SDC 20

BY Developers FOR Developers

Storage Developer Conference
September 22-23, 2020

Ransomware—Is it the Ultimate Malware?

Eric Hibbard, CISSP, CITP, CISA
PrivSec Consulting LLC

About the Speaker

Eric Hibbard, CISSP-ISSAP, ISSMP, ISSEP, CIPT, CISA, CCSK

Security/Privacy Professional
eric.Hibbard@gmail.com

Chair, SNIA Security Technical Work Group
Chair, INCITS TC CS1 Cyber Security
Chair, IEEE Computer Society, Cybersecurity & Privacy Standards Committee (CPSC)
Co-Chair, Cloud Security Alliance (CSA) – International Standardization Council (ISC)
Member, American Bar Association – Science & Technology (SciTech) Law Council
Member, American Bar Association – Cybersecurity Legal Task Force
Co-Chair, American Bar Association – SciTech Law – Internet of Things (IoT) Committee
ISO Editor: ISO/IEC 27040, ISO/IEC 27050 (multi-part), ISO/IEC 17788, ISO/IEC 22123 (multi-part), ISO/IEC 20648
IEEE Editor: IEEE Std 1619 (XTS-AES)

Abstract

Malware, short for malicious software, is a blanket term for viruses, worms, trojans and other harmful software that attackers use to damage, destroy, and gain access to sensitive information; software is identified as malware based on its intended use, rather than a particular technique or technology used to build it. Ransomware is a particularly nasty version of malware that typically encrypts a victim's files and then requires the victim to pay a ransom (usually in crypto currency) to the attacker to regain access to the data upon payment (no guarantees). A more aggressive variant on this theme, which some call doxware or extortionware, goes further and threatens to release copies of private data to the public if payment is not made.

This session provides information about ransomware, including common vectors, as well as detailing some of the types of ransomware that are currently plaguing organizations. Current counter techniques are presented along with their limitations. Lastly, the storage layer is explored as a possible defensive mechanism (current and hypothetical).

Agenda

- Background on Malware
- Profile of Current Ransomware
- Ransomware Countermeasures

Malware Background

Malware Defined

malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability [ISO/IEC 27033-1:2015]

software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user's computer system [ISO/IEC 27032:2012]

Common Malware

- **Viruses** – a piece of code that inserts itself into an application and executes when the app is run
- **Worms** – software capable of autonomous replication without the necessity for embedding itself in another entity
- **Trojans** – hidden code in desirable code or software that allows the unauthorized collection, falsification, or destruction of information

Common Malware (cont.)

- **Adware** – captures data associated with a user's surfing activity to build a profiles to determine which ads to serve them; tracking data can be shared or sold to advertisers without consent
- **Spyware** – collects information (passwords, pins, payment information, etc.) about users' activities without their knowledge or consent

Common Malware (cont.)

- **Keyloggers** – a type of spyware that monitors user activity and can be used to steal password data, banking information and other sensitive information.
- **Fileless Malware** – malicious code that runs in memory (no installation) that makes changes to files that are native to the operating system; not caught by antivirus software

Common Malware (cont.)

- **Rootkits** – software that gives malicious actors remote control of a victim's computer with full administrative privileges; can be injected into applications, kernels, hypervisors, or firmware
- **Bots/Botnets** – software application that performs automated tasks on command; used in large numbers (botnet) to launch broad remotely-controlled floods of attacks (DDoS)

Common Malware (cont.)

- **Cryptojacking** – malware that uses a victim's computing power to mine cryptocurrency
- **Ransomware** – software that uses encryption to disable a target's access to its data until a ransom is paid; there is no guarantee that payment will result in the necessary decryption key or that the decryption key provided will function properly

How Malware Spreads

- **Vulnerabilities:** Exploiting vulnerabilities to gain unauthorized access to the computer, hardware or network
- **Backdoors:** An intended or unintended opening in software, hardware, networks or system security
- **Drive-by downloads:** Unintended download of software with or without knowledge of the end user
- **Homogeneity:** If all systems are running the same operating system and connected to the same network, the risk of a successful worm spreading to other computers is increased

How Malware Spreads

- **Privilege escalation:** Attacker gets escalated access to a computer or network and then uses it to mount an attack
- **Blended threats:** Malware packages that combine characteristics from multiple types of malware making them harder to detect and stop because they can exploit different vulnerabilities

