TLP:CLEAR

INCIDENT RESPONSE METHODOLOGY

IRM #17
RANSOMWARE

Guidelines to handle and respond to ransomware infection

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

C'EST VOUS L'AVENIR

SOCIETE GENERALE

TLP:CLEAR

ABSTRACT

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.

WHO SHOULD USE IRM SHEETS?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

→ IRM CERT SG: https://github.com/certsocietegenerale/IRM

→ IRM CERT aDvens (French version): https://github.com/cert-advens/IRM

INCIDENT HANDLING STEPS

6 STEPS ARE DEFINED TO HANDLE SECURITY INCIDENTS

1. Preparation: get ready to handle the incident
2. Identification: detect the incident
3. Containment: limit the impact of the incident
4. Remediation: remove the threat
5. Recovery: recover to a normal stage
6. Lessons learned: draw up and improve the process

IRM provides detailed information for each step of the incident response process. The steps come from NIST Computer Security Incident Handling Guide.

PREPARATION

OBJECTIVE: ESTABLISH CONTACTS, DEFINE PROCEDURES, GATHER INFORMATION TO SAVE TIME DURING AN INCIDENT.

A good knowledge of :

- The usual operating systems security policies is needed.
- The usual users' profile policies is needed.
- Architecture, VLAN segmentation and interconnexions:
  - Have the capability to isolate entities, regions, partners or Internet.

Ensure that the endpoint and perimetric (email gateway, proxy caches) security products are up to date.

Deploy an EDR solution on endpoints and servers:

- This tool became one of the cornerstones of the incident response in case of ransomware or in large scale compromise, facilitating identification, containment and remediation phases.
- Launch EDR Search and AV scan with IOC explicit rules and get first indicators for remediation progress following.
- Set your EDR policies in prevent mode.

Since this threat is often detected by end-users, raise your IT support awareness regarding the ransomware threat.

Block IOCs linked to ransomware activities gathered by Threat Intelligence.

Deploy and operate security solutions enabling detection and facilitating response:

- Log gathering in a SIEM
- Have the capacity to run tools like YARA or DFIR-ORC (ANSSI)

Have a good log retention and verbosity

Define a strict posture versus the attacker

Prepare internal and external communication strategy

If a machine is identified with ransomware, unplug it from network and keep it turned on for memory forensics investigation

BACKUPS PREPARATION:

Make sure to have exhaustive, recent and reliable backups of local and network users' data.

You can follow the **3-2-1 backup rules**: each of these rules is meant to make sure that your data is stored in multiple ways.

So, if you're backing something up, you would have:

- At least three copies: three different copies mean three different copies in different places. By keeping them on different places, it reduces risk of a single event destroying multiple copies.
- In **two different formats**: this means that you must use at least two different methods to store your data. For example, DVD, Hard drive, Cloud services are different formats. But if you store two copies into two hard drive, here you will just use one format.
- With **one of those copies off-site**: Keeping one copy off-site ensures that even whatever happen where your data is (fire, break-in, natural disaster...) at least one copy is safe somewhere else. In this rule, cloud services make sense.

Try to use one backup format stored out of your network: even lateral movement happens from the threat that harm your network with encryption one copy will be out of reach.

IDENTIFICATION

OBJECTIVE: DETECT THE INCIDENT, DETERMINE ITS SCOPE, AND INVOLVE THE APPROPRIATE PARTIES.

GENERAL SIGNS OF RANSOMWARE PRESENCE

Several leads might hint that the system could be compromised by ransomware:

- Monitoring of ransomware IOCs by a SOC.
- Supervision of EDR alerts.
- Odd professional emails (often masquerading as invoices) containing attachments are being received.
- A ransom message explaining that the documents have been encrypted and asking for money is displayed on user's desktop.
- People are complaining about their files not being available or corrupted on their computers or their network shares with unusual extensions (.abc, .xyz, .aaa, etc.).
- Numerous files are being modified in a very short period of time on the network shares.
- Publication of information on the ransomware operator websites or forums.
- Lateral movement is usually done, check all connection to the AD and ShareFile server with privileged accounts at abnormal day time.
- Look for unusual network or web browsing activities; especially connections to Tor I2P IP, Tor gateways (tor2web, etc.) or Bitcoin payment websites.
- Look for rare connections.

Scoping of the incident:

- EDR or large-scale hunting tools like YARA or DFIR-ORC allows to make the scoping of the ransomware infected machines.
- The identification of the initial access and the pivot used by the attackers is the priority, as in Large scale malware compromise. This allows to establish the following phases actions.

The identification of the Threat Actor at the origin of the ransomware attack could help the following phases based on known TTPs.

Ransomware network compromise identification have many similarities with Large scale malware compromise. Most of the time, reaction decision must be taken faster in ransomware cases. For more details about Large scale malware compromise, please refer to IRM-18.

CONTAINMENT

OBJECTIVE: MITIGATE THE ATTACK'S EFFECTS ON THE TARGETED ENVIRONMENT.

- Make a public statement as soon as possible based on the communication template elaborated in the preparation phase.
- Follow the posture defined in the preparation phase.
- Send the undetected samples to your endpoint security provider and/or private sandboxes.
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider.
- Block traffic to C2s.
- Block any IP detected as used by attackers.
- Isolate compromised VLAN, interconnexion, entities, regions, partners or Internet.
- Disable accounts compromised/created by attackers.
- Disconnect all computers that have been detected as compromised from the network.
  - You could isolate with our EDR and shut down internet just keeping your EDR connections up.
- If you cannot isolate computers, disconnect/cancel the shared drives.
  - (NET USE x: \\unc\path\ /DELETE)

Monitor ransomware threat actor websites and Internet to find if there is any dataleak publication related to the ransomware compromise.

REMEDIATION

OBJECTIVE: TAKE ACTIONS TO REMOVE THE THREAT AND AVOID FUTURE INCIDENTS.

- Remove the initial access used by the attacker.
- Remove binaries used by the attacker to lateralize on the network.
- Remove any accounts created by attackers.
- Go back configuration changes.
- Operate a systems and network configuration hardening.

For more details, check the Large-scale malware compromise IRM-18

RECOVERY

OBJECTIVE: RESTORE THE SYSTEM TO NORMAL OPERATIONS

1. Update antivirus signatures for identified malicious binaries to be blocked.
2. Ensure that no malicious binaries are present on the systems before reconnecting them.
3. Ensure that the network traffic is back to normal.
4. Restore user's documents from backups.

Prioritize your recovery plan based on your DRP (disaster recovery plan).

All of these steps shall be made in a step-by-step manner and with technical monitoring.

- Verify that backups are not compromised: only restore from a backup if you are very confident that the backup and the device you are connecting it to are clean.

  OR

- Reimage the computer with a clean install.
- Reset credentials including passwords (especially for administrator and other system accounts).

Monitor network traffic to identify if any infection remains.

If possible, apply geo-filtering on firewalls to block illegitimate foreign country traffic.

Maintain the monitoring ransomware threat actor websites and Internet to find if there is any data leak publication related to the ransomware compromise.

For more details on authentication and infrastructure recovery, check the Large-scale malware compromise IRMXXX

LESSONS LEARNED

OBJECTIVE: DOCUMENT THE INCIDENT'S DETAILS, DISCUSS LESSONS LEARNED, AND ADJUST PLANS AND DEFENSES

Report

An incident report should be written and made available to all the stakeholders.

The following themes should be described:

- Initial cause of the infection
- Actions and timelines of every important event
- What went right
- What went wrong
- Incident cost
- Indicators of compromise

Capitalize

Actions to improve malware and network intrusion detection processes should be defined to capitalize on this experience.

TLP: WHITE

RANSOMWARE:
an enterprise perspective

ENJOY SAFER TECHNOLOGY™

CONTENTS

Author: Stephen Cobb
Acknowledgements: This white paper owes much to the work of my gifted ESET colleagues James Rodewald, Ben Reed, Fer O'Neil, and David Harley, and my talented team: Aryeh Goretsky, Bruce P. Burrell, Cameron Camp, and Lysa Myers.

GOALS AND EXECUTIVE SUMMARY

The goals of this paper are to explain why ransomware is still a serious threat to your organization – regardless of size – and what your organization can do to reduce exposure to, and damage from, ransomware attacks. Three ransomware attack vectors are addressed in this order: remote access, email, and supply chain. Primarily intended for an executive audience, the paper should be helpful to CEOs, CIOs, CISOs, and risk managers. The more technical aspects of ransomware response are included in Appendix B.

THE RANSOMWARE THREAT

A ransomware attack can be defined as an attempt to extort an organization by denying it access to its data. Ransomware is a subset of malware, a collective term for all forms of malicious code, including computer viruses and worms.

Ransomware attacks are different from denying access to data by permanently removing or erasing it, although some malware that presents itself as ransomware may destroy data (wiperware) and/or render systems inoperable (brickware). For example, the widely-reported and extremely costly 2017 outbreak of malware called NotPeyta/Diskcoder.C, is often lumped together with WannaCryptor/WannaCry in discussions of ransomware; however, NotPetya was a combination of wiperware and brickware, lacking the ability to decrypt files but also modifying the MBR code "*in such a way that recovery won't be possible*."

A ransomware attack is also different from a denial of service (DoS) attack which denies access to systems by overloading them with traffic but does not intentionally damage data. The capability to mount a DoS attack may be used by an extortionist to threaten a commercial website operator, *demanding payment* in return for not temporarily incapacitating down the site. Such attacks typically target organizations that operate retail websites because even a temporary site outage can significantly disrupt revenue. We also see *DoS attacks used for hacktivism*, as well as for *attacks on competitors*.

The idea of holding data and systems for ransom is not new. Donn Parker cited a case from 1971 in his landmark book Crime by Computer. Most security experts consider *Dr. Popp's AIDS trojan* of 1989 to be the first piece of encryption-based ransomware, meaning that the victim's files are encrypted by the attacker, who promises to decrypt them for a fee.

Fortunately, this first effort was not a trend setter and it was several decades before ransomware became a major category of computer crime. Although last year's outbreak of WannaCryptor managed to grab national headlines news, ransomware has been dominating the malware news for the past five years. For example, one of the five most visited pages on the *WeLiveSecurity website* is the article "*11 things you can do to protect against ransomware, including Cryptolocker*" written by ESET researcher Lysa Myers in 2013. Here are some other numbers that reflect the scale of the ransomware problem:

- Ransomware attacks rose 350% worldwide from 2016 to 2017 (Dimension Data, 2018)
- An increase in ransomware-related support inquiries in the past year was noted by 48% of IT consultants across 22 different industries (Intermedia, 2017)
- 25% of cyber insurance claims in 2017 were ransomware (AIG, 2018)
- Total losses due to WannaCry ransomware could reach $4 billion (Cyence, 2017)
- 72% of businesses hit by ransomware lost access to data for at least two days; 32% lost access for five days or more (Intermedia, 2017)

Regrettably, despite numbers like these, organizations are still being hit by costly ransomware attacks, even as rumors of ransomware's demise have begun to circulate.

YES, RANSOMWARE IS STILL A SERIOUS THREAT

If your organization has had a recent encounter with ransomware, then this white paper's goal – to explain why ransomware is still a serious threat to your organization – may sound like a statement of the obvious. However, if your organization has not been hit by ransomware lately, you might be under the illusion – created by some 2018 headlines – that this threat is fast receding into the archives of cybercrime:

- *The Decline of Ransomware and the Rise of Cryptocurrency Mining*
- *Cybercriminals Move from Ransomware Attacks to Crypto Mining*
- *Why cryptomining is the new ransomware*
- *Ransomware is so 2017*
- *Banking Trojans Replace Ransomware As Top Malware In Email For First Time Since 2016*

Of course, headlines don't tell the whole story, and in some of these articles you will find warnings that ransomware still remains a threat. Nevertheless, the use of terminology like "rise and fall" to describe malware trends obscures two important realities of cybersecurity: information system risks are cumulative, and criminal activity is hard to measure (*especially in cyberspace*).

Consider what has happened with illicit cryptocurrency mining, the unauthorized use of computing resources to create value in the form of digital money, such as Bitcoin, Ethereum, or Monero. Security researchers have documented a surge in this type of activity in 2018: criminals using a variety of techniques associated with phishing and other forms of malware distribution to get their value-generating mining code onto your computers. However, it is important to note that this type of illicit cryptocurrency mining is much easier for security vendors to detect and track than some other forms of cybercrime.

In essence, the headlines above reflect the fact that, while cryptomining detections have been rising, some of the more obvious indicators of ransomware activity have been declining; but to be clear, ransomware is still a threat to your organization. Indeed, it might be a bigger threat than ever. Why? Because in the last two years some criminals have been perfecting a different, more targeted approach to ransomware, one for which metrics are much harder to obtain.

We have seen a shift away from victimizing large numbers of people with ransom demands for modest sums of money and towards a targeted approach that goes for much larger ransom demands from a smaller victim pool that has deeper pockets (and can ill afford to lose access to data). This has resulted in headlines like this:

- *Atlanta ransomware attack may cost another $9.5 million to fix*
- *City of Farmington, N.M., recovering after SamSam ransomware attack*
- *Davidson County, N.C., Still Reeling from Ransomware Attack*
- *Ransomware Attacks Against Riverside, Ohio, Worse than Initially Thought*
- *Ransomware strikes CDOT for second time even as agency still recovering from first SamSam attack*, Denver, CO
- *MVSU Campus Loses Internet After Ransomware Attack*, Itta Bena, MS
- *Ransomware costs continue to climb for Wasaga Beach*, Ontario, Canada
- *Ransomware recovery a work in progress*, Coweta County, GA
- *Ransomware attack forces town's employees to go back to typewriters*, Anchorage, AK

While losing family photos to ransomware can be very painful, these headlines represent truly egregious cybercrimes that caused large financial losses and impacted millions of people. For example, after the City of Atlanta refused to pay the $50,000 ransomware demand, the costs kept climbing (and may end up being *close to $17 million*). Five city departments had to perform their jobs without computers for up

to a week: Corrections, Watershed Management, Human Resources, Parks and Recreation, and City Planning. Services impacted by the attack included the ability to accept online payment for water bills and traffic tickets. The Wi-Fi at Hartsfield-Jackson Atlanta International Airport was turned off for a week.

If you look closely at the above attacks you will see that the victim in each case is a public sector organization. So, does this mean that private sector businesses are safe from such attacks? Unfortunately, the answer is no. Commercial enterprises enjoy no sectoral immunity from targeted ransomware (or any other form of cybercrime, for that matter).

RANSOMING SCHOOLS, HOSPITALS, AND THE ENTERPRISE

The reason we are seeing headlines about ransomware attacks on public sector entities is because they are public, and public services were impacted. But that does not mean criminals are limiting their targeting to victims in the SLED sector (State and Local Government and Education). Consider another set of headlines:

- *Ransomware attack targets Adams Memorial Hospital*, Decatur, IN
- *ECMC spent nearly $10 million recovering from massive cyberattack*, Buffalo, NY
- *Hospital pays $55,000 ransom; no patient data stolen*, Greenfield, IN
- *Allscripts sued over ransomware attack, accused of 'wanton' disregard*,
- *LabCorp 90% recovered from SamSam ransomware attack*, Burlington, NC

These organizations are in the healthcare sector, another sector where it is difficult to hide a ransomware attack that impacts services, especially when government regulations may mandate disclosure, and *patient safety is at risk*.

But what about organizations that are not required to disclose data security breaches? It is reasonable to assume that a commercial enterprise which gets hit by a targeted ransomware attack will try to avoid headlines if at all possible. And that means we cannot rely on published reports of ransomware attacks to assess the scale of the threat. What we do know, from speaking to support staff at Managed Service Providers and security vendors, is that ransomware continues to be a costly crime with no shortage of victims.

Something else we know is that a number of these 2018 ransomware attacks on healthcare and government entities involved a family of ransomware known as SamSam (detected by ESET products as *MSIL/Filecoder.Samas*). SamSam has been around since 2016, exploiting several different attack vectors, but at the beginning of 2018 researchers began to suspect that SamSam attacks were penetrating organizations "by brute-forcing the RDP endpoints" (*US Department of Health and Human Services*).

THE RDP FACTOR

An RDP endpoint is a device, such as a database server, that is running Remote Desktop Protocol (RDP) software so that the device can be accessed over a network, such as the internet. If a user name and password are required to access the device then an attacker, having identified the server as a target, will make repeated attempts to guess these, often at a high rate of speed, hence the term: brute force attack. Absent any mechanism to limit multiple bad guesses, such attacks can be very effective.

Gaining unauthorized internet access to devices running RDP servers may require more upfront effort than email-based ransomware, but the RDP vector offers bad actors significant benefits, like the potential to evade endpoint protections and rapidly compromise multiple systems within a single organization. Consider the ransomware attack via RDP against Lab Corp, one of America's largest

clinical laboratories, in July of 2018; even though the company was able to contain the attack within 50 minutes, by that time it had already impacted 7,000 systems and 350 production servers (CSO).

Attacks via RDP can fly under the radar of many detection methods, meaning fewer metrics, and less threat awareness. For example, any organization with a mature information security program will detect and block a piece of ransomware embedded in a file attached to incoming email. Such incidents are typically logged and reported by endpoint protection programs and vendors of such programs aggregate anonymized threat trend statistics from such reports. The same is often true of efforts to trick users into visiting infectious websites that are propagating ransomware. However, if an attacker with system administrator privileges on a compromised server turns off the endpoint protection before directing ransomware to encrypt files on that machine, that attack may well elude typical malware metrics.

The purpose of RDP is to enable an organization's computing resources to be accessed remotely. There are numerous legitimate reasons for deploying RDP – for example serving up a large central database, or running a specialized software application shared between multiple users.

The company system that employees need to access remotely is referred to as a server. Employees connect to the server by running the RDP client software, for example on their laptops. When the network address of the remote system is entered, the client software reaches out to the designated port on the server (the default port for RDP is 3389 although that can be changed and probably should be). The server-side software presents a login screen that asks for a user name and password. You can see what this looks like on a Windows system in Figure 1.

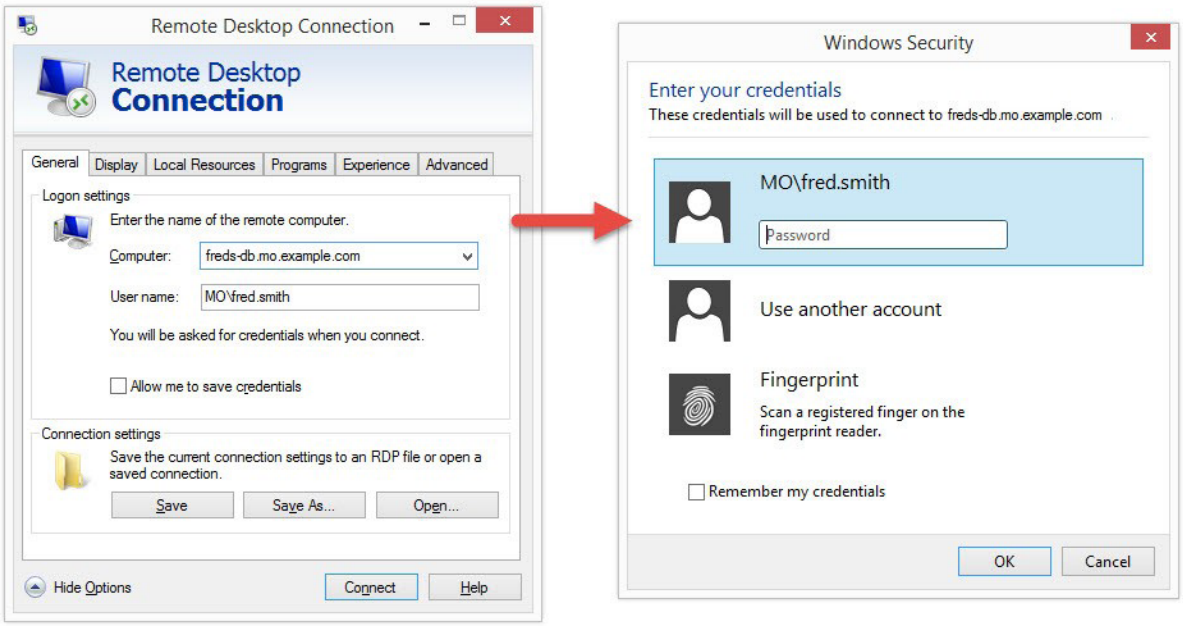


Figure 1.

