RESTECH
SOLUTIONS

A BEGINNER'S GUIDE TO
RANSOMWARE

WHAT SMBs NEED TO KNOW

WARNING:
With this ebook, we give you an insight into how simple and prevalent
ransomware attacks have become and share how sophistication on the
part of cybercriminals has improved the efficacy of these attacks.

Do not try this at home

OVERVIEW

IMAGINE BEING PART OF AN IT SEGMENT WITH SKY-ROCKETING GROWTH, MASSIVELY SUCCESSFUL WORLDWIDE DEPLOYMENT, ANNUAL REVENUE IN THE BILLIONS AND DOUBLE-DIGIT GROWTH PROJECTIONS. IT'S A HIGHLY LUCRATIVE INDUSTRY THAT IS CONSTANTLY EVOLVING, WITH NEW VERSIONS OF SOFTWARE BEING RELEASED AND DEPLOYED EVERY DAY.

Sounds like an industry you'd want to be a part of, right? Unfortunately, we're talking about ransomware.

Ransomware is a form of malware that encrypts a victim's data, rendering files, applications or entire machines unusable. The malware programming community continues to look for new targets. It's often a matter of opportunity. Organizations that have recently digitized operations, such as government agencies or medical facilities, or those with small security teams or little downtime tolerance, make for prime targets that threat actors aim to cash in on. After launching an attack and encrypting an organization's data, the perpetrator demands payment, usually by untraceable means such as cryptocurrency, in exchange for a key to unlock the encrypted files.

To put it simply:

▶ Threat actors launch targeted attacks via phishing, account takeover or other means.

▶ Ransomware locks victims' files with strong encryption, typically using RSA or customized symmetric-key algorithms.

▶ Payment is demanded for a private key to unlock encrypted data.

Barriers to entry in the ransomware industry are low. Open-source versions of ransomware are available to anyone looking to tap into this profitable market. The emergence of these open-source ransomware programs hosted on GitHub and hacking forums are expected to further spur the growth of these attacks in 2022 and beyond.

Even if the would-be perpetrators don't have the skills to create their own malware from free source code, they can still outsource development. Ransomware-as-a-service [RaaS] is a model that provides automatically generated ransomware executables for anyone who wants to attempt launching their own ransomware campaign.

RaaS is a variant of ransomware that is user-friendly and easily deployable. Cybercriminals can download a software kit either for free or a percentage-based fee. The goal of developers is to provide new variants to their subscribers, who then execute campaigns with the goal of infecting their targets' computers. Some subscribers may look to generate larger revenues by executing more widespread attacks against a larger organization's network. Once the payload detonates, victims are sent a ransom demand and payment deadline. If a victim pays the ransom, the original developer takes a commission — typically 5% to 30% of the ransom — and the rest goes to the individual or organization who launched the attack.

TO SUM UP:

56%

56% of organizations faced a ransomware attack[1]

50%

50% of it professionals believe their organizations are not ready to defend against a ransomware attack[2]

> " *These programs are freely available for anyone who has the basic knowledge needed to compile existing code.* "

ƎΞSTECH
SOLUTIONS

NEW VARIATIONS

1

SODINOKIBI

It is a Ransomware-as-a-Service variant that accounts for a third of all ransomware incidents as per IBM's Security X-Force. Sodinokibi spreads in several ways, including through unpatched VPNs, exploit kits, remote desktop protocols (RDPs) and spam mail. This variant may also be referred to as Sodin or REvil.

2

SNAKE

Gaining notoriety by wreaking havoc in the industrial sector, SNAKE ransomware is expected to create severe trouble in the coming years. Targeting industry control systems, SNAKE disables ICS processes, freezes VMs and steals admin credentials to further spread and encrypt files across the network.

3

RYUK

It is a popular variant used in targeted attacks against healthcare organizations (such as the attack against United Health Services). Ryuk is commonly spread by other malware (e.g., Trickbot) or through email phishing attacks and exploit kits.