Combating Malware

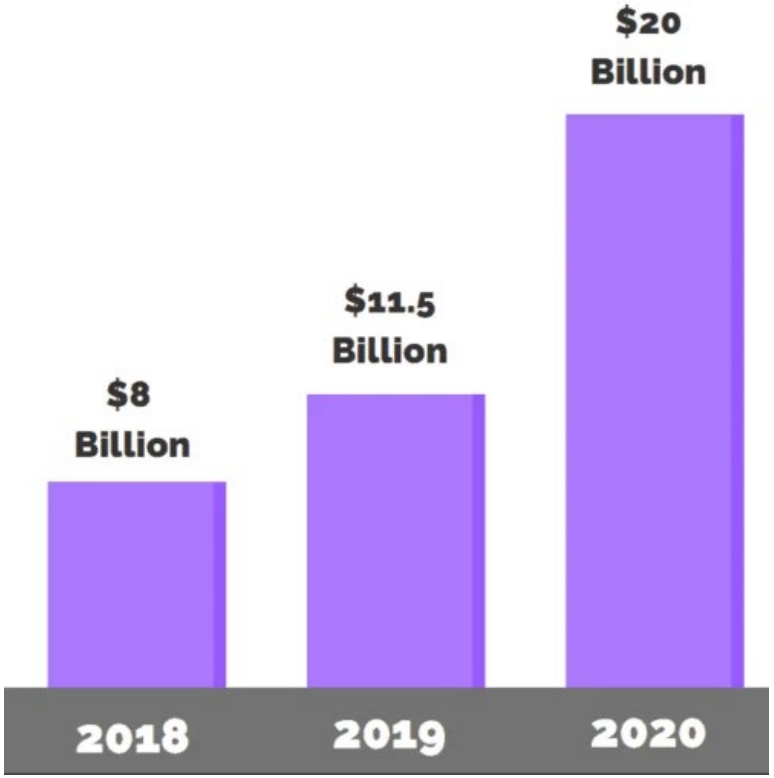
- Patch/Update OS, browsers, plugins, etc. regularly
- Update all application software regularly
- Use all the necessary security tools (antivirus software)
- Stay alert for social engineering attacks (phishing emails)
- Never click on links or download attachments coming from untrusted on unknown sources
- Practice safe browsing
- Have strong passwords, change passwords periodically
- Refrain from using un-encrypted public connections
- Layer your security starting with basic measures like firewall and antivirus

Profile of Current Ransomware

Major Ransomware Infection Vectors

- Spam/Phishing Email
- Weak Passwords
- Drive-by-Download
- Free Software
- Remote Desktop Protocol (RDP)

Estimated Global Damage from Ransomware



Average cost of a ransomware attack on businesses in 2019 was $133K

Top Ransomware Threats in 2020

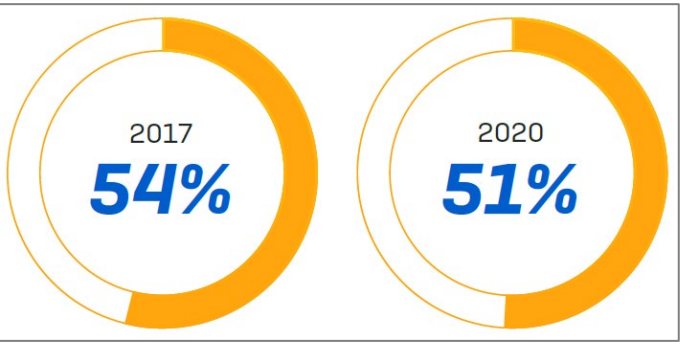
1. Maze: [exfiltrates data]
2. Revil: [exfiltrates data] $42M ransom (entertainment/media)
3. SNAKE (EKANS): ICS in Japan
4. Tycoon: JRE based; targes SMEs
5. TrickBot: phishing email; spreads laterally
6. Qakbot trojan: [exfiltrates data] leads with a banking trojan
7. PonyFinal: [exfiltrates data] Java-based; human-operated
8. Mailto (aka Netwalker Ransomware): Ransomware as a Service; using COVID-19-related lures

Top Ransomware Threats in 2020 (cont.)

