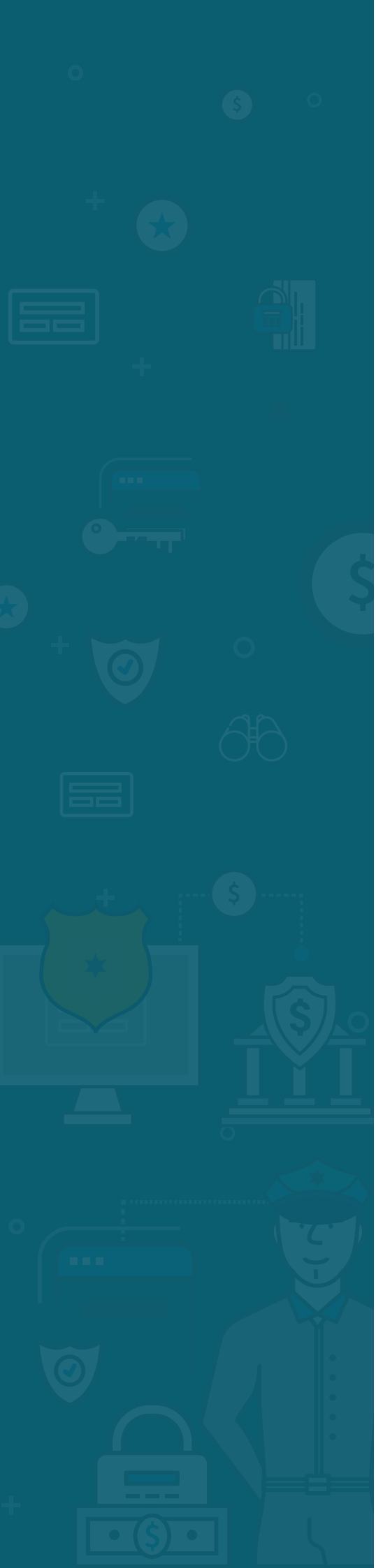
ManageEngine
DataSecurity Plus

Understanding ransomware:

FBI recommendations to limit data loss

www.datasecurityplus.com

Table of contents



Understanding ransomware: **FBI recommendations to limit data loss**

Introduction

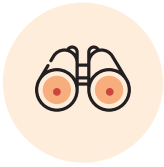
Ransomware hvas evolved over the years, and fast. Cybersecurity Ventures predicts that by 2019, one organization will be hit by ransomware every 14 seconds. So now, the question isn't if ransomware attacks will happen, but when.

With the growing prevalence of cyberattacks, it's imperative to understand the threat that ransomware poses and develop a multi-layered cybersecurity model to defend against it. With this free guide you'll learn about the measures recommended by the Federal Bureau of Investigation (FBI) to help you prevent, detect, and respond to ransomware attacks.

What is ransomware?

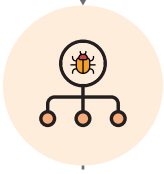
Ransomware is a type of malicious software that holds a victim's data hostage until they pay a ransom. Perpetrators threaten to either expose the victim's sensitive data, or restrict access to those files until payment is made in the form of cryptocurrencies—predominantly bitcoins.

The four phases of a ransomware attack



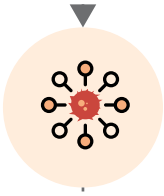
Reconnaissance

- Hackers examine targeted organizations' security systems to identify weak spots and existing vulnerabilities from which they can launch their attack.
- They then use this knowledge to fashion an appropriate attack vector.



Distribution

- Hackers can launch malware attacks through multiple attack vectors, including spear phishing, malvertisements, and exploit kits, to infiltrate organizations.
- Perpetrators often follow an affiliate scheme for ransomware distribution, where the ransomware developers get a take of the profits.



Infection

- Upon intrusion, ransomware begins infecting a network by taking advantage of inherent security vulnerabilities like unpatched applications.
- Once inside, it goes after high-privileged user accounts and encrypts files on all shared devices while distributing copies of itself to search for more victims.

