A BEGINNER'S GUIDE TO RANSOMWARE

WHAT IT PROS NEED TO KNOW!

WARNING:

With this eBook, Unitrends gives you insights into how simple and prevalent ransomware attacks have become and shares how sophistication on the part of cybercriminals has improved the efficacy of these attacks.

Do not try this at home!

UNITRENDS
A Kaseya COMPANY

Overview

Imagine being part of an IT segment with sky-rocketing growth, massively successful deployment worldwide and revenue of over $1 billion that will only keep increasing over the coming years.[1] It's a highly lucrative industry that is constantly growing, with new versions of the software being released and deployed every day.

Who wouldn't want a piece of that pie, right? Unfortunately, we're talking about ransomware.

Ransomware is a form of malware that locks up customer data. The malware programming community continues to infiltrate and block access to more and more devices, increasing its list of victims in the process. Then, ransomware distributors demand payment in exchange for a key to unlock the encrypted files, raking in billions in revenue.

To put it simply:

- **Ransomware locks victims' files with strong, unbreakable encryption.**
- **Demands payment for a private key to unlock the encrypted data.**
- **In double extortion ransomware attacks, threat actors threaten to expose, sell or permanently delete victims' data in addition to encrypting it.**

Ransomware trends

Ransomware continues to evolve, presenting new challenges for individuals and organizations alike. The rise of double extortion tactics is noteworthy, where cybercriminals not only encrypt data but also threaten to release sensitive information unless a ransom is paid. This dual threat adds a layer of complexity, compelling victims to weigh the potential damage of data exposure against the cost of ransom payment.

In recent trends, attackers are increasingly employing sophisticated techniques, targeting data in the cloud. With more businesses moving their data and workloads to the cloud, it's only natural for cybercriminals to gravitate toward it. In 2023, over 80% of data breaches were cloud-based.[2]

There's a growing concern among business and technology leaders regarding the rise of Generative AI (GenAI) in cybersecurity. The concern stems from the realization that threat actors could leverage GenAI's prowess to amplify the scope and impact of ransomware attacks, particularly through the creation of large-scale advanced business email compromises. In a recent survey conducted by PwC, 52% of business and tech leaders said they anticipate GenAI causing catastrophic cyberattacks within the next 12 months.[3]

Moreover, Ransomware-as-a-Service (RaaS) is on the upswing, enabling even those with limited technical skills to launch attacks, fostering a broader threat landscape.

Phishing emails remain a popular choice among cybercriminals to distribute malware. It is estimated that 80-95% of cyberattacks begin with a phishing email.[4] With artificial intelligence (AI), machine learning (ML) and automation coming into the picture, phishing attacks are poised to intensify further with highly personalized and persuasive content in the foreseeable future.

To sum up:

- ***66%*** *of organizations faced a ransomware attack.*[5]
- ***83%*** *of them paid the ransom.*[6]
- ***70%*** *of SMBs said the impact of a ransomware attack would be a death blow to their organization.*[7]

> *"Even with payment, organizations may not fully regain lost capabilities, and cyber insurance is not a panacea, often proving challenging to acquire and falling short of providing complete reimbursement."*[8]
>
> ***— Respondents to the CISO Report***

Advances in ransomware

A glimpse into the latest cybercriminal trends

Ransomware merchants are constantly trying to up their game to get past security defenses everywhere. Here's a glimpse into what's new in the dastardly world of ransomware and trends that are expected to continue in 2024:

Upgrading ransomware code

Ransomware gangs are increasingly leveraging the Rust programming language to write ransomware codes. Rust is believed to be superior to C and C++ and provides better memory management, which is critical for malware's efficiency and functionality. New programming languages like Rust make static analysis challenging; therefore, malware written using such languages can bypass malware detection systems that have been designed based on the signatures of widely recognized and commonly used programming languages.