9. Ragnar Locker: [exfiltrates data] targets remote management software (RMM)
10. Zeppelin: [exfiltrates data] targeting a handful of carefully chosen tech and healthcare companies in EU and US
11. Tflower: unprotected or poorly secured RDP ports
12. MegaCortex: high amount of automation to maximize victims
13. ProLock: targets ATMs; $660K ransom
14. DoppelPaymer: [exfiltrates data] $300K ransom
15. Thanos: can bypass various anti-ransomware methods

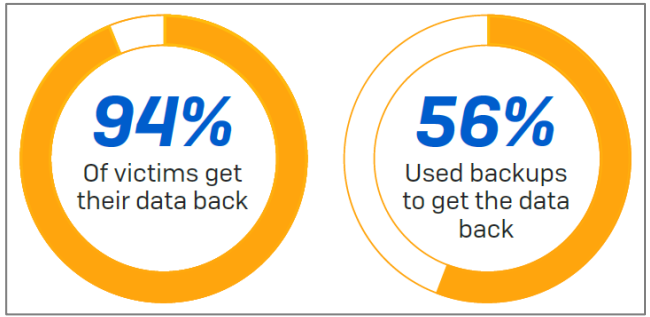
Ransomware Statistics

Prevalence of Ransomware

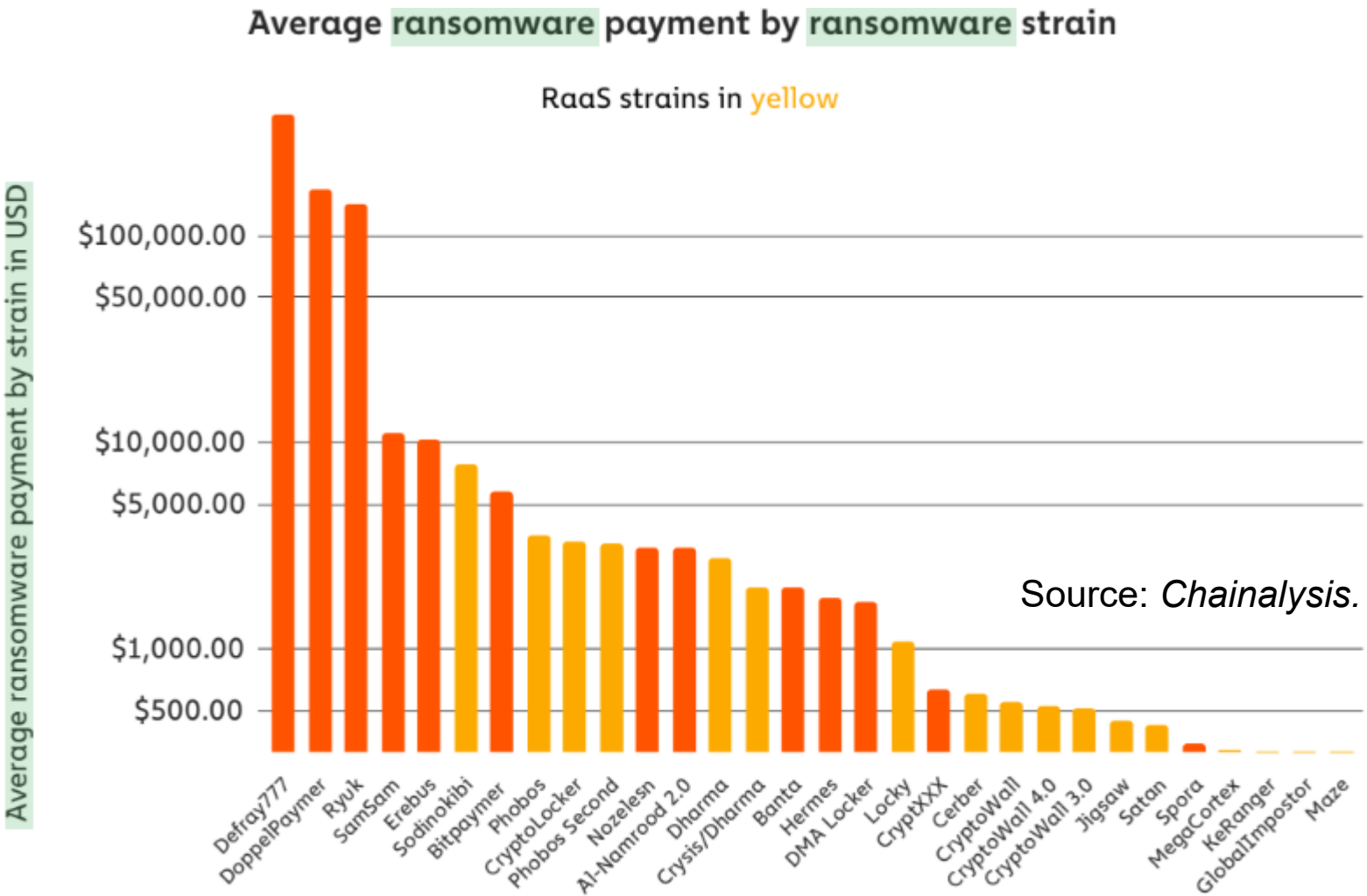


Impact of Ransomware

Getting Data Back



Source: *Sophos.*



Ransomware Countermeasures

Ransomware Kill Chain

1. Selection of a suitable “bait” (e.g. phishing emails with infected attachments)
2. Installing the malware on the target system
   - Installation can be independent of activation
3. Retrieval of the encryption key
4. Execution of the encryption code
   - Data exfiltration may occur before encryption
5. Ransom demand with deadline