Extortion

- After successful encryption, ransomware displays a ransom note to the victim demanding payment in cryptocurrency, preferably bitcoins.
- Displayed are explicit details regarding the ransom amount, mode of payment, deadlines, and consequences of non-payment.

Ransomware variants

Ransomware has consistently evolved from when it first appeared in the late 1990's. Currently ransomware can be broadly classified into two types: crypto-ransomware and lock screen ransomware.

Lock screen ransomware

This type of ransomware freezes or locks a device's user interface and demands a payment from the victim to lift the attack.

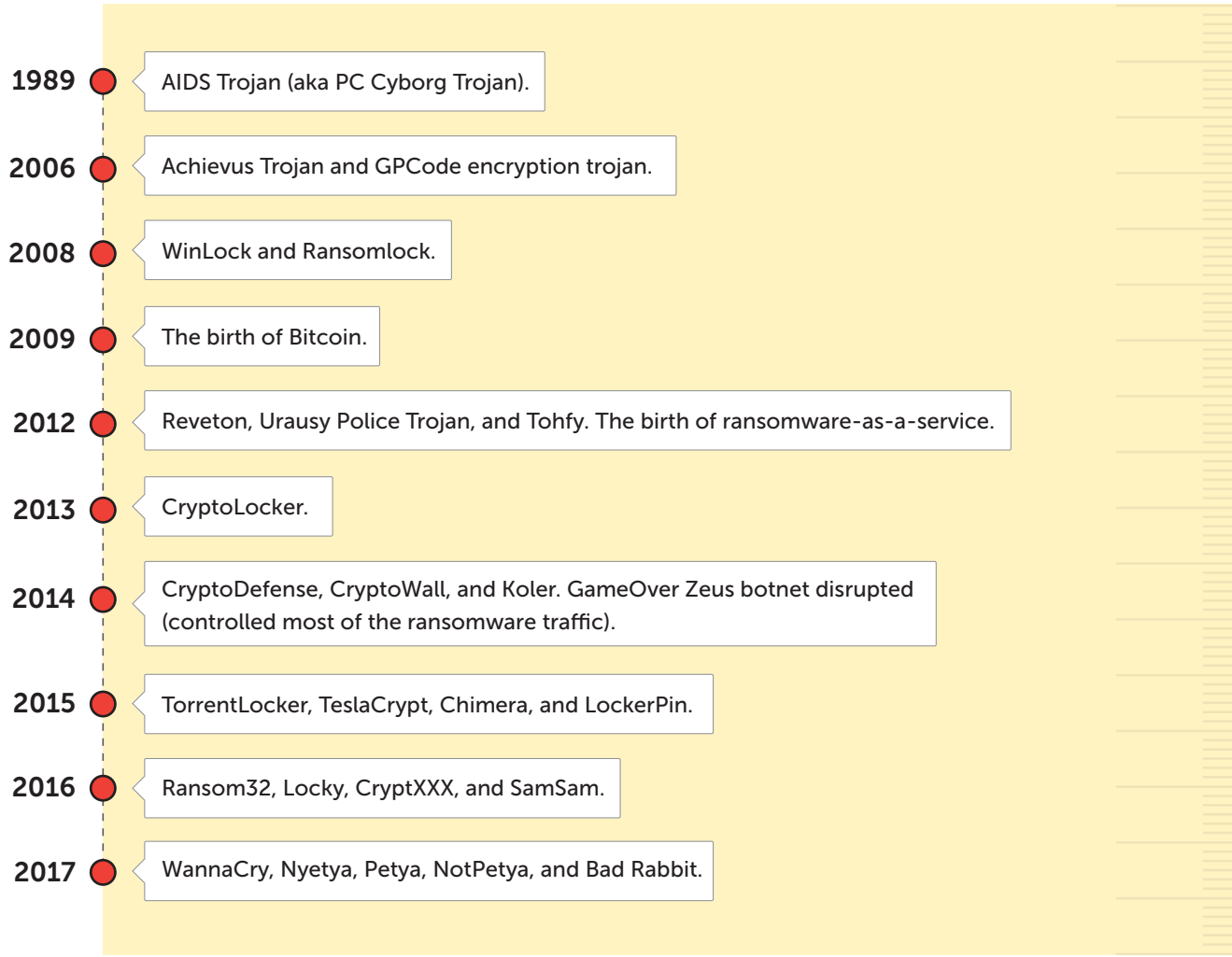
Example: **Reveton.**

Crypto-ransomware

Crypto-ransomware identifies and encrypts sensitive files. After successful encryption, this type of ransomware demands victims buy the decryption key.

Example: **CryptoWall, Locky, and TeslaCrypt.**

Ransomware variants timeline



How ransomware spreads