Exploiting known vulnerabilities

Ransomware operators are true opportunists. They constantly look for vulnerabilities, old as well as new, to exploit. The method used in many of the recent ransomware attacks involved exploiting known vulnerabilities in public-facing applications.[9] Threat actors start looking for unpatched systems as soon as a software patch is released.

Focusing on data theft rather than encryption

While encryption has been a key ransomware trait, threat actors are shifting their focus on stealing victims' data for higher payouts. Once data has been successfully exfiltrated, threat actors offer to handle the breaches discreetly. They use laws and compliance knowledge to pressure victims into paying higher ransom amounts. According to the Bitdefender 2023 Cybersecurity Assessment, over 70% of respondents from the USA revealed they had been instructed to keep a breach quiet, and 55% admitted to keeping a breach confidential even when they were aware it should have been reported.[10]

Utilizing RaaS for higher profits will continue

RaaS is a profit-sharing business model among ransomware groups. Cybercriminals can download the software either for free or for a very low fee. The goal is to trick targets into infecting their computer or generate even more revenue by locking an organization's network. Victims then get sent a ransom and payment deadline, and if they pay up, the original author gets between 5% to 30% commission — and the rest goes to the person who launched the attack.

Leveraging AI and automation

Like businesses, even cybercriminals are leveraging AI and automation to up their game. Threat actors are taking advantage of the latest technologies to automate tasks and minimize errors. The use of GenAI, ML and automation enables ransomware gangs to launch attacks more efficiently with less time and effort.

New variants

Blackcat ransomware typically targets big corporations that use outdated firewalls or VPN software. Blackcat, also known as ALPHV, gained popularity for attacking the European gas pipeline in July 2022.[11]

The Trigona ransomware had come to light in October 2022. The ransomware group used compromised credentials accessed through the Russian Anonymous Marketplace forum to gain initial access to targets. In 2023, Trigona exploited compromised Microsoft SQL and Linux servers.[12]

Akira is a ransomware family that's quickly gaining momentum. The Akira ransomware is popular for using double extortion techniques, wherein malicious actors steal victims' valuable data before encrypting files and devices.

Tools of the ransomware trade

An insight into how easy it is to be a cybercriminal

Bitcoin allows hackers to remain anonymous:

- *Over **15,000** businesses globally accept bitcoin.*[13]
- *In the fourth quarter of 2023, the number of ransomware-hit organizations increased by a staggering **66%** compared to 2022.*[14]
- *Fact: Ransomware payments hit a record high in 2023, exceeding **$1 billion**.*[15]

Resources for do-it-yourself ransomware attacks are plentiful. Part of the financial success of ransomware can be credited to the ability of the hacker to remain anonymous online. Payment is made as a non-traceable electronic payment. Bitcoin has become a widely accepted currency. There are over 30 merchant services that manage bitcoin transactions, including:

1. *Bitaps*
2. *BitBay Pay*
3. *Bitcoin Transaction Coordinator*
4. *BitcoinPay*
5. *BitcoinPaygate*
6. *BitKassa*
7. *BitPagos*
8. *BitPay*
9. *BitPOS*
10. *BitStraat SiteCite*
11. *Luno AP*
12. *Blockchain.info*
13. *Blockonomics*
14. *Coinbase*
15. *CoinBox*
16. *Cashila*
17. *CoinCorner*
18. *CoinGate*
19. *Coinify*
20. *CoinPip*
21. *Coinsnap*
22. *Cryptopay*
23. *Cubits*
24. *GoUrl*
25. *Lava Pay*
26. *OKPAY*
27. *PayFast*
28. *Paxful*
29. *Rocketr*
30. *SpectroCoin*
31. *SpicePay*
32. *XBTerminal*

Some of the major software that contribute to ransomware include:

- Cryptolocker
- TorrentLocker
- CryptoWall à CBT-Locker à TeslaCrypt
- Locky Unbreakable Encryption
- AES
- RSA
- Curve" ECC Network to C&C Server
- Tor
- 2P
- POST/HTTPS

Your personal files are encrypted!

