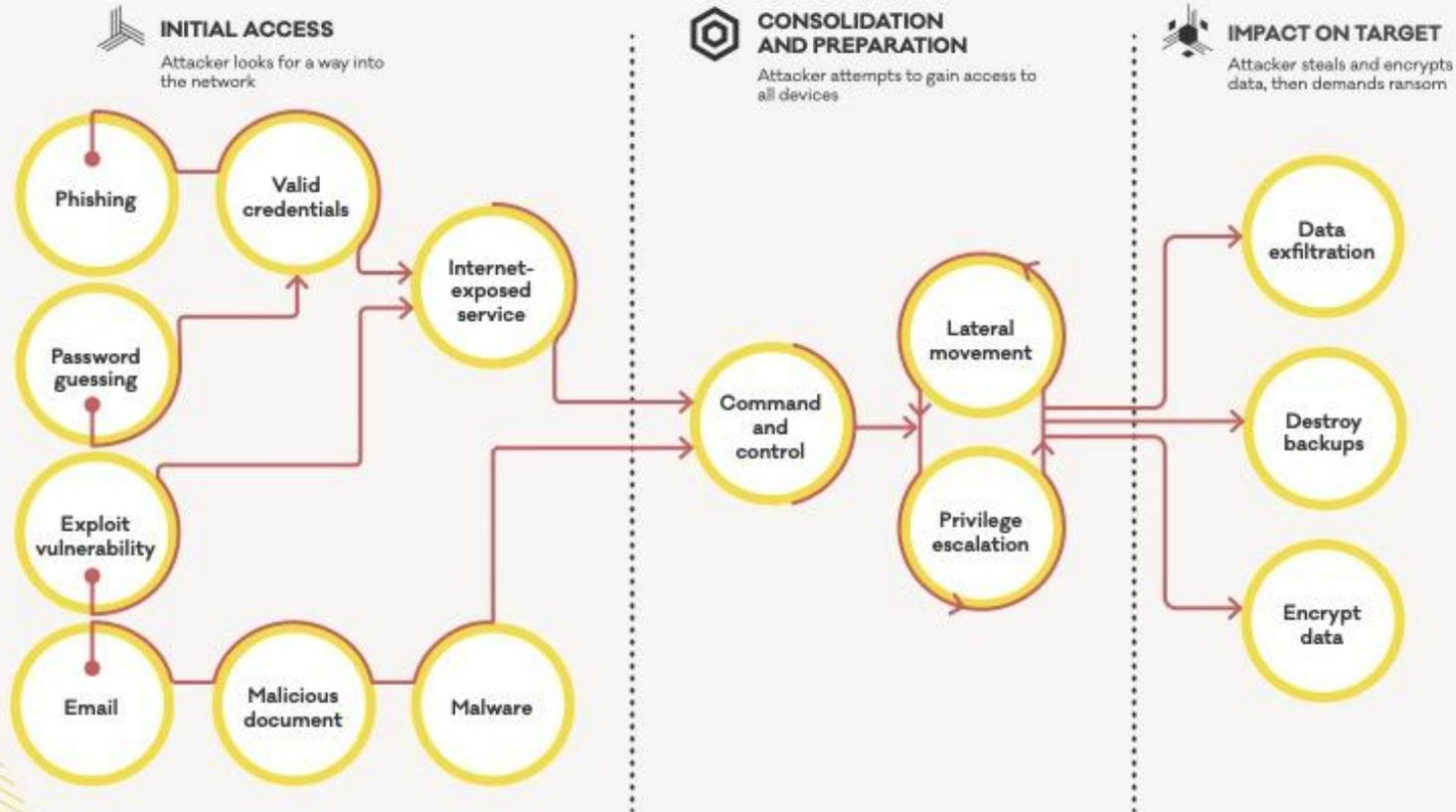


Helpful Advice

LIFECYCLE OF A RANSOMWARE INCIDENT



The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.



New Zealand Government

<https://research.splunk.com/>



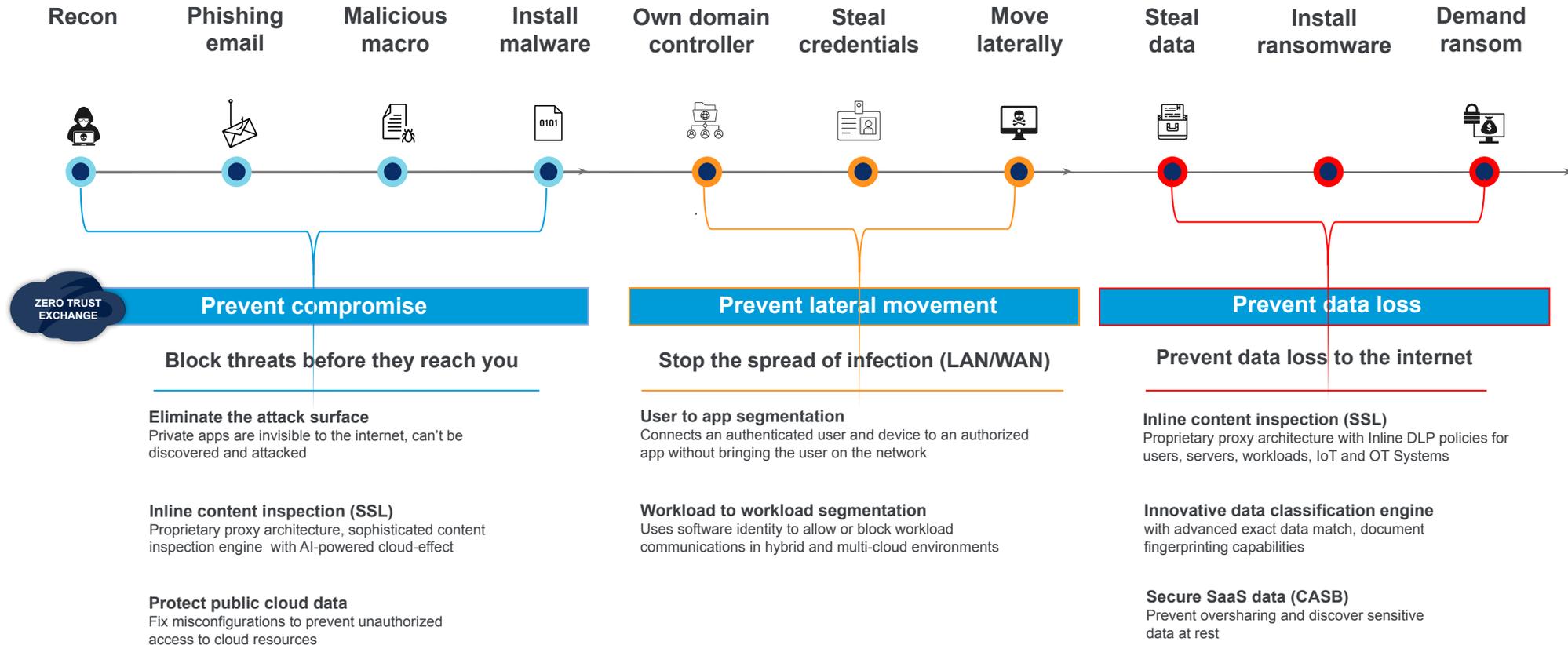
ransomware

170+ Results Found

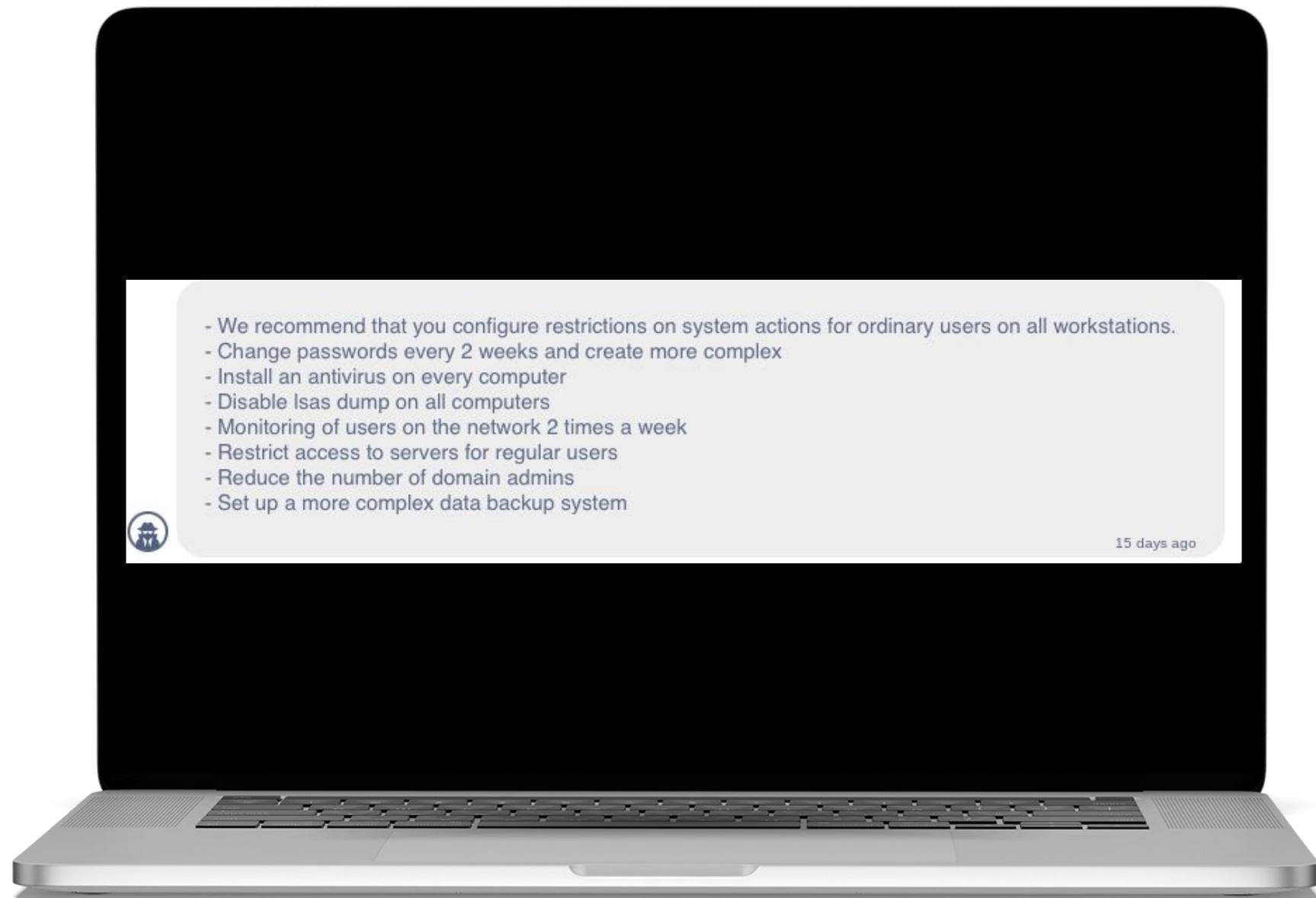


Zscaler Zero Trust Exchange

Designed to offer comprehensive protection against sophisticated attacks



Advice From Conti



Advice From the DarkSide

To prevent your network hacked again you have to:

1. Administrators must work in browsers in in-private mode
2. Administrators are prohibited from saving passwords in browsers
3. Administrators are prohibited from saving files with password lists on their computers or shared resources, as well as sending them by e-mail
4. All users are forbidden to open suspicious mail, punish with money. Allocate for this one computer without connection to the corporate network
5. Administrators work in virtual machines. Virtual machines must be in cryptocontainers
6. Configure firewalls so that administrator's computers do not have direct access to critical servers, but virtual machines have it (firewall rules and network ranges)
7. Limit the list of domain administrators. Split domain administrator password between security department and administration department (password is very long)
8. Delegate small roles to administrators for daily work (resetting passwords, creating users)

9. Use strong antivirus, Cylance or Carbon Black or Cortex (we do not advertise antivirus, think byr yourself)
10. Limit access to the Internet on servers and admin's computers. Create a terminal server in the DMZ and use the terminal browser applications
11. All suspicious letters with links should be sent to the IT department for verification on a stand alone virtual machine.
12. Configure mail filters to work with white lists. Anything that is not included in the whitelist must be moderated.
13. Prevent users from launching scripting programming languages (vbs, js and others) and unknown file extensions. If you doubt about opening link, transfer it to the IT department for verification on a stand alone virtual machine.
14. Open documents with macros only from trusted users. If you doubt about opening document, transfer it to the IT department for verification on a stand alone virtual machine.
15. If the user has launched a suspicious file, he should immediately contact the IT department.
16. Disable remote launch for powershell
17. Set 2FA Authorisation for network infrastructure. (Backups)



Shannon Davis



@DrShannon2000

shannon@splunk.com



Brett Stone-Gross



@pushecX

bstonegross@zscaler.com



Thank You