4

PHOBOS

Another RaaS variant, Phobos has been observed in attacks against SMBs, where cybercriminals gain unauthorized access to a network via unprotected RDP ports. Phobos shows similarities to CrySiS and Dharma ransomware.

ADVANCES IN RANSOMWARE
A GLIMPSE INTO THE LATEST CYBERCRIMINAL TRENDS

Updates & Promotions - Teaser Key Codes, Localized Versioning and More

Ransomware merchants are constantly trying to up their game to overcome security and backup defenses. Let's take a look at some of the latest advances in ransomware:

Experts have long touted backup (collectively, "backup" may refer to dedicated backups, replicas or snapshots) as the best defense against ransomware. Unfortunately, cybercriminals know this too, and have focused resources and development on new variants designed to overcome backup defenses. The latest ransomware innovations have built phased attacks to defeat backups in a number of ways, typically by building in periods for gestation and / or dormancy.

1

GESTATION

Modern ransomware does not detonate and encrypt immediately. The gestation period is designed to give the malware time to spread as widely as possible from machine to machine, typically by using the permissions of the systems it has infected.

2

DELETION

Once the ransomware has spread as far as it can, the next phase involves deleting network-accessible backups. Backup files have known signatures that make them easy to target and encrypt. In addition to targeting file signatures, ransomware uses APIs published by backup vendors to delete backups autonomously.

3

DORMANCY

Once spread, ransomware typically does not encrypt or delete backups immediately. With access to data, threat actors may begin extracting data to later use for extortion. The malware may lie dormant for a month, three months, six months or even longer before detonation. Dormancy poses a challenge because malware is backed up along with legitimate data, creating an attack loop. When infected backups are used in recovery, the malware remains present and will detonate again.

Data exfiltration and the theft of usernames, passwords, personally identifiable information (PII), financial records and more is becoming increasingly popular among ransomware attackers. As per a recent report, roughly 50% of all ransomware cases involved data exfiltration, with the goal of increasing leverage against victims to pay ransom demands. Should the affected organization attempt to recover and leave the ransom unpaid, attackers threaten to release data publicly or post data for sale on the dark web.[3]

Of all ransomware attacks, 65% are delivered via phishing.[4] As threat actors engage social engineering to gain access to corporate systems, techniques such as business email compromise (BEC) and account takeover (ATO) attacks carry a significant risk of delivering a ransomware payload. Cybercriminals are tapping into social media sites and staging password or security alerts to prompt users to click. Some of the most common "in-the-wild" phishing subject lines are:[5]

- Microsoft: Abnormal login activity on Microsoft account

- Chase: Stimulus Funds

- Zoom: Restriction Notice Alert

- HR: Vacation Policy Update

- ATTENTION: Security Violation

- Earn money working from home

A variety of subjects based on social media trends and current events along with the impersonation of familiar entities, such as your company or bank, are being used to take advantage of heightened stress, distraction, urgency and fear in users. These attacks are increasingly effective because they have users reacting before thinking logically about the legitimacy of the email.
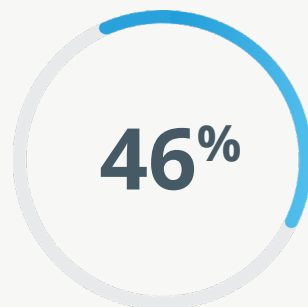
RANSOMWARE TRADE

AN INSIGHT INTO HOW EASY IT IS TO BE A CYBERCRIMINAL

Tips & Tricks To Get Started - Ransomware Resources

BITCOIN ALLOWS HACKERS TO REMAIN ANONYMOUS

46%

Nearly half (46%) of all businesses globally have faced a cybersecurity threat in the last 12 months.[6]

Resources for launching do-it-yourself ransomware campaigns are plentiful. The financial success of these attacks can, in part, be credited to the pseudonymous nature of processing ransom payments via cryptocurrency such as Bitcoin. Bitcoin is a highly liquid, decentralized, peer-to-peer digital currency, which makes it attractive for cybercriminals since payments are processed electronically without the need for a third-party intermediary. A charge processor, vendor or bank is not needed for verification of payment since every transaction is documented in a blockchain.