Minimizing Ransomware Risks

- Start with the assumption that you *will* be a victim
- User education and traing (phishing and social engineering)
- Minimize attack surface by patching vulnerabilities, antivirus updates, and disabling unnecessary services (like RDP)
- Invest in anti-ransomware technology to stop unauthorized encryption (e.g., endpoint monitoring and protection)

Minimizing Ransomware Risks (cont.)

- Protect data wherever it's held (public cloud, private cloud, and on premises)
- Make regular/automated backups and store offsite and offline
- Have an incident response plan that addresses ransomware
- Ensure your cyber insurance covers ransomware
- Deploy a layered defense; defend against all vectors of attack

Infected by Ransomware?

- **Quarantine the affected system:** Stop additional infections through the network by unplugging the network cable
- **Notify the IT/security team:** This is the team to manage the incident (may be considered a data breach)
- **Do not restart the computer:** Critical system files may have been encrypted; reboots may not be possible after infection

Infected by Ransomware? (cont.)

- **Make a copy of the infected drive:** Take an image backup of the infected system/drive because some ransomware decryptors may accidentally destroy files, even with the correct key.
- **Attempt disk decryption with ransomware decryption tools:** Decryptors have been released for flawed ransomware variants and may be able to perform decryption

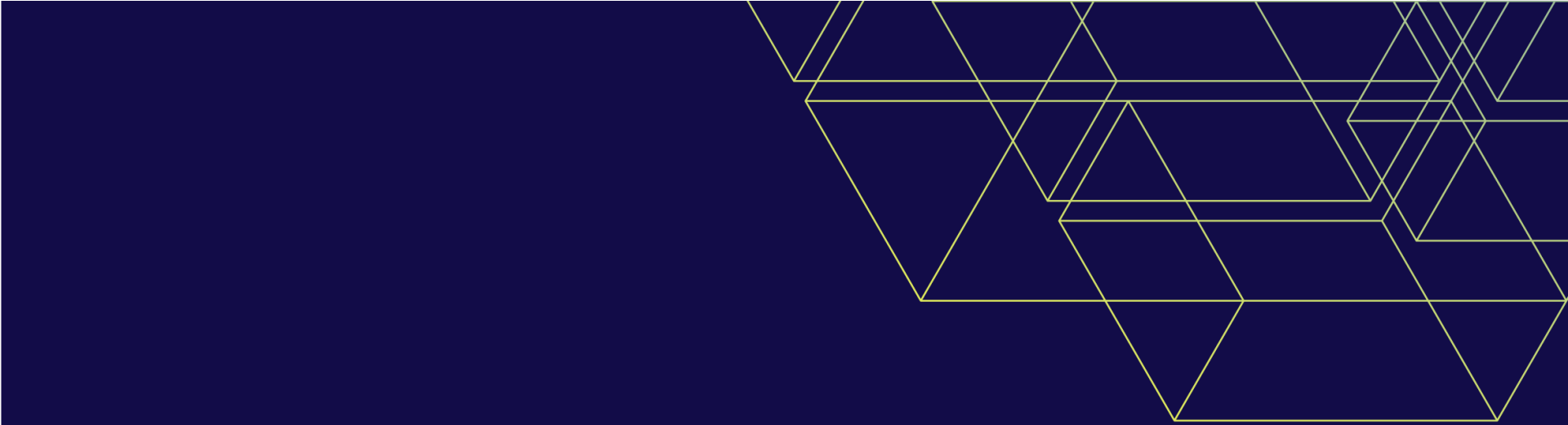
Infected by Ransomware? (cont.)

- **Restore infected systems from clean versions:** Wipe the system and do a clean install of OS and applications (with latest patches); ransomware may have persistence mechanisms
- **Restore data from clean backups:** Restore data from backups that predate the ransomware infection; protect the original
- **Sanitize removable media, connected drives, etc.:** Quarantine and sanitize other connected drives to remove the infection

Final Thoughts

- **For ransomware, prevention is the best possible cure.**
- Make sure you have appropriate security software installed, running, and up to date.
- Back up regularly.
- **A ransomware incident may be a reportable data breach for your organization.**

Thank You



Please take a moment
to rate this session.

Your feedback matters to us.