Ransomware utilizes multiple attack vectors to gain access to sensitive data. Some of the most common attack vectors are phishing emails, malvertisements, and drive-by downloads. Let's take a closer look into each of these.

Phishing emails

Email is the primary source of malware distribution, especially ransomware. Phishing emails—malicious emails that masquerade as legitimate ones—are designed to exploit your organization's most vulnerable asset: end users. Most phishing emails use social engineering to trick users into opening a malicious attachment or clicking a link which redirects them to a compromised website. Using personalized phishing emails to infect a business with ransomware is known as "spear phishing."

Malvertisements

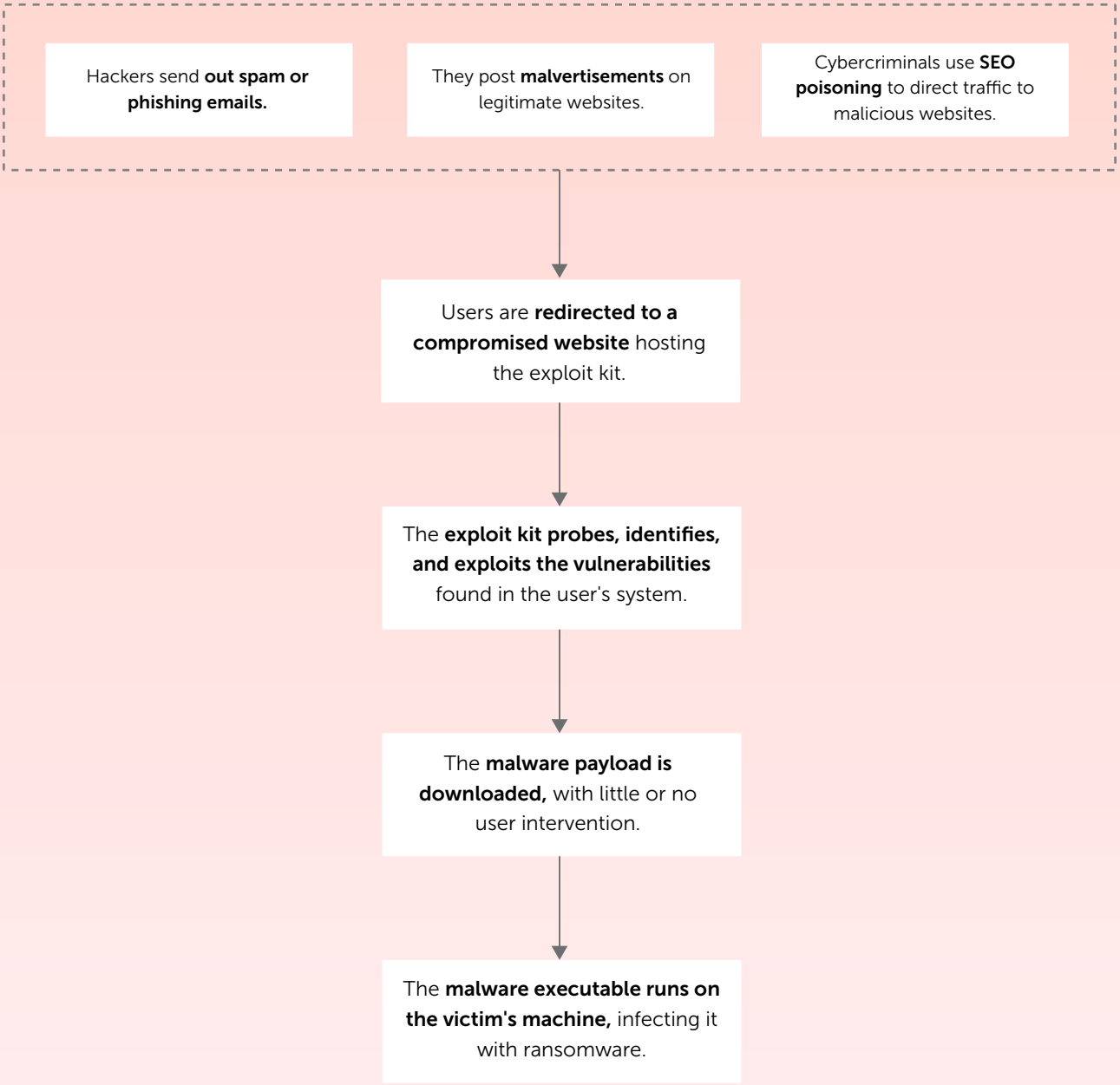
Malvertisements, a form of malicious online advertising, are used to lure gullible users into downloading ransomware. Cybercriminals invest in online ad space on legitimate websites to host malicious ads that infect users who click on them. Google identified and blocked over 1.7 billion suspicious ads in 2016 alone. Some of the websites that have displayed these dangerous ads include:

- The New York Times
- BBC
- MSN
- NFL.com
- Xfinity
- Thehill.com
- Zerohedge.com
- Infolinks.com
- Answers.com
- News Week
- Realtor.com
- The Weather Network
- AOL

Exploit kits

Exploit kits are used by cybercriminals to probe, identify, and exploit the vulnerabilities in browsers or plug-ins. The Sweet Orange and Angler exploit kits reigned supreme from 2014 to 2016; Angler alone served over nine thousand unique IP addresses in a single day.

Phases of an exploit kit malware attack



According to
IBM's 2014 Cyber Security Intelligence Index,
over **95 percent** of all security incidents involve **human error.**

What makes ransomware so successful?

Social engineering

Social engineering tricks online users into clicking malicious links or divulging personal information through psychological manipulation. Clever use of social engineering subtly persuades the user using scare tactics, or false promises to entice users into clicking on an attack vector. Successful ransomware can be attributed to socially engineered malicious emails and ads.

Cryptocurrencies (Bitcoin)

Bitcoin is a virtual form of currency that is pseudo-anonymous by nature. Bitcoin transactions are made based on a private key generated along with the bitcoin wallet, but otherwise they don't include any other personally identifying information; this makes Bitcoin transactions impossible to trace. This anonymity empowers perpetrators, fueling ransomware attacks.

FBI recommended measures to limit data loss

Preventive measures against ransomware

Educate end users

Create awareness among your employees on how to identify and avoid common ransomware pitfalls such as malvertisements, phishing emails, and more.

Employ email filtering

Block malicious attachments, spam, and phishing mails from reaching end users in the first place with the help of email filters. Use inbound email authentication technology to prevent email spoofing.

Patch vulnerabilities

Mitigate the vulnerabilities in your operating systems, browsers, and other applications by regularly updating them using a centralized patch management system.

Logically separate networks

Mitigate data loss in the event of a ransomware attack by implementing a physical and logical separation of networks.

Whitelist applications

Allow only known, approved software to run in your systems and block unauthorized programs from running.