The blockchain's ledger is distributed across potentially thousands of machines. In the world of ransomware, Bitcoin has become a widely accepted currency. More than 30 merchant services help manage Bitcoin transactions including:[7]

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

PAST AND PRESENT:

Some of the Major Software That Has Contributed to Ransomware Include:

- Cryptolocker
- TorrentLocker
- CryptoWall

- Angler (Exploit Kit)
- CBT-Locker
- TeslaCrypt

- Locky Unbreakable EncryptioAES
- RSA

- Tor
- Curve ECC Network to C&C Server

Common Vulnerabilities and Exposures (CVEs):

Researchers at RiskSense identified 223 vulnerabilities associated with 123 ransomware families in 2021. This is an alarming increase from the 2019 findings of 57 CVEs tied to 19 ransomware families and indicates a shift towards attackers targeting data-rich applications such as SaaS. These included:[8]

- WordPress
- Apache Struts
- Java
- PHP

- Drupal
- ASP.net
- Jenkins
- MySQL

- OpenStack
- TomCat
- ElasticSearch
- OpenShift

- JBoss
- Nomad

RANSOM MESSAGE USED BY THE RYUK FAMILY OF RANSOMWARE.[9]

RYUKREADME.TXT

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted. Shadow
copies are also removed, so F8 or any other methods may damage encrypted data but
not recover.

We exclusively have decryption software for your situation. No decryption software
is available to the public.


DO NOT RESET OR SHUT DOWN – files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

This may lead to the impossibility of recovery of certain files.
Ryuk

No system is safe.
```

BIG MONEY HACKS

VICTIM STORIES FROM COMPANIES THAT PAID UP

Ransomware turns to big targets, aiming to hit where it hurts – and cybercriminals are cashing in.

Recent Hacks:

1

GRUBMAN SHIRE MEISELAS & SACKS

The New York-based entertainment and media law firm suffered an attack by REvil (Sodinokibi) ransomware. Perpetrators stole 756GB of data deemed "valuable" before encrypting the rest. Initial ransom demands were $21 million, and when it was turned down, the attackers published data relating to Lady Gaga online. The law firm refused an increased demand of $42M and the remainder of the stolen data was put up for auction on the dark web.[10]

2

WESTECH INTERNATIONAL

In early June, U.S. defense subcontractor Westech suffered a ransomware attack by "Russian-speaking" threat actors using the Maze ransomware variant. Sensitive data, including employee emails and payroll information was published, as data was again stolen before the encryption detonated. Based on the information published, it is possible military-related classified data may have also been compromised.[11]

3 DUESSELDORF UNIVERSITY HOSPITAL

In September, a woman died en route to the emergency room after her ambulance was forced to reroute when the closest hospital to the accident, The University Hospital of Dusseldorf, was shut down by a ransomware attack. More than 30 internal servers were disabled by the ransomware, forcing the hospital to halt all services, including the Emergency Room. This marked the first-ever reported human death due to ransomware and was investigated as a murder case by German authorities.[12]

4 CITY OF FLORENCE, ALABAMA

Ransomware attackers DoppelPaymer gained unauthorized access to the city's IT network with the help of compromised credentials belonging to the city manager. They shut down the city's email system and simultaneously compromised data stored in the municipality's database. The city had to cough up $291,000 in Bitcoin to retrieve access to the email system and recover lost data.[13]

> *Startups and small companies are most vulnerable to cybersecurity threats in the supply chain. Adversaries aren't going after a Lockheed Martin at the top, prime level. They're going after the small businesses [that a larger organization relies on] that are the most vulnerable.*

Katie Arrington, CISO
Office of the Undersecretary of Defense
for Acquisition and Sustainment.[14]

AGAINST RANSOMWARE

5 Ways a Good Backup and BCDR Solution Helps Defeat Ransomware

1 PROTECT

An effective BCDR solution provides both local and cloud data protection options, providing users with, at minimum, 3-2-1 data protection; 3 copies of data, 2 different media formats and 1 copy off-site. Replication to removable media, such as disk, helps create an air gap from the production network.

2 SECURE

Impede hacker efforts by transitioning from a malware-susceptible Windows backup software to a purpose-built, hardened Linux backup appliance. Hardening of the Linux kernel provides more resilience against malware and ransomware attacks.

3 TEST

Look for features such as Recovery Assurance. Recovery Assurance automates the testing of backups – both locally and in the cloud. Customizable boot orders, machine reconfiguration and application-level scripts provide testing for both simple and complex environments and validate applications and services can be successfully recovered. Compliance tracking ensures defined RTOs and RPOs are being met.

4 DETECT

Using adaptive and predictive analytics against backup data, a good solution is constantly on the search for ransomware threat conditions. Algorithms use machine learning to forecast threat conditions and proactive alerts are sent when ransomware conditions are detected.

5 RECOVER

Features such as Instant Recovery enable users to spin up tested, certified backup data on-premises in minutes, minimizing the impact of an attack. This provides a virtual forcefield around the platform that ensures the digital assets of customers are protected.

A QUICK RECAP

1 OPPORTUNITY

Ransomware is a billion-dollar industry and growing. Twenty-seven percent of attack victims pay the ransom. Threat actors are increasingly targeting susceptible organizations and finding new victims.

2 TOOLS OF THE TRADE

Ransomware-as-a-Service options, Bitcoin merchants and open-source software mean a high potential for new hackers to join the fray and get started quickly.

3 NEW & IMPROVED

Advances in programming and social engineering are ongoing. The functionality of attack malware and new versioning continues to improve the efficacy of attacks and grow revenues.

4 BIG MONEY HACKS

No industry is immune from attack. Larger organizations with proprietary data make for big ransoms, but actors are looking to target business partners, subcontractors and others who are closely involved with the top of the chain.

5 UNIFIED BCDR

Having a unified BCDR solution enables users to combat the threat of ransomware from five different angles. There are plenty of organizations that have yet to move away from outdated platforms or vulnerable windows-based solutions and remain highly susceptible to ransomware attacks.

COLLABORATE TO FIGHT

AGAINST RANSOMWARE

Equipped with game-changing defensive mechanisms for its users, a good backup and BCDR solution can help transform a business by preventing successful ransomware attacks. However, taking this path alone might be quite overwhelming since it will require a lot of additional time and effort. That's why, it is preferable to work with a specialist like us who can take the heavy load off your shoulders. Feel free to contact us for a consultation.

Sources

1. Helpnetsecurity/2020/11/20/faced-ransomware-attack

2. Helpnetsecurity/2021/04/16/human-attack-surface/

3. Securityboulevard/ransomware-trends-you-need-to-know-in-2021

4. IDA/Ransomware statistics that you need to see in 2020

5. Techrepublic/watch-out-for-these-subject-lines-in-email-phishing-attacks

6. Prnewswire/top-cyber-security-experts-report

7. Wall-street.com/an-untraceable-currency-bitcoin-privacy-concerns-2

8. Darkreading/ransomware-attackers-set-their-sights-on-saas

9. Research.checkpoint/ryuk-ransomware-targeted-campaign-break

10. Securityweekly/revil-prominent-law-firm

11. Securityboulevard/westech-international-hacked-by-maze-ransomware/

12. SecurityWeekly/first-fatality-caused-ransomware-attack/

13. Crn/the-11-biggest-ransomware-attacks-of-2020-so-far-/3

14. Fcw/dod-cyber-cmmc-rules-williams

713-936-6855
info@restech.solutions
https://restech.solutions/contact

RESTECH
S O L U T I O N S