Your important files produced on this computer: photos, videos, documents, etc., have been encrypted. Here is a complete list of encrypted files, which you can personally verify. Encryption was produced using a unique public key RSA-2048 generated for the computer. To decrypt files, you need to obtain the private key. Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

— CryptLocker

Top ransomware targets by industry

Education

According to Sophos' State of Ransomware 2023, the education sector experienced the highest number of ransomware attacks, with 80% of lower education and 79% of higher education reporting being hit.[16] Cybercriminals understand that educational institutions often utilize outdated technology and have limited budgets and IT resources, making them easy targets.

Central and federal government

The central and federal government sector experienced a significant surge in cyberattacks. Around 70% of respondents in a survey conducted by Sophos said their organizations have suffered ransomware attacks in the past 12 months. Cyberattacks against government agencies increased by a whopping 40% in Q2 of 2023 compared to Q1.[18]

Construction and property

The construction and property sectors witnessed an increase in ransomware attacks, with 71% of businesses saying they experienced a ransomware attack. In fact, as per Nordlocker, an encryption software firm, from January 2022 to January 2023, the construction industry experienced the highest number of ransomware attacks.[17]

Media, leisure and entertainment

The media, leisure and entertainment industries also saw an uptick in ransomware attacks, with 70% reporting they suffered a ransomware attack. Threat actors were able to encrypt data in 81% of those incidents. Among those organizations in the media, leisure and entertainment sector that were hit by a cyberattack, 60% revealed they lost a lot of business/revenue.

> *"To be honest, we often advise people to just pay the ransom [if they don't have backups]."*
>
> ***— Joseph Bonavolonta, Asst. Special Agent, FBI Cybercrime Boston Division***

Backup vendors are trying to scare IT pros

Vendor efforts to sell more product

Why are IT backup vendors trying to scare IT pros?

Backup vendors are trying to alarm IT pros to the point that they'll buy their software to fend off attacks. But the fact is, not all backups are safe. Windows-based backup vendors are more vulnerable to ransomware. Since ransomware programs are designed for Windows, files backed up on Windows are also a strategic target. Organizations are using the cloud to store data and ransomware programmers have created ransomware that can infect files kept in the cloud. Some ransomware strains, including a variant of Virlock that actually uses the desktop, syncs clients of popular cloud services to access and encrypt files stored in the cloud. For example, if the Google Document a person is working on locally gets encrypted, the encrypted file will sync with Google Drive. The bottom line is cloud storage is not backup. Backup means to have another protected, off-site copy of the data.

While ransomware teams try to garner revenue from any platform target, the preponderance of Microsoft Windows systems makes them far and away the most lucrative prey.

On the flip side, Unitrends Unified Backup is starting to scare malware distributors with the development of a ransomware detection process that really makes it tough to mount a successful attack.

Unitrends Unified Backup offers:

- *Hardened Linux*
- *Proactive monitoring and recovery testing*
- *AI-based alerting*
- *Immutable cloud*

Unitrends Unified Backup: Five arms of defense

Advances in ransomware

Five ways Unitrends Unified Backup helps defeat ransomware:

1. Protect

Unitrends Unified Backup provides both local and cloud protection options, giving customers 3-2-1 protection, i.e., 3 copies of your data — 2 different types of media — 1 copy off-site.

2. Secure

The transition away from malware-susceptible Windows backup software to a purpose-built, hardened Linux solution exponentially hampers hackers from launching successful attacks. By running on a hardened Linux platform, Unitrends backup appliances are resistant to malware and ransomware attacks.

3. Test

A key component of Unitrends portfolio's security capability is Recovery Assurance. It provides automated testing of recovery for backups — both local and in the cloud. Recovery Assurance secures the recoverability of mission-critical applications. Recovery will occur in the time required to meet an organization's IT service demands, no matter what causes the disaster or outage, whether planned or unplanned.

4. Detect

Uses adaptive and predictive analytics against backup data, designed to search for ransomware threat conditions. Algorithms use machine learning to forecast ransomware conditions. Proactive alerts are sent when ransomware conditions are detected.

5. Recover

Unitrends Instant Recovery lets their customers spin up their backup data on-premises in minutes, thereby deflecting any attempted attacks. Unitrends has created an iron-clad security platform — a virtual force field — to ensure that the digital assets of their clients are protected. The message for anyone trying to hack Unitrends Unified Backup's customers — Don't waste your time!

It's easier than ever to deploy. To carry out such a diversity of attacks, hackers have created hundreds of strains of ransomware, many of which are variations of readily available "off-the-shelf" malware.[19]

The force field of ransomware

True technology leaders set the bar instead of fighting to keep up with the pack. While ransomware pros continue to develop new techniques, Unitrends Unified Backup is transforming business by preventing successful ransomware attacks with an onslaught of game-changing defensive mechanisms for their users. Unitrends Unified Backup has created a virtual force field to stop attacks.

However, for ransomware distributors, many businesses have failed to keep pace with evolving cybersecurity technology, which leaves plenty of prime targets vulnerable and susceptible to ransomware attacks.

A quick recap

Opportunity

Ransomware is a billion-dollar industry and growing. Over 80% of attack victims paid the ransom.

Ransomware trends

Ransomware groups are increasingly targeting cloud data. They are leveraging Generative AI to amplify the scope and impact of ransomware attacks.

Advances in ransomware

Threat actors are using new programming languages like Rust to evade malware detection systems.

Top ransomware targets

The education sector, construction and property, central and federal government, and media, leisure and entertainment, remained top targets for cybercriminals.

Scared IT pros

Companies with security platforms try diligently to alert IT pros to the fact that they are prime ransomware targets. For the time being, IT pros are either ignoring the warnings or are adding insufficient protection, giving an added boost to the ransomware business.

Unitrends Unified Backup

Unitrends Unified Backup has thoroughly examined ransomware attacks from five distinct perspectives. However, there are plenty of enterprises that have yet to install Unitrends Unified Backup and are highly susceptible to ransomware attacks.

Ready to protect data and ensure business continuity in the face of disruptions? ***Request a demo today.***

Sources:

1. https://www.chainalysis.com/blog/ransomware-2024/#:~:text=Ransomware%20payments%20in%202023%20surpassed,ransomware%20is%20an%20escalating%20problem

2. https://www.ibm.com/reports/data-breach

3. https://www.pwc.com/bm/en/press-releases/pwc-2024-global-digital-trust-insights.html

4. https://www.securitymagazine.com/articles/99696-between-80-and-95-of-cyberattacks-begin-with-phishing#:~:text=Between%2080%2D%20and%2095%25%20of,begin%20with%20phishing%20%7C%20Security%20Magazine

5. https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

6. https://www.meritalk.com/articles/report-ransomware-victims-increasingly-pay-demands/#:~:text=In%20the%202023%20CISO%20Report,percent%20paid%20the%20ransom%20demand

7. https://www.datto.com/resources/ebook-dattos-smb-market-report-for-msps

8. https://www.splunk.com/en_us/form/ciso-report.html#

9. https://www.symantec.broadcom.com/ransomware-threat-landscape-2024

10. https://businessresources.bitdefender.com/bitdefender-2023-cybersecurity-assessment

11. https://www.beforecrypt.com/en/ransomware-variants/

12. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-trigona

13. https://www.fundera.com/resources/how-many-businesses-accept-bitcoin

14. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-threat-landscape-2024

15. https://www.chainalysis.com/blog/ransomware-2024/

16. https://www.sophos.com/en-us/content/state-of-ransomware

17. https://nordlocker.com/ransomware-attack-statistics/#get-in-touch

18. https://www.itsecurityguru.org/2024/01/23/public-sector-cyberattacks-rise-by-40-in-2023/

19. http://www.wired.com/2017/02/ransomware-turns-big-targets-even-bigger-fallout/