Provide the least amount of privilege possible

Use robust access management to restrict unwarranted access and reduce the number of access points through which malware can enter your organization.

Use anti-malware software

Conduct regular deep-system scans to detect and block malicious programs from infecting your computer.

Configure your firewall

Use your firewall to monitor and control incoming and outgoing network traffic. Block malicious worms, viruses, and other threats from infecting your computer through the internet.

Disable macros

Prevent ransomware attacks that exploit macros from infiltrating your system by disabling macro scripts from Office files.

Use software restriction policies

Protect your system from both unknown and malicious code by implementing software restriction policies. These policies prevent executables from running when they are in specific locations in your system.

Measures to ensure business continuity

Back up your files

Perform regular backups of your sensitive data to periodically ensure its integrity. Use the 3-2-1 back-up rule, i.e. maintain at least three separate copies of data on two different storage types with at least one offline.

Conduct a vulnerability assessment

Identify real risks by conducting periodic penetration tests and vulnerability assessments. Use the results to help address and manage potential security pitfalls.

Reactive measures in the event of a ransomware attack

Turn off the infected device

Shut down the infected system to promptly cut off ransomware encryption.

Isolate the infected computer

The infected computer must be isolated from the network immediately to prevent the ransomware from infecting shared drives.

Secure backup data

Ensure that back up data is free of malware by moving it offline at the first sign of a ransomware attack.

Contact law enforcement

It's recommended that you notify the FBI or U.S. Secret Service in the event of a ransomware attack and ask for assistance.

Enforce a password change

Change all your online account, network, and system passwords after the malware has been removed to prevent future ransomware attacks.

Should you pay ransomware extortionists?

Paying hackers' ransom doesn't solve the underlying problem. Not only is there is no guarantee that your data will be recovered, but paying ransoms emboldens hackers, funds their illicit activities, and continues the vicious cycle of cyberattacks.

Moreover, the United States Government doesn't encourage paying ransoms to criminals.

Why you should report ransomware attacks to law enforcement agencies

Ransomware victims are often reluctant to report the attack for multiple reasons, such as lack of awareness on who to report to, fear over hurting their business's reputation, and concerns about privacy breach notification clauses in compliance requirements. However, reporting ransomware attacks helps law enforcement agencies to:

- Ascertain the true number of active ransomware infections, along with the number of victims.
- Gain greater insight into the methodology behind ransomware attacks.
- Identify and apprehend the perpetrators.

Reporting your ransomware attack, however big or small, is critically important in the fight against future attacks.

How to report a ransomware attack to law enforcement agencies

The FBI requests that ransomware victims report an attack to the Internet Crime Complaint Center (IC3) with the following information:

1. **Date of the ransomware infection.**
2. **Name of the ransomware variant** as mentioned in the ransom note or from the encrypted file extension.
3. **Victim's information** such as organization name, industry, size, etc.
4. **Attack vector** used for ransomware infection.
5. **Ransom amount** demanded.
6. **Perpetrators' Bitcoin wallet address** as mentioned in the ransom note.
7. **Ransom amount paid,** if any.
8. **Overall damage** incurred as a result of ransomware infection (including the ransom amount paid).
9. **Victim's impact statement.**

Most significant ransomware attacks of 2017

WannaCry

- WannaCry (also known as WannaCrypt) is by far the largest ransomware attack to date, infecting over 400,000 devices in over 150 countries.
- This attack exploited the EternalBlue vulnerability in Microsoft's Server Message Block (SMB) protocol back in May 2017.
- Although the patch for the EternalBlue vulnerability was released by Microsoft two months prior to the attack, many organizations' IT security teams were caught sleeping.
- The initial attack demanded $300 in ransom, but the perpetrators soon doubled their demands after successfully infecting a number of organizations.
- In total, an estimated $50,000 was paid in ransom. However, the true cost of WannaCry for organizations was downtime, data loss, and pricey forensic analysis, leading to millions of dollars in losses.
- The attack was temporarily stopped when a British cybersecurity expert accidentally found a kill switch after registering the domain name used by WannaCry however, the perpetrators were quick to release a new variant without the kill switch.

Petya

- On June 27, 2017, a cyberattack named Petya (also known as Golden Eye) started infecting users across Ukraine, the United States, the Netherlands, and more.
- Petya was distinctly different from WannaCry in its inability to spread across the public internet to infect more victims.
- More nefarious than WannaCry, Petya used a backdoor in third-party Ukranian accounting software, MEDoc, and leveraged the SMBv1 exploit (EternalBlue) as well as multiple other vulnerabilities to infect a victim's system.
- Once Petya encrypted the master file table, the victim's entire file system became unreadable and inaccessible.

NotPetya

- A ransomware variant started spreading rapidly in the beginning of June 2017 and, due to its likeness to Petya, earned the moniker NotPetya.
- Unlike Petya—which was designed for extortion—NotPetya focused on causing mayhem and irreparable damage to data.
- Upon infection, NotPetya moved laterally within an organization by leveraging the SMB vulnerability and exploiting credentials and other such attack vectors.
- NotPetya was essentially a sophisticated version of Petya, as it used legitimate administrative tools such as PsExec and WMIC to infect its victim without raising red flags.

Bad Rabbit ransomware

- On October 24, 2017, a ransomware variant named Bad Rabbit started infecting users in Russia, Ukraine, Turkey, and Germany.
- Bad Rabbit ransomware spread via a fake Adobe Flash Player installer and infected users through drive-by-downloads.
- Fortunately, this attack died out quickly; Bad Rabbit's servers went down within a day and any compromised sites were taken down.

The future of ransomware threats

Ransomware is evolving at an alarming pace in terms of severity and complexity. This emphasizes the importance of foreseeing the future of ransomware-related cyberthreats and preparing for it.

IoT-based ransomware attacks

- With the proliferation of IoT-based devices, any and every device connected to the internet is vulnerable to ransomware and other malware-related threats.
- Using remote code execution, hackers can theoretically hold your car, your pacemaker, or even your entire smart home hostage until you pay their ransom.

Ransomware-as-a-service (RaaS)

- The growth of the ransomware-as-a-service model in the dark web is a primary driver for the explosion of multiple ransomware variants in the last couple of years.
- From 2016 to 2017, there was a 2,502 percent increase in the sale of ransomware on the dark web.
- Ransomware do-it-yourself kits have potentially armed run-of-the mill cybercriminals into launching their own sophisticated cyberattacks.
- This affiliate-based ransomware scheme typically allocates 20 to 40 percent of its illicit earnings to the ransomware developers and another percentage to the promotion of the RaaS kit, while the rest goes to the perpetrators who carry out the attack.
- Philadelphia, Stampado, Frozr Locker, Satan, and RaasBerry are some of the noteworthy RaaS kits that have been put up for sale on the dark web.

Doxware

- Doxware is an evolved version of ransomware, taking the threat one step further by exfiltrating victims' confidential data once it's been encrypted. With doxware, failure to comply with the perpetrator's demands will result in confidential business data being leaked.

> Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds; and be stolen without your knowledge.
>
> **Bruce Schneier,**
> Protect Your Macintosh

Ransomware prevention checklist

Preventive measures at the user level

- [ ] Conduct security awareness training and educate your end users about ransomware attacks.
- [ ] Train your end users to spot and report phishing emails containing malicious attachments.

Preventive measures at the software level

- [ ] Ensure your firewalls are operational and up-to-date at all times.
- [ ] Logically separate your networks.
- [ ] Employ a strong email filtering system to block spam and phishing emails.
- [ ] Patch vulnerabilities and keep all your software updated.
- [ ] Set up rigorous software restriction policies to block unauthorized programs from running.
- [ ] Keep your antivirus fully operational and up-to-date.
- [ ] Conduct periodic security assessments to identify security vulnerabilities.
- [ ] Enforce the principle of least privilege.
- [ ] Disable Remote Desktop Protocol (RDP) when not in use.
- [ ] Disable macros in your Microsoft Office files.
- [ ] Use a strong, real-time intrusion detection system to spot potential ransomware attacks.

Preventive measures at the backup level

- [ ] Back up your files using a 3-2-1 backup rule, i.e. retain at least three separate copies of data on two different storage types, with at least one of those stored offline.
- [ ] Ensure that you back up critical work data periodically.
- [ ] Enforce regular checks for data integrity and recovery on all your backups.

Ransomware **response checklist**

Time-sensitive reactive measures

- ☑ Shut down infected systems immediately.
- ☑ Disconnect and isolate infected systems from the network.
- ☑ Isolate your backups immediately.
- ☑ Disable all shared drives that hold critical information.
- ☑ Issue an organization-wide alert about the attack.
- ☑ Contact your local law enforcement agency and report the attack.

Analysis-based reactive measures

- ☑ Determine the scope and magnitude of an infection by identifying the type and number of devices infected, as well as what kind of data was encrypted.
- ☑ Determine the type and version of the ransomware.
- ☑ Identify the threat vector used to infiltrate your network.
- ☑ Conduct root cause analysis.
- ☑ Mitigate any identified vulnerabilities.
- ☑ Check if a decryption tool is available online.

Business continuity reactive measures

- ☑ Restore your files from a backup.

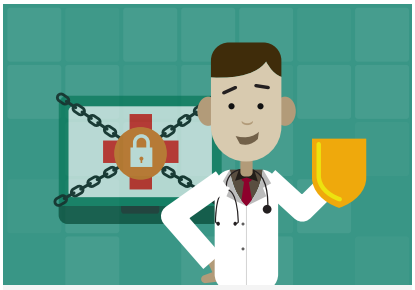
Additional **resources**

Step-by-step guide to detect and respond to ransomware attacks.

Know more >

8 best practices to prevent future ransomware attacks.

Know more >



Infographic on HIPAA guidelines on ransomware attacks.

Know more >

Infographic on how to protect your organization from ransomware attacks.

Know more >

References

- The ransomware economy, October 2017, Carbon Black
- IBM Security Services 2014 Cyber Security Intelligence Index
- Cybersecurity Ventures ransomware damage report, 2017, part 2
- FBI ransomware prevention and response for cisos
- https://arstechnica.com/information-technology/2016/03/big-name-sites-hit-by-rash-of-malicious-ads-spreading-crypto-ransomware/
- https://blog.google/topics/ads/how-we-fought-bad-ads-sites-and-scammers-2016/
- https://www.enisa.europa.eu/publications/info-notes/the-takedown-of-the-angler-exploit-kit

DataSecurity Plus

ManageEngine DataSecurity Plus is a data visibility and security solution. It tracks and alerts on critical file modifications and movement across file servers, failover clusters, workstations, and USBs. Users can locate and analyze files containing PII/ePHI stored in Windows file servers, failover clusters, and OneDrive environments using built-in data discovery rules. Its data leak prevention (DLP) capability helps detect and respond to the exfiltration of sensitive data via USBs, email, printers, and more. It also provides detailed audit reports that help organizations streamline compliance with multiple IT regulations.

To explore these features and see DataSecurity Plus in action, launch the online demo.
To learn more about DataSecurity Plus, visit www.datasecurityplus.com.

Download free trial $ Get a quote

Explore
DataSecurity Plus' solutions

File server auditing

Audit, monitor, report on, and alert on all file accesses and modifications made in your file server environment in real-time.

Learn more

NEW

Data leak prevention

Detect, disrupt, and respond to sensitive data leaks via USB deivces, emails, printers, and more through real time security monitoring.

Learn more

NEW

Data risk assessment

Perform content inspection and contextual analysis to discover sensitive data in files, and classify it based on vulnerability.

Learn more