As my ESET colleague James Rodewald points out, there are two main ways in which organizations use RDP. The first is to manage programs running on a server, for example a website or back-end database. In this scenario, the system administrator opens port 3389 to the outside world to allow remote management via an administrator account. A second use of RDP is to allow multiple non-admin users to log into a shared system to do normal everyday work. This can be done within the company network, or over the internet, in which case port 3389 is made accessible to the outside world.

For the criminally inclined, finding servers of either kind that are accessible to the outside world and then abusing them for malicious purposes is fairly straightforward because:

- Vulnerable servers are easy to find
- It is easy for attackers to obtain a foothold on RDP servers if they are in their default configuration
- Many RDP servers have default or weak configurations
- Tools and techniques for escalating privilege and obtaining admin rights on compromised RDP servers are widely known and available

Servers running RDP can be identified by specialized search engines like *Shodan*, which constantly scour the Internet for connected devices and collect information about them. As of September 1, 2018, Shodan indicated that there were over three million systems on the internet using *port 3389* (registration may be required to view filtered Shodan queries). As you can see from the Shodan interface in Figure 2, over one million of those systems were in the US.

Figure 2.

Using a different query, over two million machines were found to be *explicitly running RDP*. For an attacker, all of these machines are potential targets to be explored. While logging into an RDP server typically requires a user name and password, these can be surprisingly easy to for attackers to guess and many will yield to a brute force attack (repeated attempts to login in using a database of plausible credentials).

One shortcut for attackers who have sufficient funding is to simply purchase access to compromised servers. Server credentials are available in marketplaces on the dark web. For example, the xDedic website provides potential buyers with a wide range of information about its server offerings, allowing targeting that is both geographic and logistical (you filter and select by OS version, CPU, RAM, connection speed, installed applications, blacklist status, currently installed antivirus, and more). For more on the black market in credentials, see Appendix A.

Note that targeted ransomware is not the only reason for buying hacked server credentials. Indeed, xDedic's documentation helpfully lists 12 different uses for a compromised server, including sending spam, hosting malware, password cracking, mining cryptocurrency, and a range of activities for which anonymity is desirable and attribution is not; think fraudulent purchasing and money laundering. The site also offers tools for exploiting severs once you gain access.

Pivoting and living off the land

For the ransomware attacker, a compromised server can mean much more than extorting money to unencrypt the files on that machine, especially if that server can provide an entry point to an entire network of devices, potentially enabling large scale encryption of mission-critical data. That's what happened in many of the headline cases cited earlier, and the techniques for carrying out this type of attack are no secret.

Upon gaining remote access, the attacker will want to learn more about the compromised machine, evaluating its potential for abuse, including mapping connections to other systems. If access was not gained with admin credentials, several techniques can be used to "escalate privilege" to admin level. If there is endpoint protection installed on the system and it can be turned off by a user with admin privileges, the attacker will likely turn it off. This makes it easier for the attacker to download additional software, based on an assessment of the system's potential for abuse. (Note that when actions are described as being performed "by the attacker" they may not be performed by a person at a keyboard but by software used to automate aspects of an attack.)

Some attackers will try to introduce as little malicious code as possible in order to minimize the chances of detection. Instead, a strategy of "living off the land" will be employed, using legitimate software to extend network penetration. For example, the NotPetya malware used two popular tools, PsExec and Windows Management Instrumentation Command-line (WMIC), to achieve lateral movement in compromised networks. There are valid reasons for these programs to be executed and so detecting abusive use by an attacker can be difficult, although not impossible (see the later discussion of EDR tools, as in Endpoint Detection and Response).

The term "pivot" is used to describe the strategy of gaining a foothold on one system and using that to compromise all of the devices which can be reached from there. For example, in the attack on the hospital in Greenfield, Indiana, cited earlier, the attackers "utilized compromised account credentials to target a server located in the emergency IT backup facility utilized by the hospital – located many miles away from the main campus – and made use of the electronic connection between the backup site and the server farm on the hospital's main campus to deliver the SamSam payload" (*HHS Report*).

In addition to living off the land, ransomware attacks may take advantage of unpatched vulnerabilities in legitimate system software. For example, some ransomware spreads by using the *EternalBlue exploit* which targets a vulnerability in some versions of Microsoft's implementation of the Server Message Block (SMB) protocol (see *Microsoft Security Bulletin MS17-010*). Unpatched instances of this network filesharing protocol were infamously abused by the WannaCry ransomware (except on systems that were running endpoint protection products that *block EternalBlue*).

Of course, it is possible that in some cases an attacker's first point of contact with an organization will be a server running a mission critical database, in which case an opportunistic criminal may decide to save some time and effort and go for a quick win by simply encrypting and ransoming the files used by that one asset.

Defending against RDP ransomware attacks

Fortunately, it is possible to defend servers running RDP against unauthorized access and thus deny criminals this increasingly popular attack vector, whether they are purveying ransomware or engaged in some other abuse of unauthorized system access. While defensive strategies are covered in this section, a more technical checklist of anti-ransomware techniques is provided in Appendix B.

Of course, your organization may already have policies in place to address remote access security. You might have rules requiring all RDP access to be routed over a VPN (Virtual Private Network), secured

by 2FA (Two Factor Authentication), limited to specific roles, on specific systems that are configured securely, patched promptly, monitored constantly, firewalled appropriately, and backed up regularly.

However, it has to be said that, whether you have such rules in place or are working towards putting them in place, rules alone will not ensure your remote access is not hacked. You still have to make sure everyone is complying with the rules, while also being prepared to handle an attack that somehow succeeds despite those rules.

A foundational first step in defending against RDP ransomware attacks is to inventory your internet-facing assets. To say that you cannot defend a system if you are not aware of its existence might sound like a statement of the obvious, but based on our investigations the following scenario is not that unusual: an organization is attacked via an internet-connected asset of which the organization's security folks were not aware until after that attack.

You need processes in place to ensure that does not happen to your organization. For example, it should not be possible for either a contractor or an employee to connect either a physical or a virtual server to both the organization's network and the internet, unless that server is securely configured; said configuration must occur before the server goes live, particularly if the server is running RDP with a domain admin account.

Case study: The CDOT Cyber Incident

According to a *report released to the public*, the attack vector for the ransomware attack on the Colorado Department of Transportation (CDOT) that occurred in February of 2018 was an internet-connected virtual server that was compromised within two days of its creation. The attackers "broke into the Administrator account using approximately 40,000 password guesses until the account was compromised".

When you have finished creating your inventory of internet-facing assets, you need to document which ones have remote access enabled, and then decide if that access is necessary. If access is necessary, determine whether or not it is feasible to place those systems on the internal network and access them using a corporate VPN.

If a system does have to be accessible from the public internet via RDP, and using a VPN is not feasible, at least install 2FA so that you are not relying on passwords alone for protection. However, be sure to use a *2FA solution that is not SMS-based*. Criminals have plenty of ways to *thwart SMS-based authentication* (often developed by malware authors targeting customers of banks in Europe, where *SMS-based 2FA* has been used for many years to confirm banking transactions).

If you are forced to rely on passwords because 2FA is available – possibly due to short-sighted budgetary policy – at least stop would-be intruders making repeated attempts to guess credentials. Set a threshold of maybe five invalid login attempts, after which no login attempts are recognized for a set period of time, for example, 30 minutes. In Figure 3 you can see what this looks like in Windows.

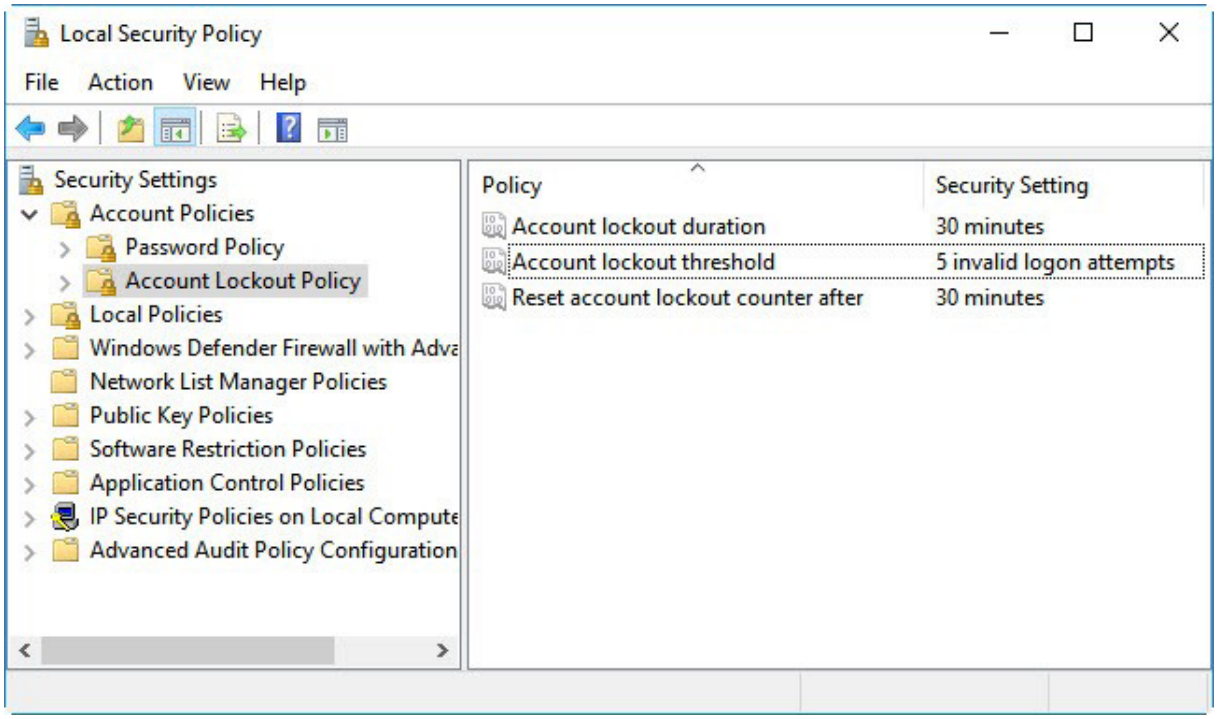


Figure 3.

You can also change the RDP listening port from 3389 to something else to make accessible machines harder for attackers to find. This can be done through system settings, but you will also need to change firewall rules to accommodate the designated port. Bear in mind that this is merely security by obscurity and should not be relied upon to keep RDP systems safe (see Appendix B for more details).

Hardening and patching should be performed for all remotely-accessible devices. One reason that WannaCry ransomware spread so quickly was that there were so many unpatched instances of SMB. In addition to making sure that all security vulnerabilities are identified and remediated, you want to make sure that all non-essential services and components have been removed or disabled, and that settings are configured for maximum security. For example, on Windows systems you can use Software Restriction Policies (SRP) to prevent files running from folders such as AppData and LocalAppData that are sometimes used by malware.

Of course, the last line of defense against RDP ransomware is a comprehensive and well-tested backup and recovery system. Given that backup is key to surviving ransomware regardless of attack vector, it will be discussed after two more vectors are considered.

Ransomware via email and other vectors

As any seasoned security expert will tell you: threats to information systems are cumulative. For example, just because some criminals have shifted their focus to remote access-enabled servers as a ransomware attack vector does not mean you can ignore the other vectors. Some criminals are still using email attachments to install ransomware. They may use this vector to install ransomware on the email recipient's machine, or to establish a foothold on a networked machine within an organization. That foothold can be the basis of an attempt to encrypt files throughout the organization, prior to making a very large ransom demand, as in the case of targeted ransomware attacks via RDP described earlier.

When it comes to protecting your organization against ransomware attacks via email, the first line of defense is filtering all incoming email for spam and phishing messages. There were several good reasons

for doing that even before email became a conduit for ransomware, and many organizations already have basic spam filtering and phishing detection in place.

You may want to go a step further and implement blocking of all attachment types that your business does not normally use; however, the suitability of this strategy will depend on the type of business you are in and may involve changing some work habits (for example, if employees are in the habit of emailing each other Excel spreadsheets and Word documents the organization may want to adopt a secure file sharing solution).

Next, you want to make sure that all endpoints are running top quality endpoint protection (EPP) software that will stop employees going to web pages that are known to be hosting malware. You may also want to use web content filtering as an added layer of protection (as well as blocking malicious websites, a web content filter can prevent employees visiting any websites deemed inappropriate for work use).

Your EPP should be centrally managed to enforce relevant security policies, such as limiting the ability to turn off antivirus protection or introduce removable media. Make sure that all endpoints are running the latest version of the product, and that it is successfully retrieving updates. If your EPP vendor has a cloud component, make sure this is turned on, because it enables even faster reaction to new threats (ESET calls this component LiveGrid®).

Prompt and comprehensive patching of operating systems and applications will help to prevent ransomware entering via email attachments or drive-by infection. Secure configuration can also be helpful. For example, consider using Group Policy to completely disable Microsoft Office macros. This will limit your ransomware attack surface, although this may not be feasible if the organization's workflow relies upon macros.

These days there can be little doubt that security is a shared responsibility, so make sure that your employee cybersecurity training is up to date and reflects the latest trends in email-borne ransomware. According to Ben Reed, who led the development of ESET's *free cybersecurity awareness training*: "You can reduce the number of malware incidents that your company has to deal with by letting employees know what to look for and what to avoid when it comes to phishing and other malicious content."

Make it clear to employees that they should report suspicious messages and attachments to the help desk or security team right away. In addition to the potential to prevent or limit damage, early warnings can help the organization tweak its spam and content filters, and bolster its firewalls and other defenses.

RANSOMWARE, SUPPLY CHAIN, AND DRIVE-BY INFECTION

Two further ransomware attack vectors that warrant close attention these days are the software supply chain and drive-by compromises. Just as ransomware dates back to the last century, so do software supply chain risks. Back when the primary attack vector for computer viruses was computer disks, and computer disks were the main way that people acquired software, malware would sometimes end up on production disks, or on the *disks of trial software* that used to be distributed with computer magazines.

Last year, in an award-winning piece of research, ESET discovered that a legitimate accounting software application was used by criminals to push *the NotPetya/DiskCoder.C malware*. The attackers penetrated the software company's update servers and added their own code to the legitimate application update files. When users of the accounting software clicked to install program updates, they were also installing a malware backdoor, opening the way for ransomware. The first line of defense against this type of attack is a good endpoint protection product, backed up by EDR tools.

An ironic version of software supply chain malware distribution is the "abuse" of software cracking sites. These sites exist to share information on how to defeat licensing restrictions on legitimate software, including providing code that can be downloaded to crack those restrictions. In 2018, researchers discovered that the GandCrab ransomware, detected by ESET as *Win32/Filecoder.GandCrab*, had been disguised as a free download of cracking code (as reported by *Bleeping Computer*). Risks from this avenue of attack can be reduced by endpoint protection products together with employee education as to the dangers of such sites, as well as their dubious legality and ethics.

Researchers have also detected a resurgence of the "drive-by" vector as a means of carrying out ransomware attacks, compromising visitors to specific websites. A piece of ransomware that ESET detects as Win32/Filecoder.Princess has been spread using this technique (hat tip to Malwarebytes Labs). To execute a drive-by attack the bad actor installs code known as an exploit kit on a website. This can be a legitimate site that has been compromised for this purpose or a site made by the attacker so that victims can be directed there. When someone visits a website that is hosting an exploit kit, the malware will compromise the visitor's machine using one of a number of different exploits, based on the configuration of the visitor's machine (for example, if the machine is running an unpatched web browser a known vulnerability in that version of the browser can be exploited). Defending against this type of attack involves keeping up with patches, using endpoint protection software, and educating users about unsolicited emails that encourage them to visit unfamiliar websites.

CLOUDS AND SEGMENTS

Whatever attack vector is employed by ransomware, if it gets into your organization there is a fair chance it will try to spread to as many machines as possible. In the case of Lab Corp, cited earlier, thousands of machines were hit in less than an hour. When NotPetya hit the network of shipping giant Maersk it rapidly impacted *45,000 PCs and 4,000 servers*. Clearly, limiting the number of machines that an attacker can reach from a single entry point has significant benefits as a defensive strategy. There are several approaches to implementing such a strategy, notably network segmentation.

A discussion of network architecture is beyond the scope of this paper, and converting a broad and easily traversable "flat" network into a segmented one can be both challenging and expensive (*this KPMG report* provides a useful perspective). However, every organization needs to understand the security strengths and weaknesses of its current network architecture. A simple, interview-based audit can improve that understanding by asking "can I get from here to there?" or "what is stopping someone from getting from there to here?"

If those questions had been asked at Target before the November, 2013 breach, the company might have avoided the now infamous intrusion that went from a trojan-bearing phishing email – clicked on by an employee at one of the giant retailer's HVAC contractors – all the way to malware on the Point-of-Sale terminals in its stores. If ransomware had been deployed through those same connections it is conceivable that the damage to Target could have been even worse than the massive credit card theft it sustained.

A popular system architecture strategy in recent years has been to move data to the cloud, but the cloud provides no automatic immunity from ransomware attacks (despite efforts by less scrupulous vendors to create the impression that cloud = security). In fact, the low cost and relative ease with which new servers can be provisioned in the cloud and connected to the rest of the organization's digital infrastructure has made the cloud a fertile hunting ground for criminals. The ransomware attack on CDoT cited earlier came via an internet-connected virtual server that was compromised by a brute force attack within two days of its creation. Clearly, any use of the cloud by any part of the organization needs to be properly authorized and securely configured. Also, like all other systems, those in the cloud need to be enrolled in an appropriate backup and recovery regimen.

PATCHING AND BACKUP AS RANSOMWARE DEFENSE

Patching and backup are two aspects of operating and administering systems that play vital roles in defending against a ransomware attack. Patching of systems closes off potential avenues of attack and can prevent ransomware getting into your organization, or if it does get in, reduce the damage it can do. For example, organizations that promptly patched the Windows File and Printer Sharing service (SMB) in the wake of Microsoft Security Bulletin MS17-010, were protected against the EternalBlue exploit used to spread WannaCryptor and NotPeyta within organizations.

Of course, as any system administrator knows, patching can be a lot more complicated than it sounds. Patches and updates need to be tested before they are deployed. Some of your organization's systems may have software dependencies that are broken by upgrading to the latest version of an application or operating system. However, the high price of ransomware getting into your network – in the hundreds of millions of dollars for some companies hit by NotPetya – justifies the effort to address those challenges and maintain a prompt and thorough patching regimen to keep ransomware out.

It is often said that if ransomware does get into your organization – be it via RDP, email, the software supply chain, or malicious insider – a comprehensive and properly managed backup and recovery program can be your best line of defense. There is a lot of truth to this – and a lot of good reasons to have such a program – but bear in mind that some ransomware attacks are executed over a period time, during which the ransomware may also be backed up, compromising the potential for a smooth recovery. That is why backup is not a set and forget defense, it needs to be monitored and managed, and the recovery process needs to be regularly tested.

Fortunately, these days there are more options than ever for backup and recovery, notably cloud storage, whether remote, on premise, or hybrid. However, there is also more data to be backed up, from more places. Unless you have a comprehensive backup strategy there is always a chance that the purveyors of ransomware will find that one device that you did not back up. According to the backup experts at *Xopero*, a member of the ESET Technology Alliance, comprehensive backup includes data and system state on all endpoints, servers, mailboxes, network drives, mobile devices, and virtual machines.

Detailed discussion of enterprise backup and recovery strategy is beyond the scope of this white paper, but it should be clear that having such a strategy is more critical than ever these days. Ransomware simply adds to the long list of reasons your organization should not stint on this part of the IT program, but, as ESET Senior Research Fellow David Harley pointed out in "*Trends 2018: The ransomware revolution*," there are some caveats specific to ransomware. For example: "when storage is 'always on', its contents may be vulnerable to compromise by ransomware in the same way that local and other network-connected storage is". Harley recommends that offsite storage:

- Is not routinely and permanently online.
- Protects backed-up data from automatic and silent modification or overwriting by malware when the remote facility is online.
- Protects earlier generations of backed-up data from compromise so that even if disaster strikes the very latest backups, you can at least retrieve some data, including earlier versions of current data.
- Protects the customer by spelling out the provider's legal/contractual responsibilities, what happens if the provider goes out of business, and so on.

Harley also warns against underestimating the usefulness of write-once media for archiving data, pointing out that files stored on media that is not rewritable are immune from the predations of ransomware.

Of course, there are many other reasons why your organization needs a backup and recovery program – such as recovery from fire, flood, storm damage, and so on – and there is one reason backup may not

RESPONDING TO A RANSOMWARE ATTACK

In addition to erecting defenses against ransomware, every organization needs to be prepared to respond to any attack that succeeds in penetrating those defenses. Fundamental to this preparation are company security policies updated to cover ransomware. You need to spell out how employees at all levels should respond to ransomware demands. Make sure your policies answer these questions:

- To whom should employees report suspected ransomware?
- What is company policy on paying ransomware demands?
- Who is allowed to pay/negotiate ransoms payments?

Policies should be crafted to avoid the following problems:

- Employees not reporting suspected ransomware for fear of retribution.
- Network admins paying ransoms because it is easier than recovering systems from backups.
- Unauthorized release of information about actual or suspected ransomware attacks.

After updating your information security policies to address ransomware, you need to make sure that your security awareness and employee training programs include appropriate ransomware-related content.

You will also want to make sure your Incident/Crisis Response Plan is ready in case of a ransomware attack. Here's an outline of the ground that your response plan needs to cover:

- At first signs of attack, notify designated personnel
- Isolate and analyze affected machines
- If attack confirmed, activate Incident/Crisis Response Team
- Alert legal counsel
- Contact vendors who may be able to assist
- Remind employees of press and social media policy
- Assess attack scope and specifics of ransomware (if a key available)
- Contact law enforcement
- Prepare a holding statement
- If files have been encrypted determine whether they can be restored from backup
- Keep employees updated on status
- If necessary, activate business continuity plan

It is a good idea to have at least one ransomware scenario in your crisis planning playbook and to go through it in a table top exercise with relevant personnel, including executives. This can reveal gaps in backup and recovery plans, and help you anticipate the impact of not being able to access basic services due to systems being encrypted (services like email, VoIP phones, and internet access).

ENDPOINT DETECTION AND RESPONSE

There is one category of security software that can help to limit the impact of ransomware attacks and strengthen your response to them: endpoint detection and response tools, or just EDR for brevity. Either as a collection of internally-developed tools or an integrated security product, EDR can be used to assist manual threat-hunting efforts on your networks as well as automate a wide range of defensive measures. In Figure 4 you can see several ransomware-related EDR rules designed to alert security personnel to suspicious activity (this particular EDR is *ESET Enterprise Inspector*).

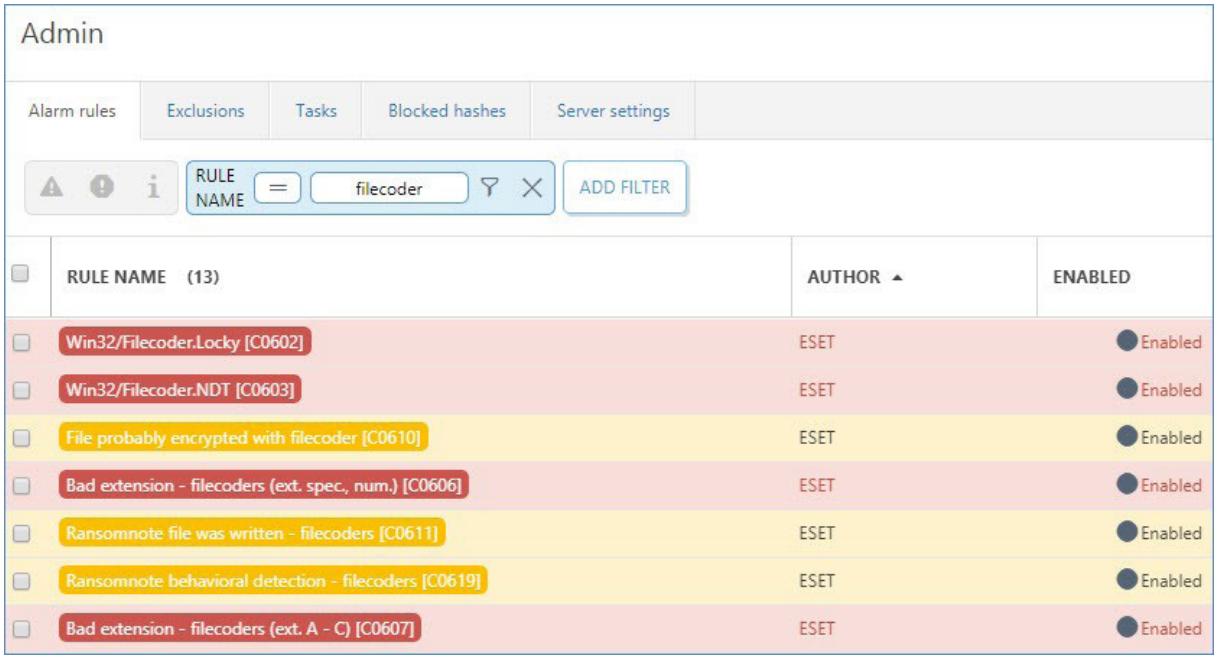


Figure 4.

An EDR can monitor all of your organization's endpoints for suspicious activity like the changing of file extensions typically seen in a ransomware attack. You security team would definitely like to be alerted to the presence of attack tools like Mimikatz, created to steal user credentials from memory, or xDedicRDPPatch, used in the creation of additional users once you have accessed a server via RDP (it is available from the previously mentioned xDedic website).

Early warning signs of intrusion can be coded into rules and alarms. These can be continually refined with fresh data from threat intelligence such as indicators of compromise (IOCs). A good EDR will have rules that enable the operator to find compromised systems immediately once a rule is triggered, isolate those systems, and then diagnose the problem, including rolling back the history of commands executed by the affected systems. These capabilities mean an EDR can increase your security team's ability to thwart attacks, respond to attacks, and perform forensic analysis after an attack.

A WORD ABOUT RANSOMWARE PAYMENT

That word is: don't. Why? Because paying the criminal who has encrypted your files means:

- You are validating the business model behind the crime
- You are encouraging criminal activity
- You may be hit with further demands for money and future attacks

Furthermore, paying the criminals who have encrypted your files by no means guarantees that you will get the decryption key; after all, it's not like you can take them to court or report them to the Better Business Bureau. There are numerous reasons that paying may not get your files back:

- The ransomware does not work properly – coding errors in malware are notoriously common.
- There are numerous ways in which the process for delivering the decryption key fails.
- The attacker is acting in bad faith and has no plans to provide decryption keys.

The above should be sufficient to deter organizations from paying ransomware demands, but to underline this advice, here is what the *FBI says about paying*:

"Paying a ransom doesn't guarantee an organization that it will get its data back – we've seen cases where organizations never got a decryption key after having paid the ransom. Paying a ransom not only

emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

In practice there appear to be two arguments for paying the ransom, the first being "we cannot restore the encrypted information from backups". This could be because the backups do not exist or they do exist but they are damaged in some way. However, there may be alternatives to paying up. As *David Harley has suggested*: "Before paying up, check with your security software vendor (a) in case recovery may be possible without paying the ransom (b) in case it's known that paying the ransom won't or can't result in recovery for that particular ransomware variant.

The second argument for paying the ransom is that "it's cheaper than restoring from backups." If this statement is based solely on time and labor calculations, it might be technically correct, but the decision to pay is nevertheless deeply flawed for the reasons stated earlier, notably the unreliability of decryption promises and the probability of being attacked again after the first payment – after all, you are not dealing with law-abiding citizens.

You may have heard that some purveyors of ransomware offer victims proof that the decryption works. This does happen, but can lead to even more problems, as in the recent *Health Management Concepts* breach. Suppose the attackers have you send them an encrypted file which they then decrypt and send back to you as evidence of good faith; you have just facilitated disclosure of the contents of that file to persons of dubious moral character.

Here is one further complication to consider, *pointed out David Harley*: "bear in mind that removing active ransomware with security software that detects ransomware is by no means the same as recovering data: removing the ransomware and then deciding to pay up means that the data may no longer be recoverable even with the cooperation of the criminals, because the decryption mechanism is part of the malware." In other words, if you decide to pay, proceed with caution.

THE FUTURE OF RANSOMWARE

Demanding money to restore access to systems and data targets the "A" in CIA, the classic security triad of Confidentiality, Integrity, and Availability. In essence, ransomware leverages an organization's dependence on technology and so the more that organizations come to depend upon technology, the greater the scope for ransomware. That means we can expect ransomware to persist and evolve in the future (barring unforeseen shifts in global politics and economics).

Based on our experience with malicious code over the past thirty years we can say that malware threats tend to evolve like this:

- vulnerabilities in a new technology are discovered and their potential for criminal abuse is discussed;
- efforts to remediate and mitigate those vulnerabilities begin;
- attempts at criminal abuse of the latest technology are at first rare because criminals are making easy money from established strategies;
- absent widespread criminal abuse, remediation and mitigation efforts lose steam;
- eventually criminals discover that this "new" technology is ripe for exploitation;
- a new malware trend emerges.

Examples in recent years are the distributed denial of service attacks that leverage internet-connected surveillance equipment (*Mirai*) and the emergence of router malware (*VPNFilter*). In terms of ransomware, the explosive growth in the deployment of poorly-secured IoT (Internet of Things) devices is creating a fertile landscape for future efforts, as is the increasing use of internet-connected industrial control systems, smart buildings, and vehicles, including autonomous vehicles (see the article "*RoT: Ransomware of Things*" and the webinar "*Ransomware Today: What's New, What's Coming Next*").

Several scenarios are plausible if a drop in the revenues from more established cybercrimes lead criminals to pursue new schemes. Malware on routers could potentially limit or block traffic until a toll is paid, backed by threats to brick the router, or reveal traffic content, if you try to remove the malware.

Remote locking of vehicles, homes, and buildings could be abused for extortion. Manipulation of BAS (building automation systems), such as those controlling HVAC (heating, ventilation, and air conditioning) could serve as a basis for extortion schemes (we are seeing signs of this already). As for commercial robots, the feasibility of ransomware attacks on them has already been *demonstrated*.

These evolving ransomware scenarios have multiple implications for enterprises. The following responses are recommended:

- Start to address these potential threats in your risk management strategy and planning
- Begin to get a handle on "ransomable" assets now: IoT devices, SOHO routers, robots, control systems, autonomous systems
- Track vulnerability reports related to these assets
- Keep up with patching and firmware updating of these assets
- Segment IoT devices and other new technologies from production networks

These recommendations will also help your organization defend against another trend in crimeware evolution: cryptomining, the unauthorized use of computing assets to generate cryptocurrency, such as Bitcoin, Litecoin, Ethereum, and Monero. As was noted earlier, many criminals are already looking to cryptomining for additional revenue streams. It was also noted earlier that cyber threats tend to accumulate, and it is not unreasonable to predict a future blend of ransomware and cryptomining. For example, compromised systems could be held hostage until a certain amount of digital currency was mined. Alternatively, an organization with a large number of IoT devices is compromised by a cryptomining scheme then receives an extortion offer: pay X amount and we stop the mining.

SUMMARY

For several decades now, we have witnessed a global struggle to prevent malicious code from undermining the technology upon which so much of modern life now depends. The parties to that struggle include, on the one side, financially motivated criminals, agenda-driven activists, agents of ethically challenged governments, and occasionally some hoodie-wearing code junkies who haven't properly thought things through. On the other side are companies and consumers and any organization that has data which could be leveraged or destroyed by someone with criminal intent.

Gaining the upper hand in this struggle begins with understanding the attackers and attack vectors. Naturally, these evolve over time, but in a cumulative manner. The fact that criminal abuse of computing resources to mine cryptocurrency has surged recently does not mean that there is a shortage of criminals to develop and deploy RDP exploitation techniques in order to create a profitable attack vector for ransomware. Likewise, battening down your organization's use of RDP – which needs to happen for a variety of good reasons – does not mean anti-phishing training should be neglected.

Along with effective employee education, you need: sound security policies that are comprehensively applied and firmly enforced; the right mix of security products and tools, including tested backup and recovery systems; and a constantly updated incident response plan. Even with all of these, plus constant vigilance, you are not guaranteed immunity from attack; you can however greatly increase your odds of deflecting attackers, and recovering from an attack.

Until the world's economies improve dramatically and its governments achieve global détente, the struggle against cybercrime will not only continue, it will also expand, along with the benefits that

society reaps from new technologies. Hopefully, by explaining why ransomware is still a serious threat to your organization and what can be done to defend against it, this white paper will help to secure those benefits while minimizing losses caused by bad actors.

APPENDIX A:

Ransomware attacks via RDP are fueled by the commercial availability of compromised credentials in dark markets. In Figure A1 you can see what one such market, Ultimate Anonymity Services or UAS, appears like to a customer seeking to buy credentials that grant admin rights on an RDP server in Florida:

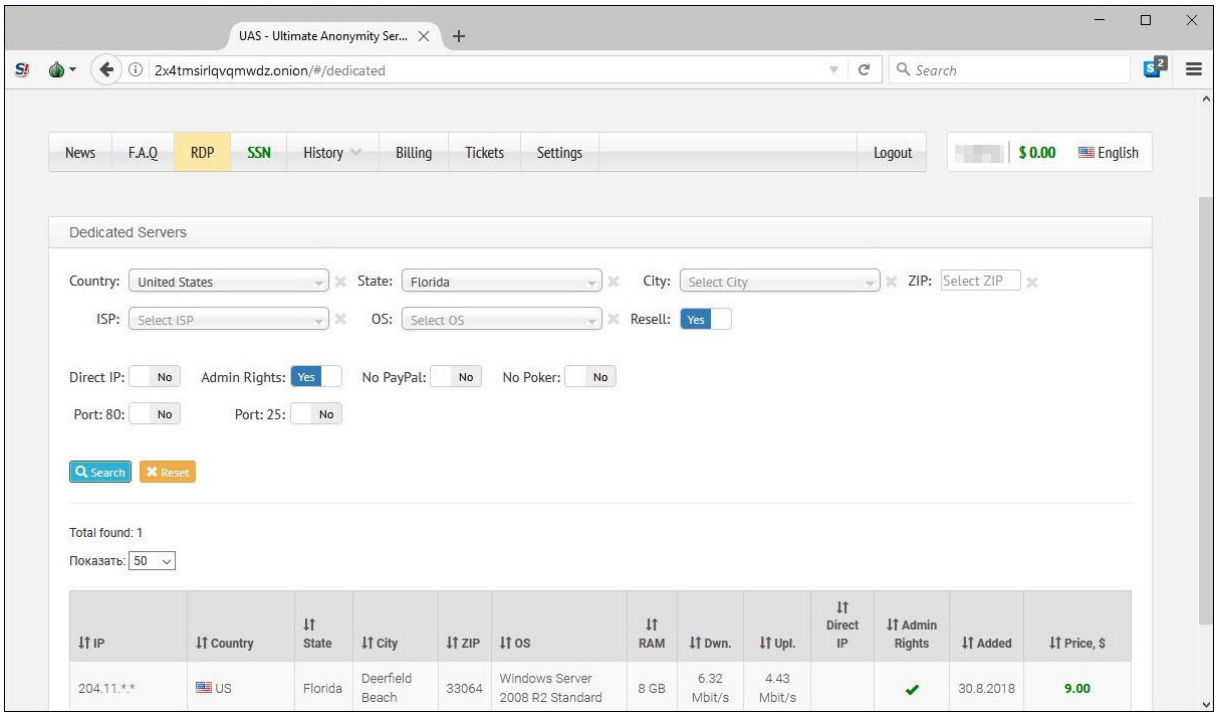


Figure A1.

Note the wide range of search filters that allow buyers to fine-tune their selection of victims. Also note the level of detail provided about the listed item. The price for credentials on the Windows server shown above is $9.00 US. A larger but typcially more expensive RDP market is xDedic (for dedic-ated server). Since its inception in 2014, xDedic has attracted hundreds of credential sellers from around the world – people who hack servers to gain access and then list that access for sale.

Somewhat surprisingly, Xdedic did not start out on the dark web but it moved behind a paywall on the Tor network after several investigations and articles by security researchers (hat tip to Kaspersky). These days, would-be criminals need to buy a $200 invite to get an xDedic account. In addition, they need to immediately depost $50 on account, which is forfeited if not used for purchases within 30 days.

For criminals with specific needs, the xDedic web interface offers filters like those on UAS. In Figure A2 you can see what xDedic looks like to a customer seeking servers with direct IP access and admin privileges in the state of New York:

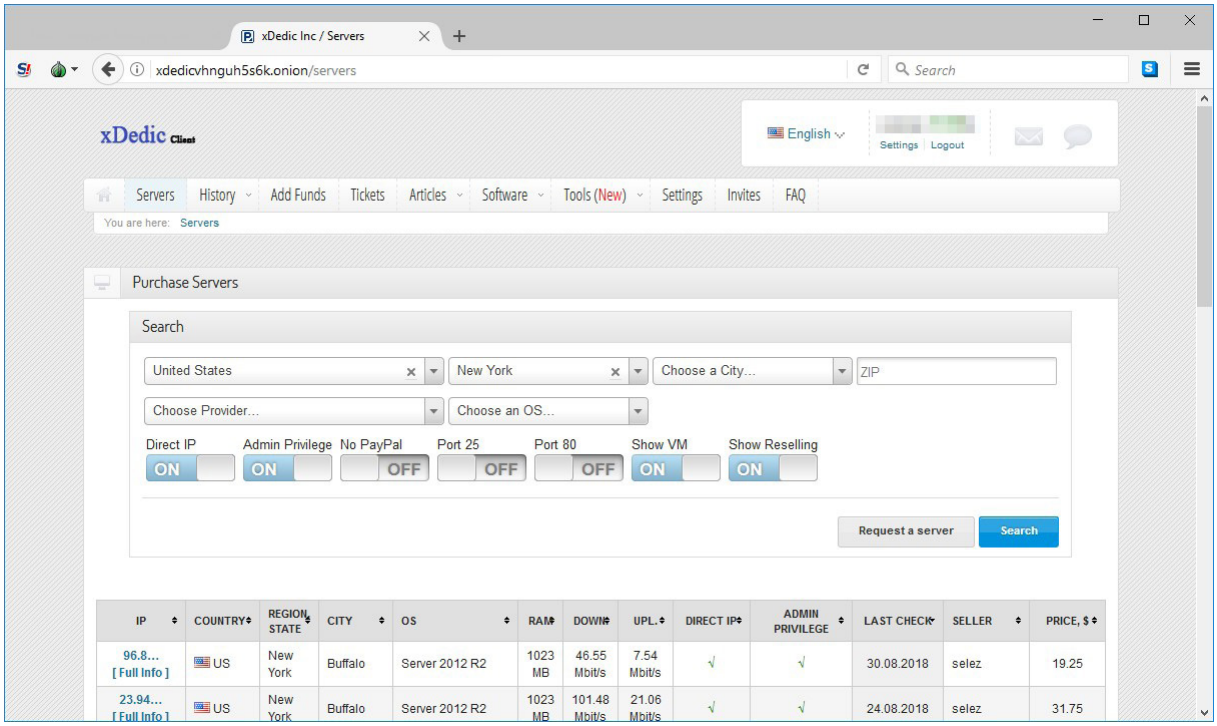


Figure A2.

Any xDedic customer thinking of purchasing access to a particular server can obtain a wide range of details before buying. While the exact IP addresses of targets are not revealed without payment, it is possible to find out where the machine is hosted, its technical specifications, the speed of its internet connection, and whether or not it is a virtual machine. You can also learn what antivirus it may be running and whether or not the IP address has been blacklisted by organizations that fight spam and malware hosting. The information is efficiently presented in a pop-up window, as seen in Figure A3.

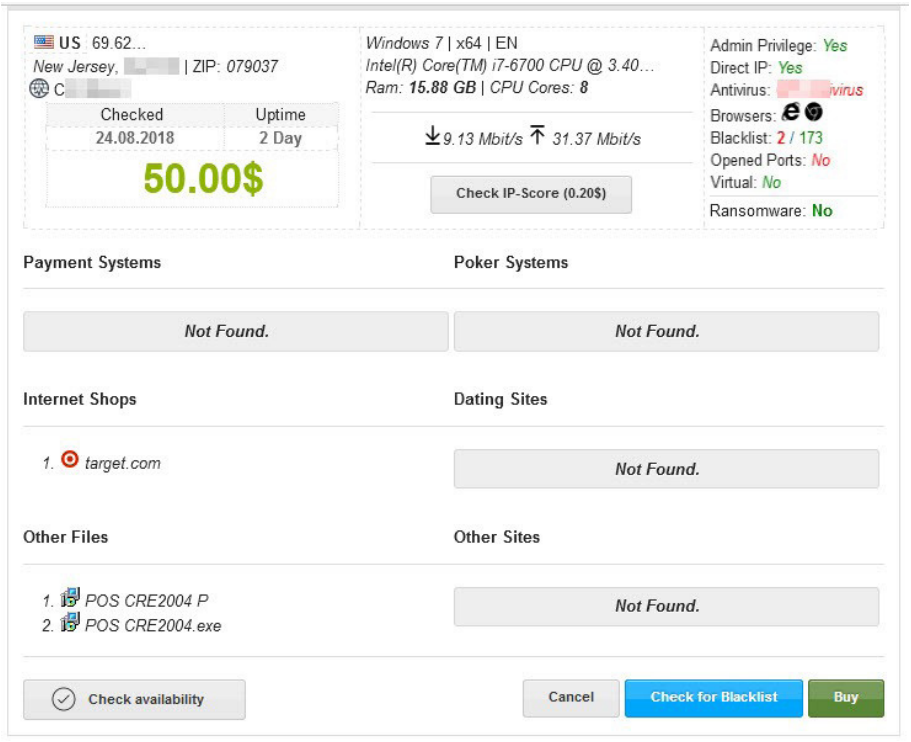


Figure A3.

Note that a point-of-sale software executable has been detected on this server, which might account for the relatively high price. This server could be an attractive target for a criminal looking to steal credit card data, and it is important to note that not everyone who is in the market for a compromised server simply wants to encrypt its contents in a ransomware attack. There are many reasons why criminals like to get their hands on internet-connected servers, and thus many reasons why your organization should have a fully-fledged remote access defense program.

APPENDIX B: SECURING RDP AGAINST RANSOMWARE

A collection of strategies and techniques to consider.

1. Document the problem

Make sure that all of your organization's internet-connected assets are known to the people who have been tasked to secure them. Have a process in place for ensuring that all new devices are included.

2. Limit exposed assets

Make sure that no digital assets are remotely accessible direct from the internet unless they have been approved for use in that manner and configured appropriately. Ask why access to the asset cannot be provided via VPN (Virtual Private Network).

Disable RDP whenever it is not required (these articles show how on different versions of Microsoft Windows: *Server 2016*; *Server 2008/R2*; *Windows 10*; *Windows 8*; *Windows 7*; *Windows XP*).

3. Protect exposed assets

If you absolutely positively have to use RDP without a VPN, be sure that you do as many of the following as you can:

a. Change the default admin password.
b. Enforce password complexity (length, mix of characters, etc.).
c. Set an account lockout threshold to lock remote access after consecutive failed attempts to log in.

By setting your computer to lock an account for a period of time after a number of incorrect guesses, you will obstruct attackers who use automated password guessing tools (a "brute-force" attack). To set an account lockout policy in Windows:

Go to Start-->Programs-->Administrative Tools-->Local Security Policy

Under Account Policies-->Account Lockout Policies, set values for all three options. 3 invalid attempts with 3 minute lockout durations are reasonable choices.

d. Use Network Level Authentication to enhance RD Session Host server security by requiring that the user be authenticated to the RD Session Host server before a session is created.
e. Change the default port for RDP away from port 3389 (but note that this is merely security by obscurity and should not be the only measure you take).

To change the port edit the following registry key (WARNING: do not try this unless you are familiar with the Windows Registry and TCP/IP):
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp.

f. Restrict which public IP addresses can connect via RDP (this can be burdensome if remote users do not have static IP addresses, for example, when traveling or working from home).
g. Use more than one authentication factor. There are three possibilities: things you know, like user name and passwords; things you are, like fingerprint or voiceprint; something you have, like your phone, to which a onetime passcode can be sent.

However, if using codes sent to phones as a second factor, avoid SMS codes because criminals have a history of defeating SMS-based authentication (as described in *this article*). There are good 2FA solutions that leverage the ubiquity of phones but do not communicate via SMS (*such as ESET Authentication*).

h. Tighten up user permissions and rights. Disable files running from the AppData and LocalAppData folders. Block execution from the Temp subdirectory (part of the AppData tree by default). Block executable files running from the working directories of various decompression utilities (for example, WinZip or 7-Zip). Additionally, if you have a good endpoint protection product you can create HIPS rules to allow only certain applications to run on the computer and block all others by default).
i. Password-protect your endpoint protection to prevent unauthenticated settings modification, disabling the protection or even uninstalling the product (but use a different password from the one used for the RDP login credentials).

ABOUT ESET

For 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn *100 Virus Bulletin VB100* awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.

ENJOY SAFER TECHNOLOGY™

SafeBreach

HACKER'S PLAYBOOK

A Ransomware Special Edition

July 2017 | Analysis of findings by SafeBreach Labs

SafeBreach Labs

ABOUT THE HACKER'S PLAYBOOK

First published in Q1 2016, the SafeBreach Hacker's Playbook is the first to report enterprise security trends and risky behaviors from the point-of-view of an "attacker". How do we actually simulate a hacker?

We deploy simulators across endpoints, network and cloud; these simulators play the role of a "virtual hacker" and execute breach methods from our hacker's playbook. This allows us to quantify actual risks and validate whether security controls in the environment are working as expected. The insights from these deployments are incorporated in the Hacker's Playbook report.

We're excited to kick off a "Special Edition" that focuses on a specific type of attack that's in the headlines.

As always, our goal is to give you the perspective of the hacker – a point of view that we find is sorely missing in most security organizations. In order to properly understand your risks, validate your security controls and better prioritize your resources, you must play the role of an attacker. By putting yourselves in the mindset of an attacker, you can better anticipate how well security controls will work against actual attacks, allowing you to quickly take corrective action on the things that matter.

This Special Edition is focused on Ransomware for three reasons:

- **Top of mind concern:** Many security organizations we worked with were worried about ransomware. In fact, it is one of the highest volume "attack searches" on Google, with almost 170,000 searches a month. In April 2016, the FBI issued a warning about ransomware attacks on the rise [1]. In fact, according to the 2017 Verizon Data Breach Investigations Report[2], ransomware has moved from the 22nd most common variety of malware in the 2014 DBIR to the 5th.

- **Booming business:** Over the past five years, ransomware attacks have grown, along with the corresponding ransom. Estimates from the FBI indicated that ransomware is a $1B dollar source of income[3], with the average ransom per machine in the amount of $679 in 2016, more than double the $294 average ransom in 2015[4]. Symantec's recent report indicates that in 2017, this number has risen to $1077[5].

- **Multi-vector attack:** From the perspective of a "virtual hacker", we find ransomware targeted at enterprises to be an extremely interesting attack that challenges almost every single security product deployed—from email security, secure web gateways and next-generation firewalls, to intrusion prevention systems and endpoint security. Ransomware also strongly advocates for a defense-in-depth approach, and the need for controls across the entire cyber kill chain.

OVERVIEW

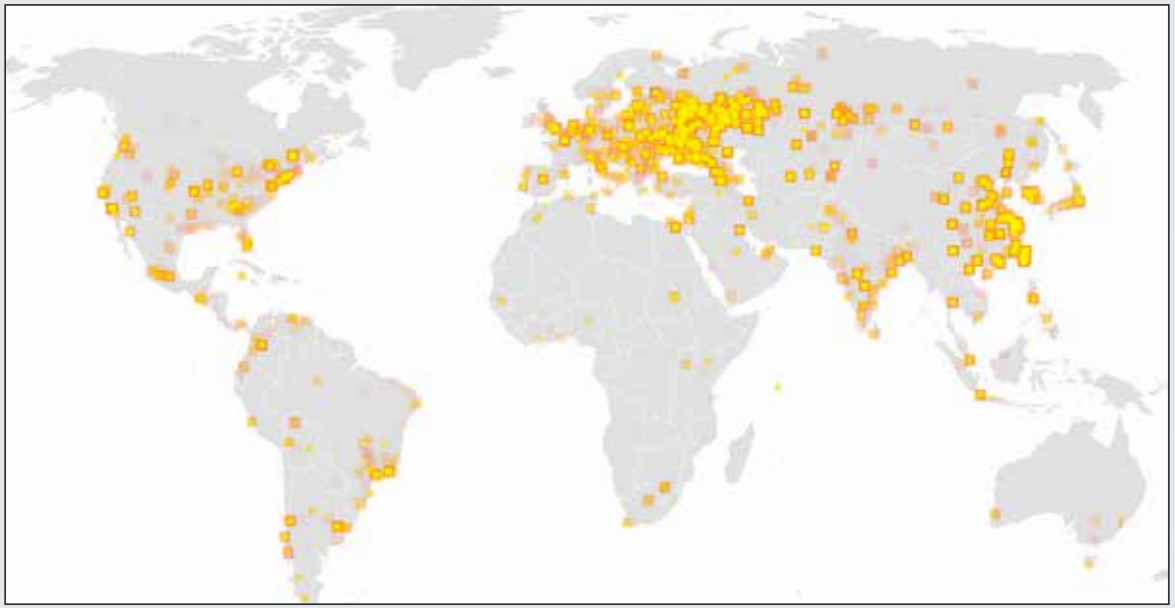
We started working on this document in early Q2 this year, as a "Special Edition" version of our annual Hacker's Playbook. About halfway through our research and analysis for this document, WannaCry hit the headlines.

According to the Federal Bureau of Investigation[7], on average 4000 ransomware attacks occur daily. In May 2017, WannaCry infected 230,000 computers across more than 150 countries in just 48 hours before it was stopped[8]. James Schlesinger's quote rang true for many security organizations, "We have only two modes—complacency and panic," as many scrambled to patch or deal with the aftermath of the attack.

In less than 24 hours, SafeBreach Labs delivered WannaCry breach methods (infiltration of the ransomware, download/save to disk and C2 communications) to our customers to validate that their security controls were working.

One major enterprise spent two days updating and patching 40,000 endpoints, and used SafeBreach to confirm the updates they had made were actually working. WannaCry is incorporated in this report, and (no surprise) is one of the most successful infiltration methods we used followed by older ransomware like CryptoLocker.

WannaCry Infection Map



Source: New York Times WannaCry infection map[9]

Here are some of our key findings from this report:

1

TOP SUCCESSFUL RANSOMWARE DOWNLOADED IS WANNACRY

The WannaCry analysis is included in this report, and as expected, is one of the top successful infiltration breach methods we used.

2

ENCRYPTED TRAFFIC IS A BLIND SPOT

We simulated a variety of infiltration methods, and found the most success with HTTPS traffic.
Most security organizations did not inspect encrypted traffic, leaving them blind to SafeBreach simulated attacks.

3

EMBEDDED EXECUTABLES BYPASSED SECURITY PRODUCTS

Most security products in our customers' deployments would block a traditional executable, but did not stop executables embedded within a variety of file formats.

4

MULTIPLE RANSOMWARE SUCCEEDED WITH C2 COMMUNICATIONS

The majority of security teams aren't inspecting outbound connections, enabling us to successfully simulate C2 communications without being detected or blocked.

5

OLD RANDSOMWARE STILL SUCCESSFUL

Other than the WannaCry, a fairly new attack, the majority of ransomware that we used (for example: CryptoLocker) were several years old; yet we were still successful. In some cases, the right security practices weren't in place; in other cases, it was a misconfigured security product.

THE WHAT AND WHY OF RANSOMWARE

Ransomware is a type of malware that prevents user access to their system or data by encrypting the data or files on the device. Decryption keys are provided once the ransom has been paid.

Ransomware has become a financially rewarding weapon for cyber attackers. Ransom prices depend on the data and the victim. As described earlier, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. This is a 300-percent increase over the approximately 1,000 attacks per day seen in 2015[10].

From a monetary angle, ransomware victims shelled out $24 million in all of 2015 but by 2016, in the first three months alone, victims had paid out $209 million. According to the FBI[3], $1B in ransomware payments were paid in 2016.

It's no surprise then why ransomware attacks have increased in the last three years – there is better reward/risk ratio, there is an untraceable payment method and there are multiple ways to infect very large numbers of victims.

Three reasons ransomware attacks have increased:

Untraceable payments

The lack of an untraceable payment method has been one of the biggest barriers with ransomware. With the emergence of Bitcoin, cybercriminals now have a hard-to-trace method for victims to pay them. Bitcoin wallets can be easily generated for each infection, making it easy for attackers but complicated for law enforcement to follow the money trail.

Better reward/risk ratio

The criminal Willie Sutton was once asked why he robbed banks, and his response was simple -- "Because that's where the money is". The recent 2017 Verizon Data Breach Report[1] states that ransomware is the reigning champion in Crimeware, and the number of attacks will increase each year. As a cyber criminal, ransomware is a great way to make a living because it represents low risks and high rewards. An attacker just needs to encrypt a user's data instead of moving laterally into the network and looking for sensitive data. Even though the FBI continues to advocate that organizations should not pay a ransom to recover their data, there are many high-profile organizations such as the Hollywood Presbyterian Medical Center[11] that have done so, and will continue to do so if attacked.

Widespread infection

There are myriad ways to infect very large sets of users very quickly via mass phishing campaigns. Additionally, ransomware as-a-service programs are available for novice cybercriminals where the author of the ransomware takes a cut of the profits while his/her affiliates focus on infection.

HACKING ACME CORP

A VIRTUAL HACKER PERSPECTIVE

If you've read our Q4 Hacker's Playbook report[12], you know that we've been successful at breaching environments protected by some of the most comprehensive security controls. We were successful using old exploit kits and executables to infiltrate the network, we took advantage of misconfigured malware sandboxing products,and bypassed security segments. We also continue to hold a 100% success rate in data exfiltration in all of our deployments.

Knowing all this, how would we design a ransomware attack?

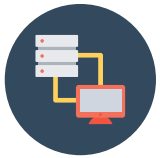
We would use many of the successes outlined above. Ransomware infiltrates and propagates in the same ways as any other malware. The primary difference is that the last step for ransomware is encryption rather than data exfiltration. You can see that each of these different phases challenges different security products.

Infiltration

There are multiple ways ransomware can infect an organization. Certain techniques such as malicious emails and exploit kits tend to be more successful compared to others. In our case, we would take advantage of social engineering to get Bob at Acme Corp to click on a link and download a file containing ransomware. Alternately we could use the techniques involved in WannaCry, wherein we would instead cleverly package our dropper into an otherwise innocuous file, like an AOL IM installer, or a malicious PDF.

Ransomware written to disk

Bob at AcmeCorp saves the attachment on his computer. An endpoint security or malware sandboxing product should have detected that the attachment contained an executable file and warned Bob, and prevented this action from taking place. If the attachment seemed innocuous, but an executable called out for further payloads, network scanning tools should see that malicious traffic, either outbound or inbound, and block the communication and subsequent payload.



Ransomware talks to command and control

In some cases, before the ransomware can start attacking, it will contact the command and control server operated by the attacker. The ransomware client and server identify each other, and share cryptographic keys. This allows the attacker to store one key on Bob's computer, and the other key on their server for decryption once the ransom is paid. This C2 communication should be inspected by a firewall looking at outbound connections. Most of the time, this may not stop the ransomware attack, but it would at least initiate the beginning of an investigation and prevent further infections As an attacker, our communication would be via SSL as the majority of organizations don't decrypt and inspect SSL traffic. In certain ransomware cases, this C2 communication does not occur. For example, Cerber is a ransomware which can encrypt files in offline mode, it doesn't need to fetch the keys from the C2 server.

Ransomware executes and encrypts files

The final step for the ransomware is searching for files on Bob's computer, and encrypting them. Once the files are encrypted, the victims are shown a lock screen demanding ransom.

RANSOMWARE INSIGHTS FROM SAFEBREACH DEPLOYMENTS

Now that we've outlined the steps we'd take for the "perfect ransomware crime," how does this idealized version compare with what actually works in actual SafeBreach customer environments? Specifically, we wanted to gain more insights on our successes as a virtual hacker and which methods were most effective. We wanted to be able to answer the following:

- The top techniques to get ransomware on an organization's computer?
- Top ransomware that was successful infiltrating an organization?
- How we were able to install ransomware on disks?
- What were the top ransomware we were able to install on disks?
- What were the top ransomware we used that performed C2 communications?

INFILTRATION FINDINGS:

Encrypted Traffic A Blind Spot

We simulated a variety of infiltration methods, and found the most success with HTTPS traffic. When it comes to success rate overall: HTTPS wins over HTTP, 443 wins over 80 and 8080. This isn't a surprise. A significant amount of traffic is already encrypted on corporate networks, and because most security organizations don't decrypt traffic, it is easy for an attacker to slip past any security solution undetected. Encrypted traffic is a blind spot for most security teams.

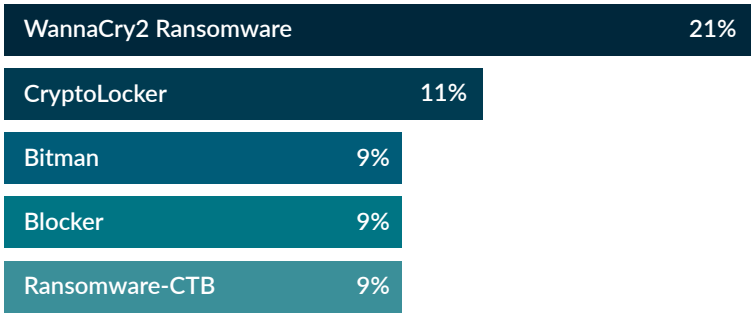
Top Infiltration Techniques Via Executable Files

With ransomware simulations, the top infiltration techniques were via executable files delivered over HTTP/S. We drilled a little deeper into the data to see which three methods were most successful; here are the top 5:

- EXE inside a VBS - Visual Basic is a scripting language that MSFT supports. SafeBreach was successful in breaching an environment using both an executable file hidden in VBScript, and by packing the executable within the scripts we were able to bypass deep packet inspection.
- EXE inside a DOC with macro - Microsoft Office™ for many years contained macros that allow you to program custom events. Over the years, attackers have abused macros to create malware. In fact, in June 2016, the US Cert issued a warning about the resurgence of using macros but it appears most organizations are still struggling with the balance between business continuity and security.
- EXE inside encrypted zip - In this example, SafeBreach used encrypted ZIP file/archive over HTTP. One of the oldest tricks by attackers, encrypted zip files over HTTP should be limited by policy or inspected by next-generation firewalls.
- EXE inside JAR - "JAR" is a package file that aggregates many Java class files and associated metadata and resources (text, images, etc). In this example, SafeBreach embedded an executable file within JAR for exploitation and malware delivery.
- EXE dropper inside a PPT with macro - A dropper is a program that has been designed to "install" some sort of malware (virus, backdoor, etc.) to a target system. In this case, we embedded the dropper within a powerpoint with macro.

WannaCry Tops Successful Ransomware Installed

The top 5 ransomware malware samples we used, based on success quantity were:

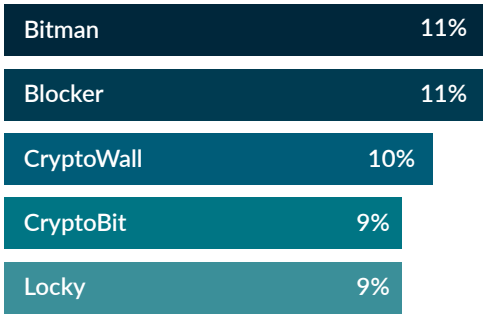


WannaCry2 clearly needs no introduction, and was one of the more successful ransomware utilized by SafeBreach. Others included CryptoLocker, ransomware from 2013 and 2014 targeting Microsoft Windows; Bitman or TeslaCrypt, a ransomware from 2015 targeting gaming files. Blocker and Ransomware-CTB round up the top 5.

RANSOMWARE WRITTEN TO DISK:

Top Five Successful Ransomware Dropped To Disk

Bitman, Blocker and Cryptowall topped the list of successful ransomware we were able to write to disk in our simulations.

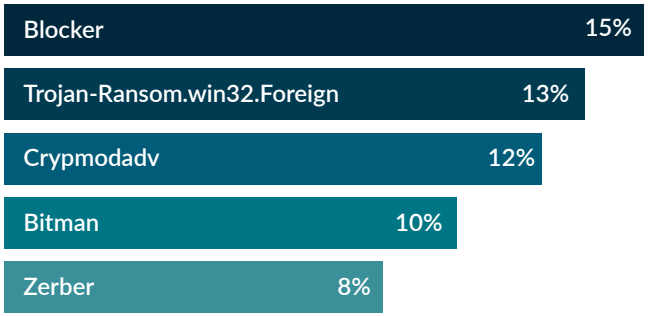


When we simulated ransomware written to the disk, typically the second phase of a ransomware attack, many different types of ransomware were successful. Similar to the results from successful ransomware installed, the biggest surprise to us was the success of ransomware that had been around for many years. In these customer deployments, endpoint security products that should have stopped SafeBreach from dropping ransomware to disk did not do so. In some cases, we found products that were misconfigured or simply didn't work.

RANSOMWARE C2 COMMUNICATIONS:

Blocker Tops Successful Ransomware Executing C2 Communications

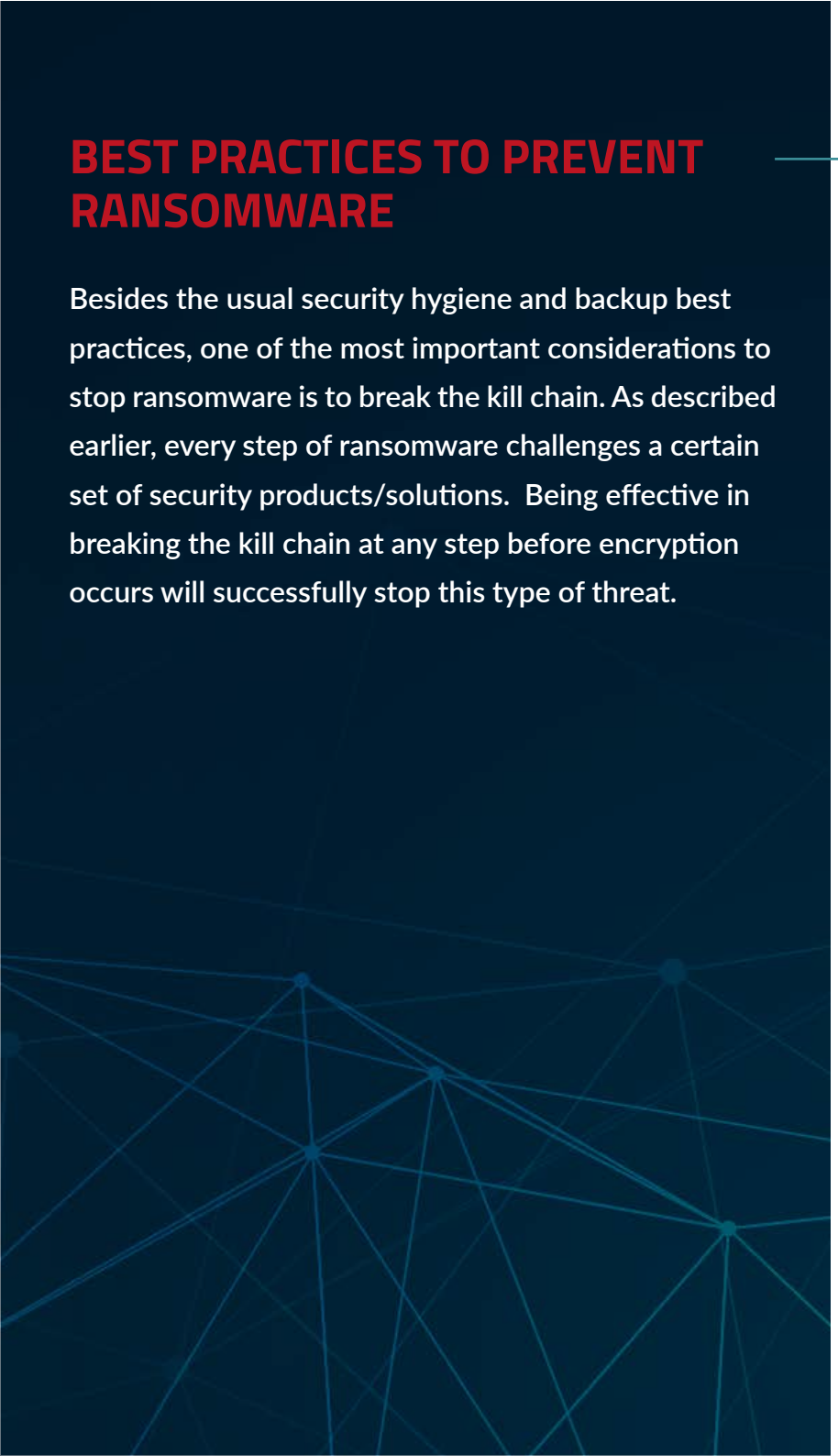
We simulated C2 communications from various ransomware, and the following were the top five:



C2 communications does not always occur with all ransomware, but when it does, it's an opportunity to detect an attack in progress and stop more endpoints from being infected. SafeBreach simulated C2 communications to challenge security products that should have inspected this traffic. The top 3 in success quantity were Blocker, Foreign and Crypmodadv.

BEST PRACTICES TO PREVENT RANSOMWARE

Besides the usual security hygiene and backup best practices, one of the most important considerations to stop ransomware is to break the kill chain. As described earlier, every step of ransomware challenges a certain set of security products/solutions. Being effective in breaking the kill chain at any step before encryption occurs will successfully stop this type of threat.



Eliminate Blind Spots

Ransomware payloads aren't any different from other types of malware. Security teams need to control what's coming into the organization and eliminate their blind spots. This means:

- Blocking exploit kits that point users to either visit a site that contains malicious exploit code, or to download a seemingly legitimate file with hidden malicious code
- Inspecting encrypted traffic (HTTPS/SSL) that hides user actions
- Blocking macros or hidden executable file formats that may not be inspected by email security or endpoint security malware sandboxing solutions

Control What's Being Saved

With the right endpoint security solution, you can blacklist known signatures or hash of files for ransomware, or prevent potentially malicious files being saved to the disk. Ensure that endpoint security solutions deployed are scanning all folders including temporary folders.

Inspect C2 Communications

Some ransomware families need to call home to establish the encryption keys. Inspect the command and control communications using a next-generation firewall, proxy, or IPS. Blocking the C2 communications may not stop a ransomware, but you'll be able to alert and begin investigation to prevent more computers from being infected.

Don't Wait - Simulate!

Utilizing breach and attack simulation technology allows security teams to validate whether the security controls they have deployed to stop ransomware are working. Breach and attack simulations allow you to also visualize the entire kill chain so you can observe where to focus security efforts. Most importantly it validates all security controls before attackers do the testing instead.

Back Up That Data

Backups are critical in ransomware incidents; if you are infected, backups are often the best way to recover your critical data. It is important to not only regularly back up data but also verify the integrity of those backups to ensure the right data is maintained, and that malicious payloads are not accidentally propagated. Periodically running a data restoration drill would also be a good idea.

SafeBreach

FOOTNOTES

[1]https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise
[2] Verizon Data Breach Investigation Report, 2017
[3]http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
[4]http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf
[5]https://www.symantec.com/security-center/threat-report
[6]Trend Micro 2016 Security Roundup https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup
[7]https://www.justice.gov/criminal-ccips/file/872771/download
[8]http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/
[9]https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html
[10]https://www.fedscoop.com/ransomware-attacks-up-300-percent-in-first-quarter-of-2016/
[11]http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
[12]https://go.safebreach.com/Website-Content-Report-Hackers-Playbook-Second-Edition-LP.html

SafeBreach 111 W Evelyn Avenue Suite 117 | Sunnyvale, CA 94086 | contact@safebreach.com

Ransomware Prevention and Mitigation Techniques

Article *in* International Journal of Computer Applications · February 2020

DOI: 10.5120/ijca2020919899

3 authors:

Hesham Alshaikh
Faculty of Graduate Studies for Statistical Research (FGSSR)
3 PUBLICATIONS **12** CITATIONS
SEE PROFILE

Nagy Ramadan
Cairo University
103 PUBLICATIONS **377** CITATIONS
SEE PROFILE

Hesham A. Hefny
Faculty of Graduate Studies for Statistical Research (FGSSR)
308 PUBLICATIONS **2,455** CITATIONS
SEE PROFILE

Ransomware Prevention and Mitigation Techniques

Hesham Alshaikh
Sadat Academy for Management Sciences, Egypt

Nagy Ramadan
Department of Information Systems and Technology
Faculty of Graduate Studies for Statistical Research, Cairo University, Egypt

Hesham Ahmed Hefny
Department of Computer Science
Faculty of Graduate Studies for Statistical Research, Cairo University, Egypt

ABSTRACT
Ransomware is a malware family that using security techniques such as cryptography to hijacking user files and associated resources and requests cryptocurrency in exchange for the locked data. There is no limit to who can be targeted by ransomware since it can be transmitted over the internet. Like traditional malware, ransomware may enter the system utilizing "social engineering, malware advertising, spam emails, take advantage of vulnerabilities, drive-by downloads or through open ports or by utilizing back doors". But in contrast to traditional malware, even after removal, ransomware influence is irreparable and tough to alleviate its impact without its creator assistance. This kind of attack has a straightforward financial implication, which is fueled by encryption technology, cyber currency. Therefore, ransomware has turned into a profitable business that has obtained rising popularity between attackers. As stated by "Cybersecurity Ventures", ransomware is the quickest increasing type of cybercrime. Since, global ransomware wastage expense is predicted to hit $20 billion in 2021, up from just $325 million in 2015 which, is 57X extra in 2021. In this paper, a brief of the recent research in the prevention of ransomware attacks and the best practices to mitigate the attack impact is presented.

General Terms
Ransomware prevention technique, ransomware mitigation technique, signature-based, behavior-based.

Keywords
Ransomware, Cryptography, Cryptocurrency, Cybercrime, Malware, Cybersecurity, Vulnerability, Cyberattacks.

1. INTRODUCTION
Cybercriminal attackers understand that data, files, networks and all digital resources are the key factors for the growth of regular working and any business [1]. These digital assets are so precious to the business therefore, the quickest and preferable way to earn great money is to keep all these resources at ransom. Thus, rise ransomware which, a malware that commonly encrypts all files and requests for a payment in bitcoin to give the victim the decryption key [2].

As stated by the "Cisco/Cybersecurity Ventures 2019 Cybersecurity Almanac" cybercriminal activity considered one of the major challenges that mankind will confront in the following two decades. Cyberattacks are the quickest increasing crime globally, and they are growing, in size, sophistication, and expenses.

Also, they predict that cybercrime losses will cost the world $6 trillion annually by 2021 and more than 70% of all cryptocurrency bargains yearly will be for illegitimate activity.

Advances in technology are the main driver for economic growth but, have also led to a higher incidence of cyberattacks. The 10 major data breaches in the last two decades combined with the number of hacked accounts and year occurred. As claimed by Quartz, Yahoo, three billion (2013); Marriott, half billion (2014-2018); Adult FriendFinder, 412 million (2016); MySpace, 360 million (2016); Under Armor, 150 million (2018); Equifax, 145.5 million (2017); eBay, 145 million (2014); Target, 110 million (2013); Heartland Payment Systems, 100+ million (2018); LinkedIn, 100 million (2012).

Moreover, other research from "Cybersecurity Ventures" that approximate there are 111 billion code lines of new software being generated yearly, which brings in the possibility for an enormous number of vulnerabilities that can be exploited. Utilizing zero-day attack alone is forecasted to be once a day by 2021, up from once a week in 2015 [3]. This attack technique makes the prevention task very difficult, even for giant firms with a generous cybersecurity fund [4].

The 5 most cyber attacked industries over the previous 5 years are transportation, healthcare, financial services, manufacturing, government. "Cybersecurity Ventures" forecast that media and entertainment, retail, petrol and natural gas, teaching (kindergarten to 12 grade and higher education) and legal will be among the top 10 industries for 2019 to 2022.

Hacking tools and equipment for identity theft, cyberattacks, malware, ransomware, and other nefarious intent have been obtainable in the online market for many years at a low price as $1 which, makes it nearly free to enter the life of cybercrime.

Cybersecurity worldwide market value was $3.5 billion in 2004 while, its value was more than $120 billion in 2017. The cybersecurity marketplace rises by about 35X during that period. The 2019 U.S. president's financial plan includes $15 billion for cybersecurity, the Department of Defense (DoD) was the greatest subscriber with $8.5 billion in cybersecurity financing in 2019 [3].

Ransomware is a malware family that using security techniques such as cryptography to hijacking user files and associated resources, then requests cryptocurrency in exchange for the locked data [5]. Some ransomware gets into the system utilizing social engineering, malicious advertisements, spamming, drive-by downloads, while others try to discover vulnerabilities to exploit it, using open ports or exploiting a backdoor to get inside [1]. Consequently, vulnerability testing and security loopholes must be identified, and people must be aware of these kinds of exploiting

mechanisms [6].

Ransomware as a service (RaaS) is a service that grants easy attainment of ransomware codes without any special programming skills at a monetary value. The price could be an explicit buy, or a profit margin scheme could be employed. This shows that collaboration exists between criminals [7]. One side oversees originating a custom binary ransomware code, while the other side simply downloads the customized binary ransomware and organize the dissemination of the contagion or the attack campaign usually through botnet email, and both parties enjoy the profit from a successful attack [8].

Therefore, ransomware has become a profitable profession that has gained boosting popularity between attackers [5]. The publicity of ransomware has originated an extraordinary ecosystem of cybercriminals. The ransomware attack has a direct financial implication, which is fueled by encryption technology, cyber currency. Encryption is effective and almost unbreakable. Anonymous cyber currency can obviate traceability. Easily attainable ransomware code permits easy entry to the cybercrime world. A combination of these provides an attractive avenue for cybercriminals, producing specialist cybercriminals [7,9].

The U.S. Department of Justice (DOJ) has depicted ransomware as a new profession model for cybercrime, and a universal phenomenon. Global ransomware devastation price is forecasted to hit $20 billion in 2021, up from just $325 million in 2015, as stated by "Cybersecurity Ventures". So, it is 57X extra in 2021. That turns out ransomware into the fastest increasing type of cybercrime. "Cybersecurity Ventures" anticipates that businesses shall fall prey for ransomware onslaught every 11 seconds by 2021, up from every 40 seconds in 2016. Hence, global spending on security awareness training for employees one of the quickest increasing categories in the cybersecurity industry is predicted to reach $10 billion by 2027, up from about $1 billion in 2014 since, training operator on how to reveal and behave with ransomware is a critical obstacle [3].

Ransomware is the biggest threat to businesses, and it is the main reason for enormous damages such as *first:* business deadlock and massive casualties to the economy [1]. In May 2019, the town of Baltimore uncovers that it was a martyr of a ransomware attack, in which crucial files are encrypted remotely till a ransom is settled. The town instantly puts systems offline to hinder the ransomware from propagating, but unfortunately, it was after taking down the parking mulcts database, email, voice mail and the water invoices system, property taxes and vehicle citations [10].

Second: breakdown production of Renault and Nissan motor manufacturing UK, after the ransomware infected some of their systems. Spain's Telefónica, FedEx and Deutsche Bahn were hit with WannaCry ransomware infection as well in 2017.

Third: life-threatening damages. National Health Service hospitals in England and Scotland, and up to 70,000 devices, including computers, MRI digital scanners, Operation room gears, and blood storage fridges have been infected with WannaCry [11].

In this survey, a comprehensive review of ransomware recovery, mitigation, and prevention techniques are performed to facilitate future research, study, and analysis. Furthermore, understanding of ransomware and assist researchers and developers in their efforts to find adequate solutions. The obtained results hopefully may be used to form a base for designing and developing more effective defense solutions against ransomware attacks.

This survey is organized into five sections, *the first one* being the present introduction in which, the relevant background information on cybercrime in general and particularly on ransomware is presented to provide an insight into how the ransomware attack is achieved. Then, *section 2* shows an updated review of research in the area of ransomware and the employed techniques for detection, mitigation, and prevention of ransomware attack. *Section 3* discusses the present research directions in ransomware and summarizes its pros and cons. The concluding remarks are presented in *section 4*. Finally, *section 5* discusses potentially future directions. *Table (1), (2)* shows a summary of related work.

2. RELATED WORK

There are a lot of research efforts have been done to prevent the ransomware attacks employing different approaches to identify the presence of ransomware such as:

2.1 Signature-based Approach:

The signature approach focuses on, detecting ransomware unique patterns such as a distinctive sequence of bytes in the ransomware source code, the order of call functions and the content of the ransom demand message. Such sequences are saved in a database and during the scanning, the anti-malware software tries to detect such patterns in executable files.

Signature-based malware detection techniques have conventionally been hugely preferable because they have a low false positive ratio. So that an alarm is triggered if a certain well-known pattern is observed. However, Goyal et al. [12] Emphasize that the signature-based approach is unable to cope with the obfuscated code in ransomware and cannot detect new strains until they have been analyzed by analyst [13].

2.2 Behavior-based Approach:

In this approach, the researchers create an artificial, realistic execution environment and monitors how ransomware interacts with it. Behavior-based detection is the notion of observing the characteristics of how the malware operates. Hence, it relies on study typical ransomware behavior like file access, file system activity, and network activity.

2.2.1 File Access and File System Activity:

Grant and Parkinson [13] investigated the behavioral characteristics of ransomware focusing on interplay with the underlying file system. They implemented a file monitoring application to monitor all interactions with files in a delimited directory due to the utilization of windows core functionality. This study identifies that each ransomware instance has a unique behavioral pattern regarding file system activity which is, remarkably dissimilar to those of normal user interactions. Furthermore, it shows that ransomware may be identified using individual or shared patterns.

Furthermore, Kok et al. [14] proposed a pre-encryption algorithm that composed of two phases the first, is a machine learning algorithm used to detect the ransomware before encrypting user files, which based on API pattern recognition. Hence, it uses Cuckoo sandbox to captures the (API) generated by the suspicious program and analyzes them, but it may have a high false positive rate. The second phase is a signature repository used to store the generated signatures of suspicious programs that, used to detect the crypto ransomware in the pre-execution stage using signature

matching however it, can only detect known crypto ransomware. Therefore, each of the two phases complements each other and provides an efficient method to protect users from crypto ransomware.

Whereas Scaife et al. [15] presented an early warning awareness system called CryptoDrop, which generate a notification at the time of suspicious file activity and allow users to make the final decision on whether the activity is desired or not. Using a set of behavior denotations CryptoDrop can eliminate any process that seems to be manipulating an enormous amount of user data. The authors allege this system prevent ransomware from executing with a median loss of only 10 files and does not inspect files outside of the user documents directory. Though, Wolf [16] underdetermined the CryptoDrop efficiency, claiming that 40 files on average could be properly encrypted before it can detect suspicious activity.

While, Continella et al. [17] proposed a technique called ShieldFS that copying files when it altered, saving the copy in a preserved area permitting any alterations to be made to the original file while it keeps track of changes made to it. The detection system established on the integrated analysis of entropy of write operations, frequency of reading, write, and folder itemization operations, fraction of files renamed, and file type usage statistics. Subsequent if ShieldFS determines that the process is normal, the saved file can be discarded from the kept area since the original file has not been encrypted by ransomware. However, if ShieldFS decided that a process is harmful, the aggressive process will be suspended, and the saved copies can be brought back, substituting the altered (encrypted) versions.

Likewise, Kharraz and Kirda [18] proposed a similar approach to ShieldFS called Redemption where file operations are being redirected to a dummy copy. This technique initiates a copy from each file subject to be modified by the ransomware, and then redirects the file system processes (demanded by the ransomware to encrypt the target files) to the copies, hence leaving the original files undamaged. Redemption uses the Windows kernel development framework to reflect the write requests from the target files to the preserved files in a transparent data buffer. However, rewrite and create operations can experience slowdowns ranging from 7% to 9% when dealing with many small files. Creating the reflected files and redirecting the write demands to the restricted area are the main reasons for this performance hit under high workloads.

Different perspectives adopted by, Winter et al. [19] they emphasize that technology is not improving as fast as the complexity of threats. They have started a cyber-autoimmune disease where an antivirus system is responsible for destroying the computer's operating system after they infected system files with malicious code. To draw interest to flaws in protection systems which, allow attackers to reach their targets more easily causing serious damage.

However, Lika et al. [20] concluded that no actual solution could be used to decrypt the hard disks that have been encrypted by NotPetya, ransomware. While crucial answers are lacking, the vaccine has been found where, the existence of a local file, prevents the NotPetya execution. Hence, the authors intended to educate users to increase their awareness reactively through gamification.

2.2.2 Network behavior:

Some of the research works were interested in finding the network behavior of ransomware. Zimba et al. [21] studied the emerging cyber threat to crucial infrastructure and magnify the network segmentation approach, prioritize the security of production network devices and limiting ransomware propagation. By applying reverse engineering on WannaCry ransomware and perform source code analysis they uncover the employed techniques to discover vulnerable nodes.

Thus, Zimba and Mulenga [22] employed reverse engineering on the underlying malware program logic. Using the dynamic analysis to captivate the corresponding network actions associated with such logic to unmask WannaCry ransomware network interactions. The source code analysis shows that the ransomware fetches the network adapter properties to determine whether it's residing in a private or public subnet to effectuate substantial network propagation and subsequent damage. Nonetheless, the employed network techniques are specified to WannaCry ransomware only.

Furthermore, Almashhadani et al. [23] established a thorough behavioral analysis of crypto ransomware network interactions, taking Locky, one of the extremely dangerous ransomware families. A devoted testbed was constructed, and a set of worthy and informational network characteristics were educed and categorized into multiple types. A network-based invasion discernment system was implemented, utilizing two separate classifiers working side by side on packet and flow levels. The authors assume that most ransomware families try to get in touch with command and control servers before harmful payloads are achieved which, is not the case in all ransomware families. Also, monitoring outbound connections can be simply eschewed by connection encryption.

Moreover, Akbanov et al. [24] accomplished extensive dynamic analysis on WannaCry ransomware and they found out that its mechanism based on two different components. The first enables WannaCry to disseminate through network devices like a worm by generating a list of local and global IP addresses and scanning both internal and external networks for Microsoft's MS17-010 vulnerability by sending packets via port 445 to infect unpatched systems. The second is the encryption process since it has embedded RSA keys used for decrypting the required malicious DLL representing the encryption component. Also, they have revealed that WannaCry communicates with command and control server through embedded. onion addresses via a secure channel on port 443 and the common Tor ports 900, 9050 to download the "Tor-browser" installation software. The outcome of this research may help to accomplish an efficient mitigation mechanism against WannaCry and any ransomware family that has the same behavior.

2.3 Contemporary Prevention Methods

2.3.1 Categorizing Ransomware Characteristics:

To facilitate the ransomware detection operations. Rajput [6] studied the different types of ransomware families as he focused on their evolution and characteristics. The result of this analysis shows that many ransomware families exhibit similar characteristics.

Therefore, the main contribution of Hull et al. [25] is a predictive model for categorizing ransomware behavioral characteristics, which can then be used to ameliorate uncovering and dealing with ransomware incidents. The categorization was done with respect to the deployment stages

of ransomware, by establishing a predictive model called "Randep". The stages are fingerprinting, propagate, communicate, map, encrypt, lock, delete and intimidation. This model concluded from a study of 18 ransomware families. By observing windows Application Programming Interface (API) function calls throughout each ransomware execution, to comprehend what actions a ransomware strain might do. Nevertheless, not all ransomware families go through all these deployment stages.

Moreover, Chen and Bridges [26] established an automated method to extract distinguishing features of malware from host logs, which contain many non-malicious events. They have utilized behavior logs from analysis reports created by Cuckoo sandbox under several situations of ordinary and malware interactions.

likewise, Verma et al. [27] focused on the indicators of compromises (IOCs) for ransomware using Cuckoo sandbox. Which will be used to set the base for analyzing and classifying new ransomware based on their behavior. Using supervised machine learning classifiers to classify the ransomware samples to their respective 7 families that they have worked on.

While Popli and Girdhar [1] ran the ransomware in a simulated environment using Cuckoo to analyze their attack process, then predict future ransomware, its expected impact and how it will be difficult to be detected if polymorphic, metamorphic and other obfuscation techniques used by ransomware. Even though these methods reveal how ransomware interacts with the environment, but it can't be used to reveal ransomware infection immediately.

2.3.2 Access Control:

Another prevention technique is to adopt an authentication-based access control mechanism under the name of "AntiBotics" presented by Ami et al. [28]. "AntiBotics" has three components. *The first component* is the Policy Enforcement Driver which acts as an initial gate that records and halts any file modification attempts such as, renames or deletions. To modify a file, a challenge is created such as CAPTCHA or biometric authentication to authenticate the user actions. *The next component* is the Policy Specification Interface, which is a GUI program that allows administrators to configure the system policies. *The last component* is the Challenge-Response Generator wich, controls the generated challenges, i.e. the time-out rate, and mechanisms to prevent large generations of challenges. Since humans, are always the fragile bond in any defense system. Users may grant access to a process which, is infected with malignant code.

Also, Christopher and Kumar [29] Presented a preventative technique based on ransomware behavior, targeting three Indicators of Compromise (IOC), file changes within a time interval, file entropy and manipulation of canary files. The File system watcher filter used to monitor two artificial network drives and disabling methods used to alter Access Control Levels (ACL) of files and folders to revoke the writing privileges when compromise confirmed. Nevertheless, the system will suffer from a lot of strain when the monitoring is done on physical drives instead of artificial drives.

2.3.3 Recovery After Infection:

This is a different technique aims to recovering from the ransomware attack without ransom paying to accomplish this, Zimba and Chishimba [9] suggested to follow mitigation strategies and recommend best practices based on clarifying core components of successful ransomware attack campaigns. Such as securing email since emails are a major source of ransomware and apply security patches regularly to fix vulnerabilities and avoid ransomware. Results show that lack of offline backup and poorly implemented offline backup strategies end up costing businesses more than the ransom demand itself. Nonetheless, systems may still vulnerable to zero-day attacks.

Likewise, Lee et al. [30] provided a new technique to recover from a ransomware attack using the key backup. They assumed that the ransomware uses windows operating system CNG cryptography library to encrypt user files. Therefore, they seek to pick up the keys when ransomware generating it inside the host or receiving it from the server. Hence, using it for file recovery after ransomware infects the system and encrypt the files. Despite this, some ransomware uses libraries other than CNG such as Cryptolocker which uses the CAPI cryptography library and others implement their own cryptography library. Furthermore, a few ransomwares don't obtain a key from the server, such as Ordinypt and Petya instead, they encrypt files with randomly generated keys which lead to data loss. Moreover, monitoring the outbound communication can be simply bypassed by encrypting these connections.

Whereas, Zimba et al. [31] used a ransomware categorization framework to classify the ransomware attack maliciousness based on data deletion and file encryption attack structures. The categories classify the technical skill and the overall effectiveness of potential ways of retaining the data without paying the ransom demand. This framework helps to understand potential inadequacies and glitches to be utilized for data retrieval via system volume shadow copies or third-party software.

Furthermore, Zimba et al. [32] employed reverse engineering and dynamic analysis to assess the underlying attack structures and data deletion techniques that ransomware use. And have concluded that no matter how destructive a crypto ransomware attack might seem, the key to data recapture options lies in the underlying attack design and the implemented data deletion methodology. Though other ransomware has an irreversible impact, for example, no actual solution could be used to decrypt the hard disks that have been encrypted by NotPetya.

2.3.4 Trapping Attacker:

lately, some authors have developed further prevention methods. Gómez-Hernández et al. [33] proposed a general methodology called R-Locker to thwart crypto ransomware actions. It is based on the deployment of a honey file design of the Linux system to block the ransomware when it accesses a canary file, thus allowing it to maintain the rest of the data. In addition to that, this approach can automatically launch steps to solve the infection. Nevertheless, this solution has some limitations such as, that just a part of the complete file system (that corresponding to the user that installs R-Locker) is protected, also the poor distribution of the traps can reduce the efficiency of the actual protection of the data. At the same time, this defense can be passed over by the removal of the central trap file. Moreover, it can be partially bypassed by accessing given folder files by ransomware in a random way where all files in the folder may be encrypted before the sample can be blocked.

Whereas, Wang et al. [34] utilized an advanced defense schemes to protect important hosts under targeted ransomware attacks. By employing the cyber deception technology to blocking attackers via a network deception environment to

help protect crucial systems through attack guidance, by drawing attackers off from these preserved systems. As a result, they deliberately set the administrator privileges of the deception environment as weak passwords and leave common vulnerabilities in the environment, such as EternalBlue, to attract attackers. Furthermore, they have developed an automatic analysis system by taking preference crypto ransomware natural language processing and machine learning techniques to trace-back (RDP) Remote Desktop Protocol-based ransomware attacks and identify the original attack sources. Accordingly, this approach is just for hindering RDP-based ransomware attacks only.

Furthermore, Shaukat and Ribeiro [35] works is based on analyzing an extensive dataset of ransomware families presents RansomWall, a layered safeguard system for protection versus cryptographic ransomware. It follows a hybrid approach of combined static and dynamic analysis to generate a compact set of features that characterizes the ransomware behavior. It uses trap layer to help in early detection and supervised machine learning algorithms for unearthing zero-day intrusions. When preliminary layers of RansomWall tag a process for suspicious ransomware behavior, files altered by this process are copied into a protected place for preserving user data until it is classified as "ransomware or benign" by the machine learning layer. Nevertheless, user critical files may be attacked earlier than honey files.

3. DISCUSSION

It is significant to note that the research community has put attention in detection, prevention, and even recovery techniques to prevent ransomware infections and mitigates its impact to avoid data and large economic loss. The main contribution of this paper is to summarize the presented literature which, employs different mechanisms to protect the business from ransomware attacks, and revealing its strengths, weaknesses. Moreover, realizing the related challenges that confront with this kind of attack. Therefore, this work may be used as a starting point for future research. The pros and cons of the related work are summarized in table (1), (2).

Table (1) (Related Work Summary)

No.	Researcher/s	Contribution	Pros.	Cons.
1	Popli and Girdhar [1], 2018	Ran recent ransomware in a simulated environment and analyze their attack process	Make a prediction of future ransomware, its expected impact and how difficult it would be to detect if polymorphic, metamorphic techniques used.	They didn't suggest a specific solution to prevent or detect ransomware infection.
2	Rajput [6], 2017	Studied the characteristic of ransomware families and its evolution	He shows that many Ransomware families exhibit similar characteristics.	They didn't suggest a specific solution to prevent the ransomware infection.
3	Zimba and Chishimba [9], 2019	Suggested mitigation strategies utilizing the recommend best practices based on successful ransomware attacks campaigns	Availability of offline backup will mitigate the impact of ransomware infection	The system still vulnerable to a zero-day attack which, can break the system.
4	Goyal et al. [12], 2020	Detected crypto ransomware using a classification model	This paper demonstrates the limitation of signature-based detection methods, and emphasize the behavior-based detection mechanism capability to detect crypto ransomware.	Misclassification may happen due to decision boundary errors.
5	Grant and Parkinson [13], 2018	Proposed a file monitoring application	Identify the ransomware behavioral pattern	It just monitors interaction with files only in a "specific directory", not all user data.
6	Kok et al. [14]	Proposed a pre-encryption algorithm	The proposed LA algorithm has accomplished the prediction utilizing only API data to detect crypto ransomware.	The LA can only be implemented using a new dataset with API from the pre-encryption stage.
7	Scaife et al. [15], 2016	Proposed "CryptoDrop" an early warning detection system	It can halt a suspicious process.	- Does not inspect files outside of the user documents directory. - Needs user interaction. - 40 files could be encrypted before it can detect suspicious activity.
8	Continella et al. [17], 2016	Proposed "ShieldFS" detection system	No file encrypted by ransomware	Creating the reflected files and redirecting the write requests to the protected area are the main reasons for performance hit under high workloads.
9	Kharraz and Kirda [18], 2017	Proposed "Redemption " detection system		

10	Winter et al. [19], 2018	Started a cyber-autoimmune disease	Emphasize that technology is not evolving as fast as the complexity of threats.	There is no specific solution proposed other than requesting anti-virus companies to update their inefficient methods and techniques.
11	Lika et al. [20], 2018	Proposed cyberattack prevention through awareness via gamification	Educate users to increase their awareness in an interactive manner	- They didn't suggest a specific solution to prevent or detect ransomware infection. - They just confirmed the efficiency of using the "perfc" file to avoid "NotPetya" ransomware.
12	Zimba et al. [21], 2018	Studied the emerging cyber threat to the critical infrastructure	Uncovered the WannaCry employed techniques to discover vulnerable nodes.	The discovered network interactions adopted only by WannaCry ransomware.
13	Zimba and Mulenga [22], 2018	Employed reverse engineering on the underlying malware program logic	Unmasked WannaCry ransomware network interactions	

Table (2) (Related Work Summary)

No.	Researcher/s	Contribution	Pros.	Cons.
1	Almashhadani et al. [23], 2019	Proposed a multi-classifier network-based ransomware detection.	Implemented a network-based intrusion detection system.	- The extracted network traffic is specified to "Locky" ransomware. - Not all ransomware families connect to command and control servers such as "win-locker" for example.
2	Akbanov et al. [24]	Accomplished extensive dynamic analysis on WannaCry ransomware	The results of this research can help to accomplish an efficient mitigation mechanism against WannaCry	The uncovered network attitude is utilized by WannaCry ransomware only.
3	Hull et al. [25], 2019	Proposed Randep a predictive model for categorizing ransomware according to its behavioral characteristics.	It can be used for improving detection and handling of ransomware incidents.	Not all ransomware families go through all these deployment stages.
4	Chen and Bridges [26], 2018	Presented a method to automatically extract distinguishing features of malware from host logs.	- It can be used to improve ransomware detection and make it more robust to polymorphism.	They didn't suggest a specific solution to prevent or detect ransomware infection.
5	Verma et al. [27], 2018	Implemented an automated system using supervised machine learning classifiers to classify the ransomware samples.	Classifying the ransomware variants in the real-time environment.	- Misclassification due to decision boundary errors. - Some ransomware has limited file system activity. Though, a few user files may be encrypted.
6	Ami et al. [28], 2019	Adopted authentication-based access control mechanism.	It can halt file modification attempts such as renames or deletions.	Users may grant access to a process which, is infected with a malicious code.
7	Christopher and Kumar [29], 2019	Presented a preventative technique based on ransomware behavior.	Alter access control levels of files and folders to revoke ACL writing privileges when compromise confirmed.	The system will suffer from a lot of strain when the monitoring is done on physical drives instead of artificial drives.
8	Lee et al. [30], 2017	Provided a new technique to recover from a ransomware attack using key backup.	The recovered key used for file recovery after ransomware infects the system and encrypt user files.	- Not all ransomware uses the CNG library such as "Cryptolocker"

				- Not all ransomware obtains the key from the server like "Ordinypt" and "Petya". - Monitoring the outbound communication can be easily avoided by encrypting these connections.
9	Zimba et al. [31], 2019	Categorized ransomware based on data deletion and file encryption attack structures.	This framework helps to uncover ransomware design flaws in order to exploiting them in data recovery, via system volume shadow copies or third-party software without paying the ransom.	Some ransomware has an irreversible impact, for example, no actual solution could be used to decrypt the encrypted hard disks by NotPetya.
10	Zimba et al. [32], 2018	Evaluated the underlying ransomware attack structures and data deletion techniques.	Its concluded that the key to data recovery options lies in, uncovering the underlying of attack structure and the implemented data deletion methodology.	
11	Gómez-Hernández et al. [33], 2018	Proposed a general methodology called R-Locker to thwart crypto ransomware actions.	The proposed methodology eliminates the ransomware when it accesses a trap file, thus allowing to preserve the rest of the data.	- just a part of the complete file system is protected. - the poor distribution of the traps can reduce the efficiency of data protection. - this defense can be passed over by the removal of the central trap file. - it can be partially bypassed by accessing given folder files by ransomware in a random way where all files in the folder may be encrypted before the sample can be blocked.
12	Wang et al. [34], 2018	Utilized cyber deception technology by trapping attackers.	- This approach helps to Protect important hosts under targeted ransomware attacks. - Utilized NLP and machine learning to trace-back RDP-based ransomware attacks and identify the original attack sources.	This approach is just for hindering RDP-based ransomware attacks only.
13	Shaukat and Ribeiro [35], 2018	Presented "RansomWall", a layered defense system for protection against cryptographic ransomware.	When the trap layer suspects a process as malicious, the modified files are backed up until it is classified as ransomware or benign by the "machine learning layer".	- User critical files may be attacked earlier than honey files. - Some ransomware has limited file system activity. Though, a few user files may be encrypted. - Another misclassification is due to decision boundary errors.

4. CONCLUSION

With the existence of ransomware as a service (RaaS) which, facilitates obtaining ransomware codes easily. In addition to the availability of free development kits, such as "Torlocker, TOX and Hidden-Tear" which, are available for unskilled individuals. This greatly reduces the entry barrier of ransomware remunerative business, and its activities are only expected to be on the rise and users should brace themselves against such attacks.

The more critical the data, the more likely the victim is to pay the ransom. Reversing ransomware encryption is quite difficult and consumes time and resources. Even though, employing techniques such as reverse engineering and cryptanalysis will contribute considerably to ransomware attacks declining. These techniques will make it possible for victims to regain access to their files without paying the ransom.

Moreover, approaches to prevent ransomware and protect devices are necessary. But ransomware developers will soon adapt to the current detection tools and new families with different behavior will spread.

5. FUTURE WORK

In the future, this work will be extended by establishing an efficient hybrid approach that combines two or more techniques to prevent ransomware and make user data more resistant to ransomware. Also, the work can be extended to be the foundation to propose a ransomware prevention model.

6. REFERENCES

[1]. Popli N, Girdhar A. Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware. In Verma, Nishchal K, Ghosh, A. K. (eds) Computational Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80.

[2]. Caporusso N, Chea S, Abukhaled R. A game-theoretical model of ransomware. In: Proceedings - International Conference on Applied Human Factors and Ergonomics 2018 Jul 21 (pp. 69-78). Springer, Cham.

[3]. Morgan, Steve. "Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics." Cybercrime Magazine Cisco and Cybersecurity Ventures. 2019, https://www.cybersecurityventures.com/cybersecurity- a lmanac- 2019.

[4]. Maccari M, Polzonetti A, Sagratella M. Detection: Definition of New Model to Reveal Advanced Persistent Threat. InProceedings of the Future Technologies Conference 2018 Nov 15 (pp. 305-323). Springer, Cham.

[5]. Al-rimy B, Maarof M, Shaid S. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers and Security. 2018; 74:144-166.

[6]. Rajput T. Evolving Threat Agents: Ransomware and their Variants. International Journal of Computer Applications. 2017 April;164(7):28-34.

[7]. Kok S, Abdullah A, Jhanjhi N, Supramaniam M. Ransomware, Threat and Detection Techniques: A Review. IJCSNS International Journal of Computer Science and Network Security. 2019;19(2):136-146.

[8]. Tandon A, Nayyar A. A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat. InData Management, Analytics and Innovation 2019 (pp. 403-420). Springer, Singapore.

[9]. Zimba A, Chishimba M. On the Economic Impact of Crypto-ransomware Attacks: The State of the Art on Enterprise Systems. European Journal for Security Research. 2019 January;4(1):3-31.

[10]. BBC-News 2019, *Baltimore ransomware attack: NSA faces questions*, BBC-News, viewed 28 December 2019, https://www.bbc.com/news/technology-48423954/

[11]. Wikipedia 2019, *WannaCry ransomware attack*, Wikipedia, viewed 28 December 2019, https://en.wikipedia.org/wiki/WannaCry_ransomware_attack/

[12]. Goyal, P.; Kakkar, A.; Vinod, G. & Joseph, G. Crypto-Ransomware Detection Using Behavioral Analysis *Reliability, Safety and Hazard Assessment for Risk-Based Technologies, Springer*, 2020, 239-251.

[13]. Grant L., Parkinson S. Identifying File Interaction Patterns in Ransomware Behavior. In: Parkinson S, Crampton A, Hill R. (eds) Guide to Vulnerability Analysis for Computer Networks and Systems. Springer, Cham. 2018;14:317-335.

[14]. Kok SH, Abdullah A, JhanJhi NZ, Supramaniam M. Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm. Computers. 2019 Dec;8(4):79.

[15]. Scaife N, Carter H, Traynor P, Butler K. CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. In: Proceedings - International Conference on Distributed Computing Systems. 2016 August;2016:303-312.

[16]. Wolf J. "Ransomware Detection." Friedrich-Alexander-University Erlangen-Nuremberg. 2018.

[17]. Continella A, Guagnelli A, Zingaro G, Pasquale G, Barenghi A, Zanero S, Maggi F. ShieldFS: A Self-healing, Ransomware-aware Filesystem. In: Proceedings - Annual Computer Security Applications Conference (ACSAC). 2016 December:336-347.

[18]. Kharraz A, Kirda E. Redemption: Real-Time Protection Against Ransomware at End-Hosts. In: Dacier M, Bailey M, Polychronakis M, Antonakakis M. (eds) Research in Attacks, Intrusions, and Defenses. Springer. 2017;10453:98-119.

[19]. Winter R, Ruiz R, Army B, Archer R. Cyber Autoimmune Disease When the Virtual Life Imitates the Real Life. International Journal of Cyber-Security and Digital Forensics (IJCSDF).2018;7(1):21-30.

[20]. Lika R, Murugiah D, Brohi S, Ramasamy D. NotPetya: Cyber Attack Prevention through Awareness via Gamification. In: International Conference on Smart Computing and Electronic Enterprise (ICSCEE).2018:1-6.

[21]. Zimba A, Wang Z, Chen H. Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. ICT Express. 2018;4(1):14-18

[22]. Zimba A, Mulenga M. A Dive Into the Deep: Demystifying Wannacry Crypto-Ransomware Network

Attacks Via Digital Forensics. International Journal on Information Technologies & Security. 2018;10:57-69.

[23]. Almashhadani A, Kaiiali M, Sezer S, O'Kane P. A Multi-Classifier Network-Based Crypto-Ransomware Detection System: A Case Study of Locky Ransomware. IEEE Access. 2019;7:47053-47067.

[24]. Akbanov M, Vassilakis VG, Logothetis MD. WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention, and Propagation Mechanisms. Journal of Telecommunications & Information Technology. 2019 Mar 1(1).

[25]. Hull G, John H, Arief B. Ransomware deployment methods and analysis: views from a predictive model and human responses. Crime Science. 2019 February;8(1)1:22.

[26]. Chen Q, Bridges R. Automated behavioral analysis of malware: A Case Study of Wannacry Ransomware. In: Proceedings - 16th IEEE International Conference on Machine Learning and Applications, (ICMLA) 2017. 2018 January:454-460.

[27]. Verma M, Kumarguru D, Deb S, Gupta A. Analyzing indicator of compromises for ransomware: Leveraging IOCs with machine learning techniques. IEEE International Conference on Intelligence and Security Informatics, (ISI). 2018:154-159

[28]. Ami O, Elovici Y, Hendler D. Ransomware prevention using application authentication-based file access control. In: The 33rd ACM/SIGAPP Symposium on Applied Computing. Pau, France. 2018 April:1610-1619.

[29]. Chew C, Kumar V. Behavior Based Ransomware Detection. In: Proceedings - 34th International Conference on Computers and Their Applications. 2019;58:127-116.

[30]. Lee K, Oh I, Yim K. Ransomware-prevention technique using key backup. Lecture Notes of the Institute for Computer Sciences, Social-Informatics, and Telecommunications Engineering (LNICST). 2017 August;194:105-114.

[31]. Zimba A, Wang Z, Chishimba M. Addressing Crypto-Ransomware Attacks: Before You Decide whether To-Pay or Not-To. Journal of Computer Information Systems. 2019 January;4417:1-11.

[32]. Zimba A, Wang Z, Simukonda L. Towards Data Resilience: The Analytical Case of Crypto-Ransomware Data Recovery Techniques. International Journal of Information Technology and Computer Science. 2018 January;10(1):40-51.

[33]. Gómez-Hernández J, Álvarez-González L, García-Teodoro P. R-Locker: Thwarting ransomware action through a honey-file-based approach. Computers & Security. 2018;73:389-398.

[34]. Wang Z, Cui X, Su S, Qiu J, Liu C, Tian Z. Automatically Traceback RDP-Based Targeted Ransomware Attacks. Wireless Communications and Mobile Computing. 2018;2018:1-13.

[35]. Shaukat S, Ribeiro V. RansomWall: A Layered Defense System against Cryptographic Ransomware Attacks using Machine Learning. In: Proceedings - 10th International Conference on Communication Systems & Networks (COMSNETS). 2018:356-363.

RAPID7

SOLUTION GUIDE

Ransomware Playbook

Actions you can take to lower the risk and impact of this kind of attack.

TABLE OF CONTENTS

Introduction

Failing to plan is planning to fail. The old adage holds true now more than ever as companies, governments, and institutions around the world grapple with the ever-changing threat of ransomware.

The Institute for Security and Technology's Ransomware Task Force Report notes that "in 2020, thousands of businesses, hospitals, school districts, city governments, and other institutions in the U.S. and around the world were paralyzed as their digital networks were held hostage by malicious actors seeking payouts."

Victims of ransomware attacks suffer both the impact of productivity and revenue loss due to work stoppage, and potentially may also incur a loss of confidence or reputational hit, which can also impact revenue. Those businesses are also likely to have to manage communications with the press, customers, prospects, and vendors as well.

But it doesn't have to be this way.

Ransomware is a unique security threat where most of the security team's effort is spent on prevention and response because once ransomware is detected, it's too late. However, there are many actions you can take to lower the risk and impact of this kind of attack. This playbook aims to provide exactly that. It will give security professionals and business leaders the knowledge and tools to not only prevent ransomware attacks to the best they can be prevented, but to create a remediation plan that can save critical information from the worst types of exploitation.

With ransomware, plan to prevent, plan to protect.

What is ransomware?

First, let's define ransomware. Ransomware is a sub-category of malware, a class of software designed to cause harm to a computer or computer network. CISA defines ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."

How do ransomware attacks happen?

Ransomware attacks happen similarly to other malware-based attacks. Here's an example of a typical phishing-based ransomware attack from an incident response engagement Rapid7 conducted, where the customer's environment was encrypted using the popular Ryuk ransomware.

The threat actors conducted targeted spear-phishing attacks against multiple users at the customer account, sending the emails from a compromised third party that the users already had an established relationship with.

The user clicked on a link in the phishing email that instructed the user to install software to view a PDF. Once executed, TrickBot malware was installed on the system.

Leveraging this initial foothold, the threat actors leveraged TrickBot modules to harvest credentials using Mimikatz, and moved laterally in the environment using PowerShell Empire. Within a few days, the threat actors gained access to an account with elevated privileges, and deployed Ryuk ransomware to hundreds of systems in the environment using the Windows system administration tool PsExec.

Typical delivery methods

As the example above shows, the first step of any ransomware attack is to get the malware installed on the host system. This typically occurs using specific techniques for initial access:

- **Spear phishing** - where the victim receives an attachment or link that they click
- **Drive-by** - where an attacker can exploit a vulnerability in the web browser or related applications
- **Exploitation** - where an attacker can exploit a vulnerability and gain access to a remote system or allow the ransomware to propagate automatically
- **Replication through removable media** - this also includes networked media that ransomware encrypts at the same time as it infects the victim
- **Valid accounts** - where an attacker has valid credentials to the target system and can authenticate to it

From there, attackers will use common techniques for execution, typically through:

- Command-Line Interface / Graphical-User Interface
- PowerShell
- Scripting
- User execution

How have attackers changed?

For many ransomware attacks in the past, threat actors employed mass spam campaigns to socially engineer users into clicking links or attachments. Once clicked, ransomware encrypted the system and, in an automated fashion, potentially encrypted other systems where access was established or allowed, such as a mapped file share. Increasingly over the past few years, there has been a shift to "big-game hunting" threat actors leveraging access established by taking advantage of poor security controls in an environment. Those controls can often be an unpatched externally facing server, unsecured remote access solutions, or an undetected banking trojan (such as TrickBot, Emotet, or Dridex).

When access is gained, the threat actors go "hands on" using post-exploitation frameworks to recon the environment and gain elevated privileges. If a threat actor gains unfettered access to the environment, they can encrypt the network en masse (deploying Ryuk or BitPaymer), leading to complete disruption of business services. Many times this leads to ransomware taking down large healthcare centers and hospitals, manufacturing facilities, educational institutions, municipalities, and other corporations.

These big-game hunting threat actors have continued to increase their ransom demands, which are now regularly exceeding seven figures. In addition to rendering the network unusable, some of these threat actors exfiltrate sensitive data and extort their victims by threatening to release the data. In this scenario, criminal groups are increasingly demanding two ransom payments: one for decrypting all the systems on the network and one for keeping the exfiltrated from attacker data sharing platforms. These types of attacks are known as "double extortion ransomware."

There is another emerging scenario of "triple extortion ransomware" whereby attackers infiltrate an organization, steal data, encrypt systems and then demand the traditional payment for decryption keys. If a victim organization refuses to pay, the attackers threaten to publicly release records either all at once, or piecemeal, until payment is made. With the release of data, the attackers then use customer, partner, and/or vendor information stolen from the victim to conduct denial of service attacks on those third-parties or contact those third-parties (to put payment pressure on the original victim organization), and demand smaller payments from these secondary victims to prevent their data from being included in any public release.

Recent years have also seen the rise of the "ransomware as a service" (RaaS) business model, which provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop malware on their own. This "as a service" model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from "software as a service" and "infrastructure as a service" business models.

The importance of having a full incident response plan

Ideally organizations want to avoid becoming the victim of ransomware attacks, and there are a number of steps that can be taken to reduce the risk and make the job harder for attackers, detailed below. These measures take time to implement though, and while they should make an organization harder to compromise and more able to recover from attack, no organization can be completely invulnerable. As such, it is critical to have a comprehensive incident response plan in place so that if the worst does happen, you are able to react quickly and efficiently to weather the storm.

It may seem counterintuitive to work on response before the incident, and even before deploying preventative measures, but we strongly recommend you do just that — develop and practice your incident response plan now. You need this in place while you work on your preventative measures so you will be prepared if you have an incident before you can fully implement your defenses. Without the proper preparation, an attack can bring your business to a grinding halt and put your critical information at risk.

A comprehensive incident response program will incorporate the following:

1. **Preparation** - Are you ready if a ransomware attack happens? Do you have a playbook? Does your team know what to do and who is responsible?

2. **Identification** - What are your measures to identify ransomware before machines are encrypted and a message asks you to pay? How can you identify that an attack is taking place before ransomware is executed?

3. **Containment** - Do you have proper methods (or have automation workflows) in place to contain threats early in the attack chain? The earlier you're able to contain the threat, the more likely you are to restrict the ability of an attacker to execute the ransomware.

4. **Eradication** - Can you eradicate the threat on your own, or do you have an Incident Response retainer set up in the event of a breach? Cleaning things up is one of the last things to do in a ransomware attack. Are you able to scope the incident thoroughly to understand what happened and prevent it from happening again? Do you have the expertise on staff to eradicate the threat completely, ensuring you're not going to get encrypted in a week?

5. **Recovery** - Do you have proper measures in place to recover from an attack and get things back to normal as soon as possible?

6. **Review Lessons Learned** - What is your postmortem process? How can you use this as a lesson to improve your security posture?

Ransomware threat prevention and response

To prevent ransomware threats, there are two distinct phases of the attack lifecycle where you can act. In MITRE ATT&CK parlance, those are the initial access phase and execution phase. The ransomware needs to get past the perimeter and run.

Before the attack: Avoiding ransomware and reducing risk

To reduce risk, organizations should focus on minimizing the attack surface by looking at the specific techniques attackers are using to deploy ransomware. From there, security teams can apply layers of preventative measures and reduce risk.

Workforce education training

Workforce education is the first line of defense in your preventative arsenal; people should not be clicking suspicious links or visiting websites that are known carriers of malvertising networks. Hopefully these sites are blocked by your organization's firewall settings, but educating employees about the risks and reinforcing the guidance in the Acceptable Use Policy will also help reduce risk.

Organizations should look to add technology and content that reminds workers to be cautious when they need to be cautious. It sounds complicated, but notices on emails originating from outside sources including a reminder to be vigilant are effective.

Education programs should address the following:

- Use caution when opening links or attachments by considering:
    - Do I know the sender?
    - Does this look suspicious?
    - Is this something that I should open or a link I should follow?
- Use a Virtual Private Network (VPN) when performing any work task to gain the benefits of all implemented security controls.
- Do not provide personal details when answering emails, phone calls, texts, or other messages, and contact the IT department as soon as possible if you receive suspicious communication.
- Validate IT resources and communications to ensure communications from new contacts are not an attempt at social engineering.
- Alert the IT department before traveling internationally.

Reduce the attack surface

One of the best ways to lower the possibility of a successful ransomware attack, or any other cyber attack, is to reduce your attack surface. While the discipline of attack surface reduction could fill several playbooks and guides on its own there are some basic tenants that all organizations should be following:

- **Detect and monitor for what you AREN'T scanning** - Your vulnerability management (VM) program should include a periodic coverage check, this can certainly be automated if accurate source data is available. Remember cloud and ephemeral assets are part of your attack surface too.

- **Make friends with the application development team** - Application weaknesses — be it from misconfigurations, logic flaws or poor coding hygiene — can all contribute to an organization's attackable surface. So aside from bureaucracy, organizational structure, incentives and time, what is stopping application security management from being a fully ascribed member of the illustrious VM team? Start with a conversation. Reporting and managing risk across the full stack will aid in securing investment and support for refactoring efforts and overdue architectural changes.

- **Vulns come in all shapes and sizes** - Pick up a recent copy of your favorite cyber security trends report and you'll be reminded that a substantial portion of recent (reported) breaches and attacks are due in some way to misconfigurations in cloud-based and traditional infrastructure. Days of ignoring good 'ole configuration management have passed. Hardening baselines must be implemented and maintained under the umbrella of an effective VM program. If you're just starting out, pick an operating system with a smaller footprint or maybe the workstation environment. Slow and steady wins the race, here.

- **Walk a mile in operation's shoes** - The men and women with the much more challenging role in the VM lifecycle are the patching and administration teams. They are tired of getting lists of unverified vulns that number in the 1000's. Simply taking the time to fully understand their workflow, stakeholders and approval gates will go a long way in giving the VM team valuable insights to rejigger their reporting and vulnerability dissemination process. Meet operations where they live — it'll make your work life more satisfying.

Far from an exhaustive list, these themes have a history of recurring across organizations, industries and entire sectors and are areas Rapid 7 can help support, educate and deliver. Defense in depth applies here and causes an echo that attack surface management is an organizational level responsibility.

Purposeful network segmentation can ensure that critical machines are isolated to prevent the spread of malware. Start with the really important stuff. There is value in getting started, if only for certain segments and CIDR ranges. This is an important step in lowering the potential, and impact, of a ransomware attack.

Ensure account permissions are managed appropriately

Creating granular controls on user rights, specifically restricting administrative rights on endpoints, can reduce the attack surface and capabilities for malware to spread across the network. These include:

- Restricting write permissions for servers
- Restricting admin users and privileged accounts
- Granting users the lowest-level system permissions that still allow them to do their job
- Removing abilities for users to install and run unapproved software applications on the endpoint

Blocking indicators of the ransomware

Blocking indicators of malicious executables will prevent the ransomware from executing and communicating with the command-and-control server. Doing so may prevent subsequent infections from fully encrypting the target data. For example, proper mail scanning should have the ability to filter files by extension, specifically ".exe" files.

Mitigate spear phishing

Spear-phishing mitigation technology can be deployed to inspect links and attachments at the mail server. The amount of risk organizations reduce is directly proportional to the layers of technology and controls applied. An optimal layered approach would include technology that looks for known threats in attachments and links, technology to run and perform analysis on suspicious attachments and links, and technology that would enforce the reputation of the sender (though this might impact the ability for the business to fully operate).

Mitigate drive-by attacks

Drive-by web proxy technology can be deployed to inspect web browsing activity for ransomware threats. The amount of risk reduction here is directly proportional to the layers of technology and controls applied.

An optimal layered approach would include domain name resolution sinkholing to prevent users from accessing malicious domains, content inspection technology to identify and evaluate applications being transferred across the network, and network threat prevention technology to block access to known bad IP addresses.

Mitigate exploitation

Exploitation mitigation is achieved by efficient patch management. Routine scanning for vulnerabilities, prioritizing them based on active threats, and quickly deploying patches are the keys to success. Ensuring operating systems and any software running on the machines on your network are patched with the latest updates reduces the number of exploitable entry points for an attack. One common area attackers are exploiting is via third-party software such as Java, Flash, and Adobe. Many common attacks can be prevented by ensuring often-targeted software is patched. It is also important that you have a way to scan and patch remote endpoints such as the laptops of remote employees.

An optimal approach would involve weekly scanning for vulnerabilities, dynamic prioritization of vulnerabilities based on how they are being used by attackers, and a less-than-24-hour patching timeline for critical remediations. It's best to use automated patching when possible.

Mitigate replication through removable media

Replication mitigation can be summarized by undoing all that Windows does to make networked computing easy:

- Do not use persistent mapped network shares.
- Do not allow removable media to be automatically mounted.
- Prohibit writing to removable media.
- Apply a layered network architecture and prohibit discovery of Windows operating systems across network zones.

Mitigate invalid accounts

Valid account mitigation can be achieved by enforcing multi-factor authentication (MFA) to valuable data assets in your environment. Further, enforcing a stricter authorization model instead of the traditional default allow will reduce the impact of credential theft.

Mitigate execution

Execution mitigation technology like next-generation antivirus (AV), endpoint detection and response, firewalls, behavioral-based detections, application whitelisting, and sandboxing can be deployed to add layered defenses to prevent the threat of ransomware on the endpoint.

In the case of AV or anti-malware solutions, this is typically one of the first lines of defense for your business, blocking payloads from launching. It's imperative to keep AV solutions up to date to ensure the most recent signatures of new malware variants are being assessed. Sandbox technology gets the honor of mitigating both risk and impact as the sandbox will typically not let the ransomware permanently encrypt resources. There are also many controls that can be deployed, including limiting user permissions, restricting scripting capabilities, and limiting administrative tools on workstations.

Monitor your environment for process-related triggers

Developing policies for disabling macro scripts unless approved by security is one way to prevent exploits delivered by common documents. However, it should be standard to disable executables, such as macros, from running from any email attachment.

Users who open attachments and enable macros often execute the payload, which installs malware on the machine. One way to spot this type of malicious execution is to monitor the process start/stop on the machine and to correlate the opening of a document, for example, PowerShell invocation spawned from a Word document. This is rarely an action taken by a user, so this type of action would most likely be correlated to an

Implement early detection mechanisms

The last lever to pull in avoiding ransomware is to detect an infection before it spreads. Of course, if you detect ransomware, it's already too late, but there is often a period of time to respond to indicators of threats before ransomware hits, or to limit the spread of the encryption and impacted data if ransomware is present on systems.

Detecting ransomware can be done with traditional detection methods like simple indicator matching, user behavior analytics, or attacker behavior analytics (including process spawning). Ransomware carries similar traits to traditional malware. Once detected, quickly implementing remediation steps is paramount.

You should consider some automation solutions with the following capabilities:

- User account actions, such as locking or deleting an account and/or forcing a reset
- Firewall IP address blocking
- Domain blocking
- Process termination
- Physical network port blocking

Important prevention considerations

Is the ransomware attack really the end goal of the attacker?

Over the last few years, we've started to see an increase in ransomware being used to cover up for other attacks. Initially, it was thought the attackers' motivation was to distract responders, but it could be possible that attackers are realizing how numb we're becoming to these types of attacks; to the point where we're not even investigating them anymore. It's best practice to investigate the rest of your detection telemetry for anomalies in addition to the ransomware attack. It's very possible that there may be something more nefarious going on. This means ensuring you have visibility into environments where intellectual property, employee, and partner/customer records are held, accessed, and processed.

Don't get caught out by recency or news bias

For those with a tested disaster recovery plan and desire to still do more, beware the common mistake the human mind makes called the "focusing illusion," or convincing oneself that a current event or problem in focus is the most important one. This frequently leads to losing sight of the bigger picture and improperly planning for the future. If you are going to focus your defensive efforts solely on ransomware, it will make you more susceptible to the many other security threats to your business. As you work to build up your ransomware prevention capabilities, see how these control enhancements fit into the bigger threat, vulnerability, and risk management picture.

During the attack: Response priorities; Containment; Payment considerations

To limit the impact of a ransomware attack, security teams need to limit its access to mission-critical data and be able to quickly recover data encrypted by the ransomware. Mapped to the MITRE ATT&CK framework, the specific technique that attackers use is "Data encrypted for impact." Security teams should ensure that all techniques for limiting access to mission-critical data are listed in the above 'Ransomware threat prevention and response' section.

Additional actions to ease the speed with which your organization recovers from a ransomware breach include the following:

Removing infected systems from the environment

This may be a technological solution like disabling a physical network port, or a manual process like physically removing the network cable from the port. Removing infected assets can help limit the replication of the ransomware to adjacent assets.

Restoring data with no loss

The first step to ensuring business continuity in the event of a ransomware attack is to employ a comprehensive data backup and recovery plan for all high-value data. The good news is that backing up your systems (and testing the restore) should be a high-priority investment anyway.

The healthiest way to think about your ransomware-locked systems is the way you'd think about laptops your employees dropped on business trips. Sure, you might recover the data on them if you keep at it, but it would save everyone a lot of time and effort if you just restore the backup images from last night to the impacted systems (or replacement laptops). Great backup hygiene is somewhat like your insurance policy. And, it's most likely something your IT team is doing anyway to prepare in the case of natural disasters (like floods) or building disasters (like broken water pipes).

Simply backing up files is not enough, however; important files and backups should be isolated on external storage devices or in the cloud, disconnected and inaccessible from any potentially infected computer once the backup is completed. It's important to perform backups and test these in a real-world environment to limit the impact of data loss and ensure the backups can recover quickly should a ransomware attack occur.

Issuing new assets

Part of reducing the impact of ransomware is ensuring employees can do their job as quickly as possible. It's important that the Security and IT teams audit and practice these business continuity plans. Teams prefer not to be in a position where they find out there are no more assets in the IT closet and data backups haven't run in 7 days when trying to recover from a breach.

Avoiding duplicate attacks

It is not uncommon for organizations who have suffered through a ransomware attack to be attacked repeatedly by the same attacker group or other attacker groups. To avoid becoming a repeat victim, you must quickly identify and remediate the initial access and execution vectors in the first attack, then ensure the original attackers have been eradicated from all networks and assets.

Should you pay the ransom?

The ultimate question when it comes to ransomware is: to pay or not to pay?

Hopefully, following the above recommendations to proactively prevent ransomware attacks and limit their impact if the attack is successful allows your business to avoid considering the question in the first place. But if your files are encrypted, what do you do?

Before you consider paying a ransom, we strongly recommend you investigate alternatives. For example, the No More Ransom project is a collaboration between Europol, various government agencies, and the private sector to gather and share decryption keys. Many governments and law enforcement agencies also offer guidance on recovery and response, so it is worth checking their websites and consulting law enforcement.

It is also critical to understand that even if you pay the ransom and the attackers do release your data and systems, that will not be the end of the matter. You will still need to thoroughly inspect your environment to determine the true scale of the incident, and confirm the attackers no longer have a presence in your system and have not stolen data or caused other harm. You will also need to take steps to harden your systems against a similar attack, and in some cases, you may have to take steps to rebuild or recover systems impacted by the attack. Although attackers involved in the ransomware attack against HSE, Ireland's national health authority, released the decryption keys, HSE has reported that it believes recovering from the attack will cost $600 million.

Most stances, including that of the U.S. FBI, recommend not paying the ransom demanded by cybercriminals. Similar to other criminal actions, it's recommended not to negotiate, since there is no guarantee the criminals will send you the decryption keys and you'll regain access to your files. Paying the ransom will encourage criminals to continue carrying out these attacks by funding their activity, and once a criminal group knows you are willing to pay, they may look for other ways to victimize you.

In addition, proceeds from ransomware may help finance child exploitation, human trafficking, or the proliferation of weapons of mass destruction. In some cases and jurisdictions, paying a ransom demand may be a criminal or sanctionable offense. In October 2020, The U.S. Department of the Treasury Office of Foreign Assets Control (OFAC) issued an Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments to highlight the risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities. The G7 issued a similar advisory in their October 2020 Ransomware Annex to G7 Statement.

After the attack: Ransomware response actions

When facing a ransomware attack, it's best to have a playbook of what to do. The majority of ransomware attacks are still initially spawned by malicious documents or malware. We recommend ensuring your team takes the below prescribed actions to stop ransomware attackers early.

Remediation steps

Rapid7 recommends:

- **rebuilding** systems from known-good baseline images to counter undetected threats.
- **scanning** systems with an up-to-date anti-malware solution to remove malware and related artifacts.
- **blocking** malicious domain(s) and IP addresses. This should be performed at all appropriate network filtering and domain name server devices such as firewalls, web proxies, switches, and DNS servers.
- **terminating** malicious processes on the compromised endpoint(s) identified.
- **quarantining** affected endpoints from the network.
- **locking** affected compromised account(s) until the credentials can be rotated.
- **changing** affected account(s) password(s) as soon as possible to prevent an attacker from leveraging the credentials to access services.
- **determining** whether other users received malicious communications and removing them from all mailboxes.
- **blocking** the sender's email address (if applicable).

Mitigation steps

Rapid7 recommends:

- **removing** a user's domain account from the local administrator group. User accounts with administrator rights allow for automated and targeted attacks to interact with system-level privileges, including dumping credentials, modifying firewall rules, disabling security controls, and deploying malware. If you need some direction, Microsoft's LAPS is a great tool to manage local administrator passwords.
- **conducting** phishing-based user awareness training and know how to forward suspicious links to the IT security group for analysis.

- **disabling** execution of macros in the Microsoft Office suite from untrusted locations via Group Policy. Office macros account for approximately 98% of Office malware; disabling macros significantly decreases the attack surface of user workstations.

- **ensuring** unique passwords for local administrator accounts (if applicable). Local administrator account passwords should be unique per system to prevent lateral movement due to local credential compromise.

- **implementing** application whitelisting for critical systems, such as domain controllers and Exchange servers. Application whitelisting reduces the likelihood that attackers could execute malware or unapproved utilities, and is less labor-intensive to implement on systems with static configurations.

- **creating** separate user accounts for privileged and non-privileged domain activities. Privileged domain accounts should only be used when required to perform maintenance or other system administration activities, and non-privileged user accounts should be used for normal daily activities.

- **reviewing** URL and firewall outbound access policies and blocking high-risk categories (adult material, games, gambling, advertisements, peer-to-peer file sharing, Dynamic DNS, as well as categories such as spyware, phishing, keylogging, and malicious mobile code).

- **following** vendor-recommended guidelines for security settings on Windows, Mac, and Linux platforms.

- **preventing** activation of OLE packages in Microsoft Word to prevent users from launching malicious packages.

How Rapid7 can help

Preventative measures

Since it is commonplace for ransomware to leverage vulnerabilities to propagate itself, maintaining a proper vulnerability risk management program is critical. Solutions like Rapid7's leading Vulnerability Risk Management Solution, InsightVM can help detect and prioritize assets that may be ideal targets for spreading malware.

Incident detection

Rapid7's leading detection and response solution, InsightIDR (the basis for the MDR technology used by our SOC) uses a variety of mechanisms to detect ransomware in your environment, utilizing the configured foundational event sources and the endpoint agents.

In addition to the actual encryption of files, ransomware depends on several main stages that our solution is designed to circumvent:

Stage	Example InsightIDR / MDR Detection
Initial Access	User behavior analytics and other authentication-based detections to alert on unusual account activity.
Execution	Detection rules for common malware launching techniques used by RansomWare groups.
Privilege Escalation	Many detections for common privilege escalation techniques.
Defense Evasion	Detections for clearing of logs, disabling backups and shadow copies, and more.
Credential Access	Various detections around password spraying and brute force attack, credential dumping and more.
Discovery	Detections for tools used by attackers for network group and account enumeration. Also for discovering network trust relationships.
Lateral Movement	Detections for WMI, Powershell, etc and other common techniques used by attackers to perform remove command execution.
Command and Control	Coverage for common C2 tools like Cobalt Strike.
Impact	Detections for the deletion of backup files and shadow copies.

In addition to what we have listed above, the Rapid7 Threat Intelligence team is continuously coming up with new detections from our honeypot network (Project Heisenberg), as well as participating in other cyber-threat feeds.

Beyond curated threat signatures, InsightIDR comes with pre-built Attacker Behavior Analytics (ABA) detections built by the Rapid7 Threat Intel team. ABA applies Rapid7's existing experience, research, and practical understanding of attacker behaviors to generate investigative leads based on known attacker tools, tactics, and procedures (TTP).

It's also worth clarifying that InsightIDR and the MDR service are both based on detection, not prevention. The detections that Rapid7 have in place for ransomware will identify ransomware should it occur; however, this will not prevent ransomware from occurring. Rapid7 strongly recommends patching vulnerabilities found in the environment, user education, and robust backup procedures to reduce the likelihood of a successful ransomware attack.

Automated response

Leveraging security orchestration, automation, and response (SOAR) solutions like Rapid7's InsightConnect can help lessen the severity of such attacks — or prevent them altogether — by reducing the time it takes to contain, block, or reduce privileges to endpoints. As such, it is important to ensure you can access such orchestration platforms from unaffected workstations.

Many of the above playbook recommendations for containment, remediation, and mitigation can be achieved through automation in conjunction with endpoint detection and response tools you've most likely already deployed. To explore our growing library of prebuilt plugins and workflows, please visit Rapid7 Extensions.

Final recommendation

If this all sounds complicated, that's because it is. Ransomware continues to evolve to evade the technological solutions we have in place; it is time that all of our security programs rise to support the tools.

The best solutions in security always involve people, process, and technology. Yet, our security programs consistently favor the technology, leaving the people to struggle with overwhelming data and inconsistent processes.

Rapid7 encourages all security teams to build a ransomware defense plan with proper security hygiene, defensive tactics, and a continuity plan to better prepare and respond to ransomware attacks.

Finally, a ransomware plan is useless unless it is practiced and kept up to date. All security staff should rehearse what to do when responding to a ransomware scenario and be prepared to act if a ransomware attack was successful.

CIRT Playbook Battle Card: **GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware**

(P) Preparation

1. Patch asset vulnerabilities
2. Perform routine inspections of controls/weapons
3. Confirm backups are free of malware
4. Establish ability to pay ransoms w/cryptocurrency
5. Obtain decryption keys for ransomware variants
6. Confirm cybersecurity insurance coverages
7. Conduct ransomware simulations
8. Conduct phishing simulations
9. Conduct user awareness training
10. Conduct response training (this PBC)
11. Examine file shares for loose/open privileges
12. Maintain Antivirus/EDR application updates
13. Create network segmentation
14. Log traffic between network segments
15. Incorporate threat intelligence
16. Incorporate deception technology
17. Perform routine inspections of asset backups
18. Validate proper functionality

(I) Identification

1. Monitor for:
   a. Ransomware notes/messages
   b. Unusual file extensions or maliciousextensions
   c. User reports of files being corrupt or notreadable
   d. Emails with suspicious attachments
   e. Unusual DNS traffic
   f. High velocity renaming of files
   g. CPU spikes on file sharing systems
   h. Unusual userland executable binaries
   i. Anomalous network connections on hosts
   j. Firewall denies to well known file sharingports
   k. Network connections to known C2 andexploit kit locations
   l. Use of TOR or I2P
2. