Ransomware - Readiness, Response and Recovery

ENTERPRISE COMPUTING COMMUNITY
NATIONAL CONFERENCE,
JUNE 12 - JUNE 14, 2022.

DAVID ROSSI
CYBERSECURITY ARCHITECT
IBM Z SYSTEMS
DZROSSI@US.IBM.COM

AGENDA

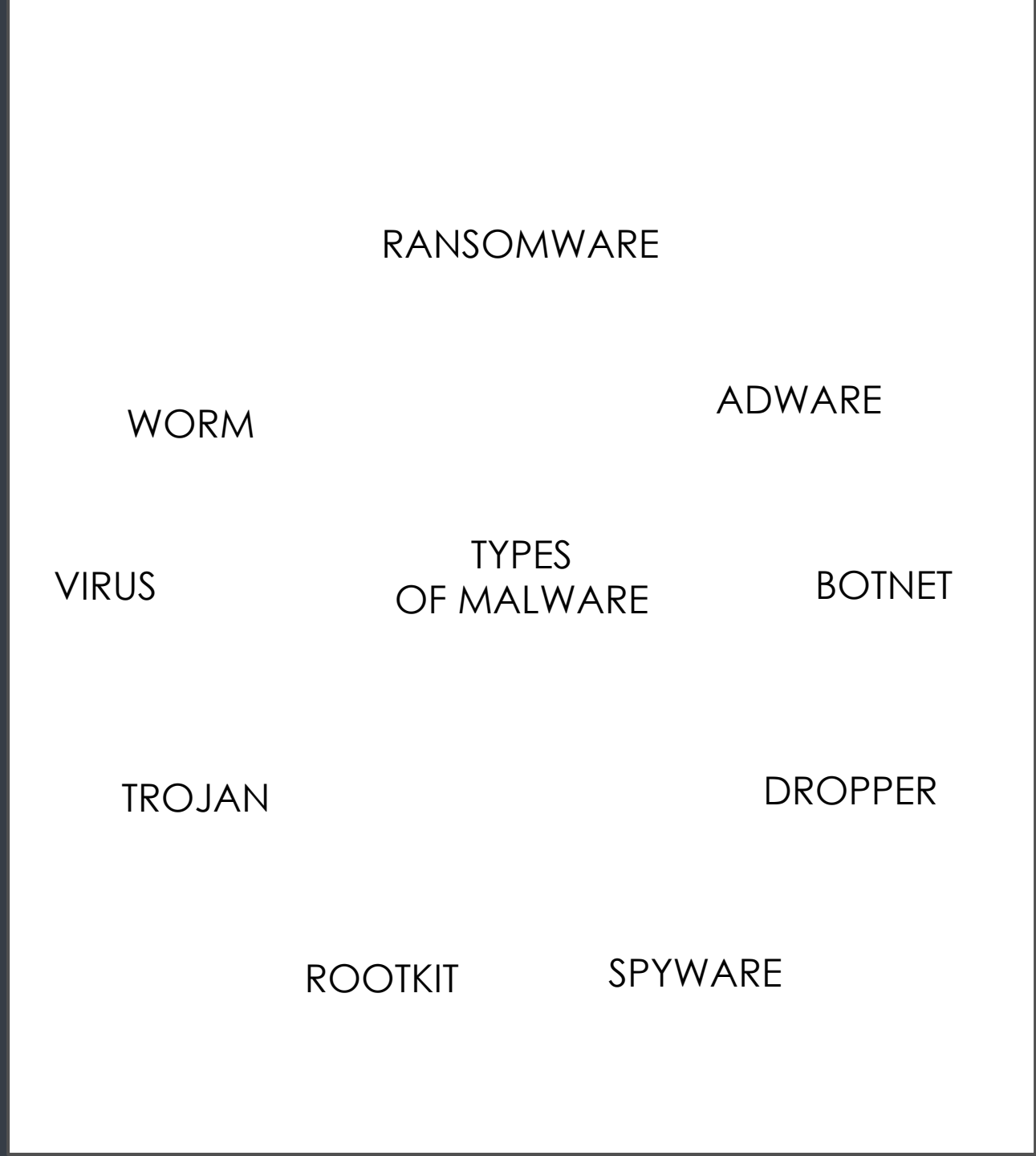
- What is Malware
- What is Ransomware
- Ransomware Trends
- Attack vectors
- General guidance

MALWARE

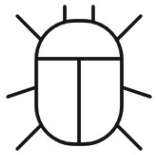
Malware Types

It is important to understand the types of malware. There are several types of malware, though to be honest, malware often falls into more than one category.

Malware is categorized using a number of factors including the delivery method or type of attack, the goal of the attack, and the target and technique of the attack.

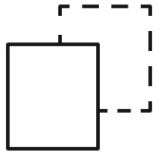


Types of Ransomware Attacks



Crypto ransomware

Crypto ransomware prevents access to files or data through encryption with a different randomly generated symmetric key for each file. The symmetric key is then encrypted with a public asymmetric key; attackers then demand the ransom payment for access to the asymmetric key.



Doxware

Doxware is a form of crypto ransomware where victims are threatened with not only losing access to their files, but also having their private files and data made public through “doxing”.

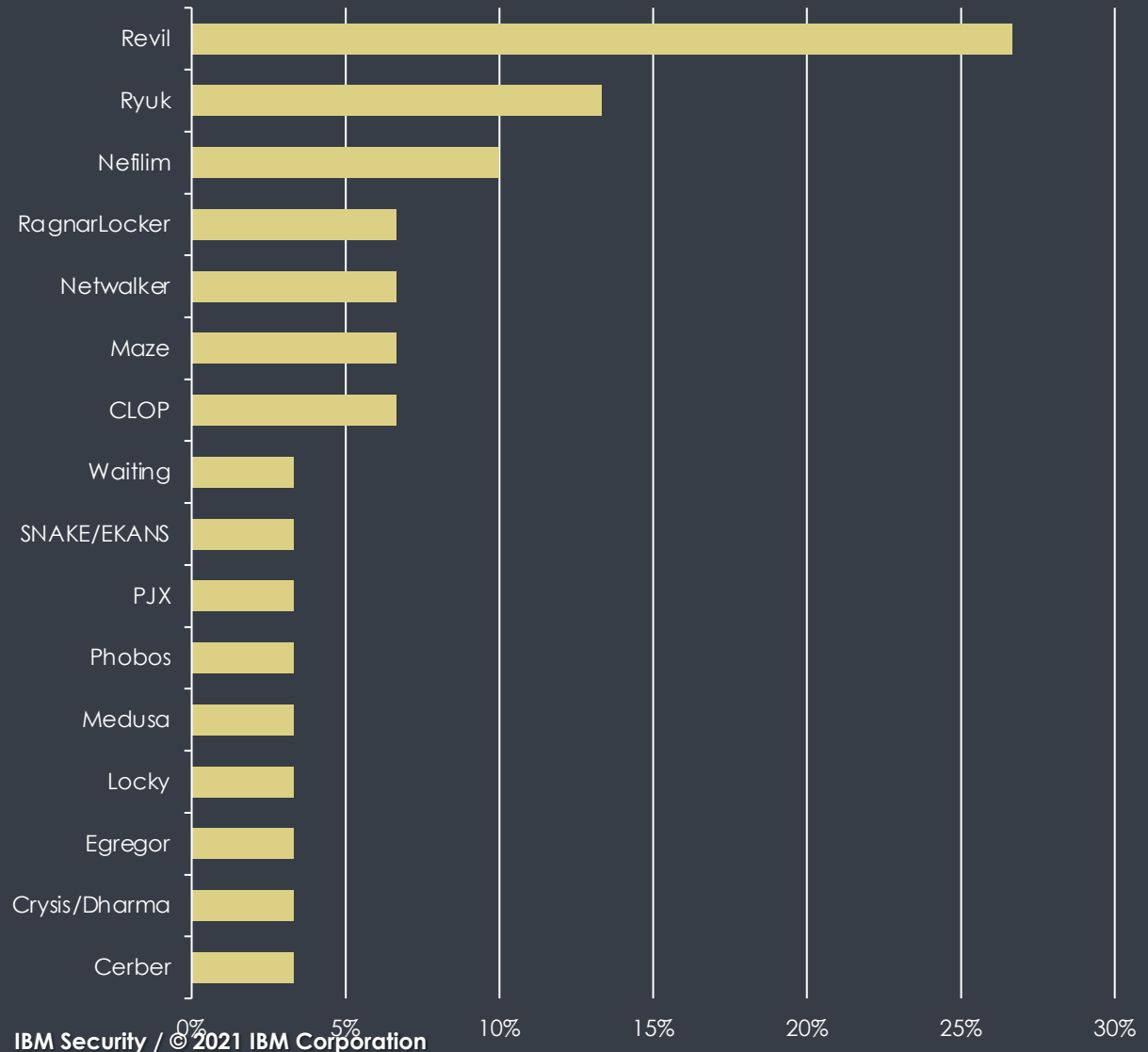
Locker ransomware

Locker ransomware locks the computer or device by preventing users from logging in; an infected machine can display an official looking message warning the user. This type of malware does not actually encrypt files on the device.

https://www.ibm.com/topics/ransomware

TOP RANSOMWARE GANGS

Percentage breakdown of ransomware types observed in 2020 – July 2021 | Source: IBM Security X-Force



Double Extortion: Occurs about 60 percent of the time attackers couple ransomware with stealing data

Ransomware pays: We estimate Sodinokibi/Revil alone earned $120m

Shift to Ransomware-as-a-Service: Affiliate or franchise operations, enables multiple infection vectors using the same ransomware

Business is booming: Ransomware could be a billion-dollar industry

ATTACK VECTORS AND GENERAL GUIDANCE

THE DEFINITIVE GUIDE TO RANSOMWARE: READINESS, RESPONSE, AND REMEDIATION

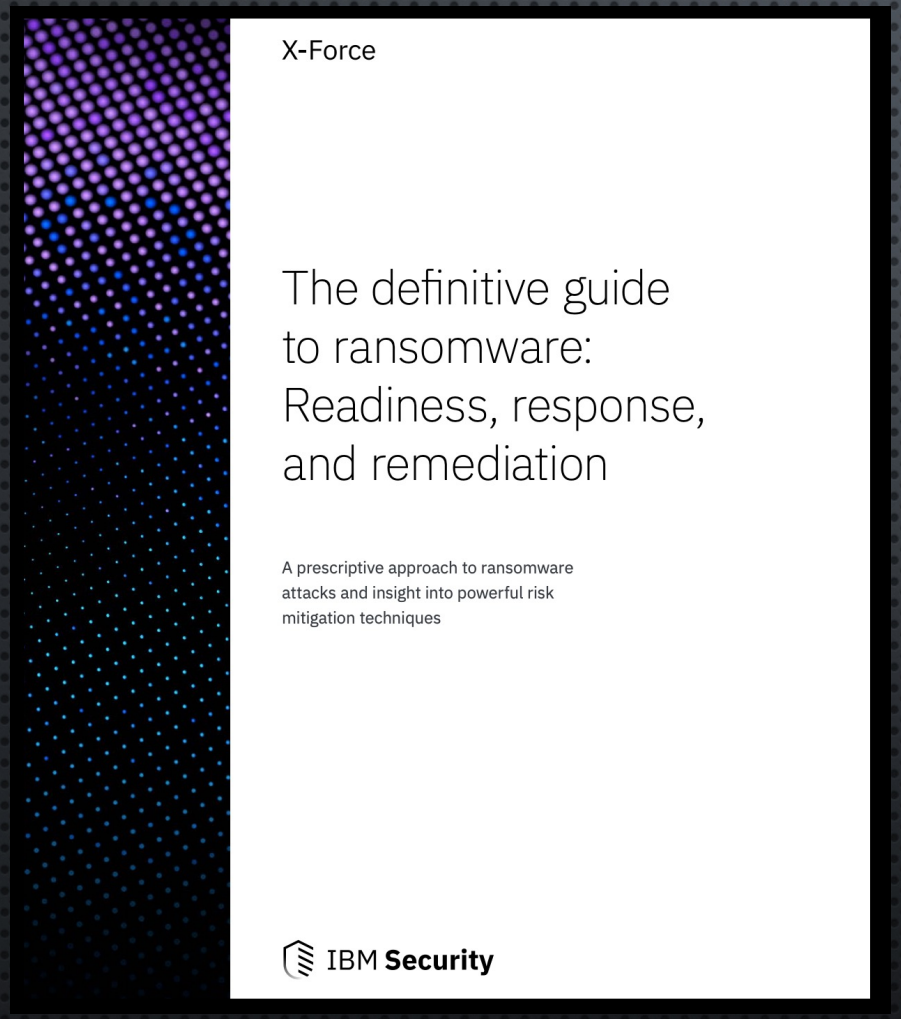


Table of contents

https://www.ibm.com/downloads/cas/EV6NAQR4

General Ransomware Attack Vectors

Infection Vectors

- Spearphishing
- Stolen credentials
- RDP
- Software vulnerabilities (occasionally)

Move Laterally

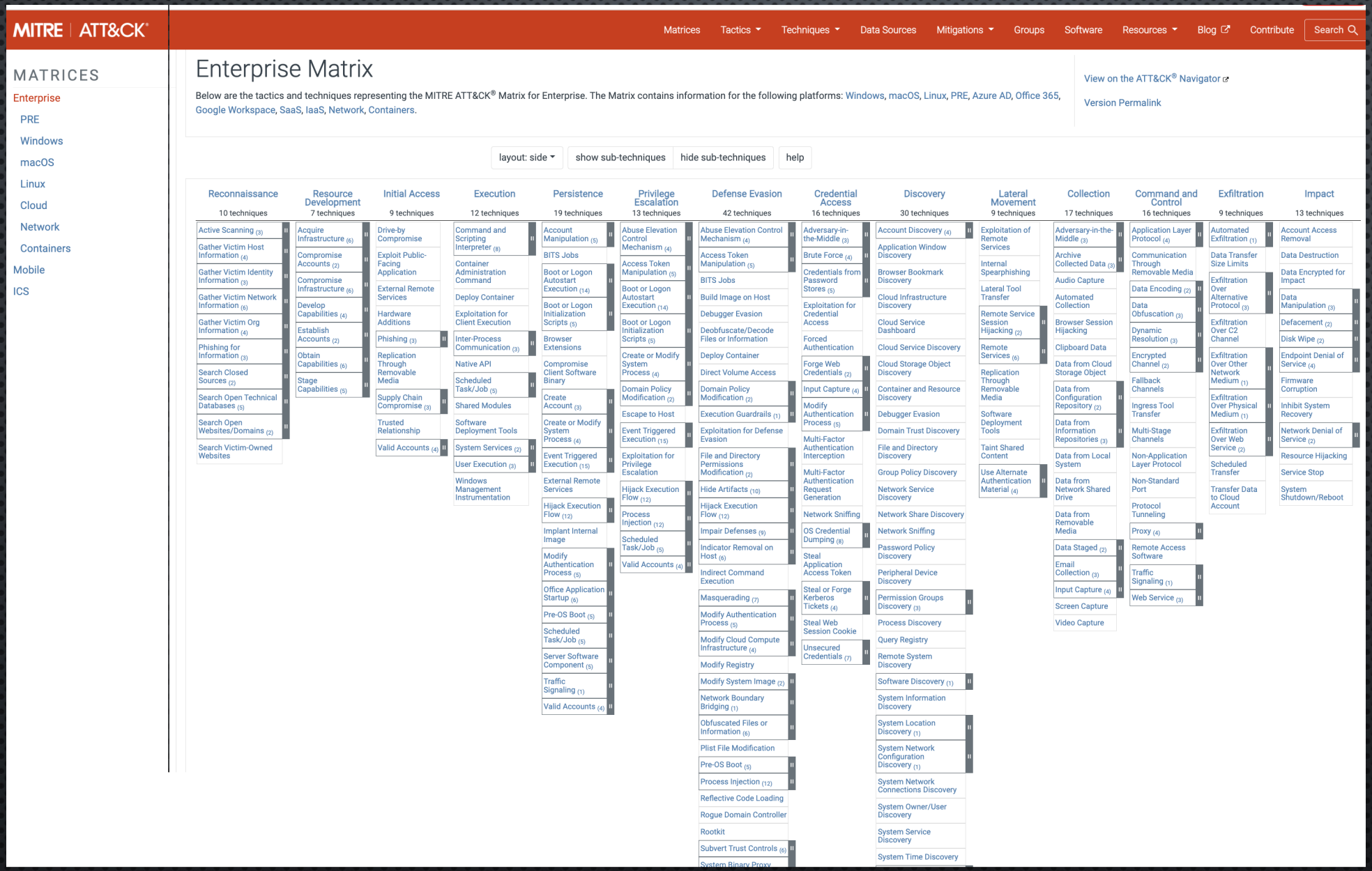
- Remote administration tools (RDP, PowerShell)
- Automated credential theft/use
- Domain Controller ("Up and Over")
- Hunt for strings containing PII

Encrypt

- Use symmetric encryption initially for speed
- Then use asymmetric encryption for security/convenience
- Algorithms vary, but all are mathematically legit

Exfiltration

- Compress data
- Send to download site (conventional and unconventional)



https://attack.mitre.org/matrices/enterprise/

REDUCE RISKS TO RANSOMWARE WITH SECURITY BASICS

- CYBER AWARES TRAINING
- ENABLE MULTI-FACTOR AUTHENTICATION
- HUNT FOR MALICIOUS ACTIVITY WITH AN ENDPOINT DETECTION AND RESPONSE TOOL AND PARTNER WITH X-FORCE THREAT MANAGEMENT
- ENCRYPT DATA
- PATCH RAPIDLY WITH INSIGHTS FROM A VULNERABILITY MANAGEMENT TEAM
- TEST BACKUPS AND CONFIRM THEY ARE NOT CONNECTED TO THE IT ENVIRONMENT
- TEST YOUR INCIDENT RESPONSE PLAN

Ransomware operators target organizations with the weakest security.

The basics mitigate risks to drive attackers to another environment.

NIST CYBERSECURITY FRAMEWORK

https://www.nist.gov/

https://www.nist.gov/cyberframework

The Urgency of Response

When a ransomware attack is discovered, every second counts. Uninterrupted, time is the ally of the attacker. As time passes, more data and files are encrypted, more devices are infected, ultimately driving up both cost and damage. Immediate—yet methodical and informed—action must be taken.

Alerting IT security teams and allowing them to launch the incident response process that they have prepared to combat ransomware should be a first step. If you have a retainer contract with a third party provider it is advisable to engage them as well.

Other parties to consider contacting are federal law enforcement and regulators, depending on the local requirements for the geographies in which your company operates.

MALWARE COURSE

Malware Types and Analysis

Threat Vectors and Kill Chain

Frameworks, Mitigations and Controls

Extended Detection and Response(XDR) and AI

NJCCIC

New Jersey Cybersecurity & Communications Integration Cell

THE WEEKLY BULLETIN

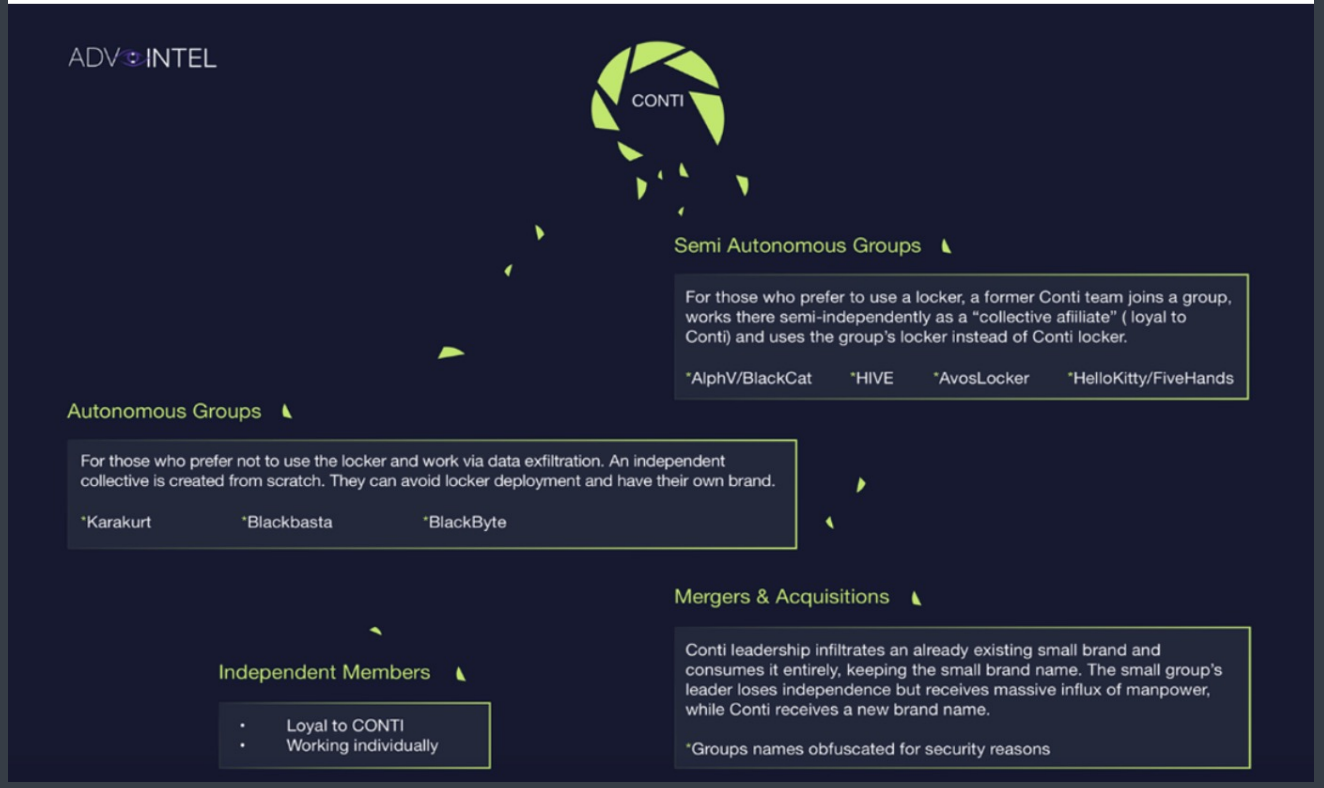
May 26, 2022

TLP: WHITE

Garden State Cyber Threat Highlight

Providing our members with a weekly insight into the threats and malicious activity directly targeting New Jersey networks.

Conti Ransomware Group Announces Shutdown, Proliferation Continues via Affiliates



https://www.cisa.gov/tlp

The prolific Conti ransomware group announced through its official website that it has shut down operations as of May 19, though activity from its affiliates continues. Internal conflict erupted after the group publicly announced allegiance to Russia during the onset of the war against Ukraine, causing the Conti brand to be synonymous with the Russian state. This allowed the United States to enforce Office of Foreign Assets Control regulations and sanctions policies, prohibiting corporations from paying ransom demands. Shortly after, a former affiliate publicly posted vast amounts of internal chat logs and source code, further crippling the group's efforts.

The group has rebranded before and is an offshoot of Ryuk. Conti dominated over other cybercrime groups due to its organizational system and business model, collecting highly skilled operators and building partnerships with other malware syndicates. For at least the last two months, Conti began creating subdivisions before dismantling and continues efforts via affiliates, forming alliances with BlackCat (a rebrand of DarkSide/ BlackMatter), AvosLocker, HIVE, HelloKitty/FiveHands, and other ransomware groups. A few subsidiaries already in operation include KaraKurt, BlackByte, and Black Basta. Just prior to the announced shutdown, Conti performed a massive cyberattack against Costa Rican government agencies, causing President Rodrigo Chaves to declare a national emergency.

The NJCCIC has observed recent attempts by Conti or its affiliates to compromise organizations. According to AdvIntel , Conti is adopting a more horizontal and decentralized network organizational structure and appears to be moving away from its Ransomware-as-a-Service model, further transitioning from purely data encryption to data exfiltration. Analysts assess that Conti will continue its efforts through its "coalition of equal subdivisions…united by internal loyalty to each other and the Conti leadership." According to the FBI, there were over 1,000 victims of attacks associated with Conti ransomware as of January, "with victim payouts exceeding $150,000,000 , making the Conti Ransomware variant the costliest strain of ransomware ever documented."

The NJCCIC advises organizations to remain vigilant and establish a comprehensive data backup plan that includes performing scheduled backups regularly, keeping an updated copy offline in a separate and secure location, and testing regularly. Additionally, keep systems up to date and apply patches as they become available, enable strong endpoint security, enforce cyber hygiene, implement a defense-in-depth strategy, segment networks, apply the Principle of Least Privilege, enable multi-factor authentication (MFA) where available, and create and test continuity of operations plans (COOPs) and incident response plans. Further guidance can be found in the Ransomware: Risk Mitigation Strategies NJCCIC technical guide. Administrators are further advised to analyze their networks using the indicators of compromise (IOCs) related to Conti and its affiliates and review the technical information found in the revised Cybersecurity and Infrastructure Security Agency (CISA) Alert AA21-265A. Users who discover signs of malicious cyber activity are encouraged to contact the FBI via the ransomware complaint form and the NJCCIC via the Cyber Incident Report form.

SECURITY NOW PODCAST

SECURITY NOW!

Our weekly audio security column
& podcast by Steve Gibson and Leo Laporte

TechTV's Leo Laporte and I spend somewhat shy of two hours each week to discuss important issues of personal computer security. Sometimes we'll discuss something that just happened. Sometimes we'll talk about long-standing problems, concerns, or solutions. Either way, every week we endeavor to produce something interesting and important for every personal computer user.

(This was **not** our idea. It was created by a fan of the podcast using GIMP (similar to Photoshop). But as a work of *extreme* image manipulation, it came out surprisingly well.)

- **You may download and listen to selected episodes** from this page (see below), or subscribe to the ongoing series as an RSS "podcast" to have them automatically downloaded to you as they are produced. To subscribe, use whichever service you prefer . . .

iTunes | iPODDER X | ODEO | podnova

- **Receive an automatic eMail reminder** whenever a new episode is posted here (from ChangeDetection.com). See the section at the bottom of this page.
- **Send us your feedback:** Use the form at the bottom of the page to share your opinions, thoughts, ideas, and suggestions for future episodes.
- **Leo also produces "This Week in Tech" (TWiT)** and a number of other very popular podcasts (TWiT is America's most listened to podcast!) So if you are looking for more informed technology talk, be sure to check out Leo's other podcasts and mp3 files.
- **And a huge thanks to AOL Radio** for hosting the high-quality MP3 files and providing the bandwidth to make this series possible. We use "local links" to count downloads, but all of the high-quality full-size MP3 files are being served by AOL Radio.

SECURITY NOW!

Episode Archive

Each episode has SIX resources:

- **High quality 64 kbps mp3 audio file**
- **Quarter size, bandwidth-conserving, 16 kbps (lower quality) mp3 audio file**
- **A PDF file containing Steve's show notes**
- **A web page text transcript of the episode**
- **A simple text transcript of the episode**
- **Ready-to-print PDF (Acrobat) transcript**

(Note that the text transcripts will appear a few hours later than the audio files since they are created afterwards.)

For best results: RIGHT-CLICK on one of the two audio icons & below then choose "Save Target As..." to download the audio file to your computer **before** starting to listen. For the other resources you can either LEFT-CLICK to open in your browser or RIGHT-CLICK to save the resource to your computer.

Episode #874 | 07 May 2022 | ... min.

Passkeys, Take 2

This week we have a response from ServiceNSW to the news of their insecure digital driver's license. ExpressVPN is the first VPN to pull the plug on India. Turning off the Internet is becoming a common practice by repressive regimes. The Windows Follina exploit explodes in the wild. Another Windows/Word URL scheme can be exploited. A critical cellular modem chip defect has surfaced. Named ransomware is being impacted by U.S. sanctions and ransomware is taking aim at our system boot firmware. We have a bit of errata and closing the loop feedback. Then, in the wake of Apple's big WWDC 2022 keynote, which mentioned Apple's forthcoming adoption of the FIDO2 Passkeys, I want to highlight one glaring concern that everyone seems to have missed.

43 MB | 11 MB | 393 KB <-- Show Notes | 138 KB | 72 KB | 337 KB

Episode #873 | 31 May 2022 | 110 min.

DuckDuckGone?

This week we examine the difficult to believe in 2022 design of Australia's New South Wales Digital Driver's License which was sold as being quite difficult to counterfeit. We examine the latest, once again fumbled, extremely pervasive Microsoft Office zero-day remote code execution vulnerability. We look at the first instance of touchscreen remote touch manipulation, and at Vodafone and Deutsche Telekom's difficult to believe yet already being piloted plan to further monetize their customers by somehow injecting persistent supercookies into their customer's connections at the carrier level. Then, after sharing some feedback from our terrific listeners, we'll dig into the discovery that the DuckDuckGo Privacy Browser carved out a privacy exception for Microsoft.

53 MB | 13 MB | 1,067 KB <-- Show Notes | 124 KB | 83 KB | 321 KB

Episode #872 | 24 May 2022 | 103 min.

Dis-CONTI-nued: The End of Conti?

This week we'll start by following-up on Microsoft's Patch Tuesday Active Directory domain controller mess. We're going to look at several instances of the Clearview AI facial recognition system making news, and at the systems which fell during last week's Vancouver Pwn2Own competition. We cover some welcome news from the U.S. Department of Justice and some disturbing news about a relatively simple and obvious hack against popular Bluetooth-link smart locks. We have some closing-the-loop feedback from our listeners, including a look at what's going on with the Voyager 1 space probe, and another interesting look into the looming impact of quantum crypto. Then we finish by sharing an in-depth examination of the surprisingly deliberately orchestrated shutdown of the Conti ransomware operation.

50 MB | 12 MB | 717 KB <-- Show Notes | 106 KB | 80 KB | 288 KB

Episode #871 | 17 May 2022 | 99 min.

The New EU Surveillance State

This week we look back at what no one wanted, an eventful Patch Tuesday. Apple has pushed a set of updates to close an actively exploited zero-day. Google announced the creation of their Open Source Maintenance Crew. A ransomware gang wants to overthrow a government. Google's Play Store faces an endlessly daunting task. The predicted disaster for F5's BIG-IP systems arrived. A piece of errata and some closing-the-loop feedback from our terrific listeners. Then we're going to look at just how far afield the European Union has wandered with their forthcoming breathtaking surveillance legislation.

48 MB | 12 MB | 610 KB <-- Show Notes | 125 KB | 77 KB | 319 KB

https://www.grc.com/securitynow.htm

QUESTIONS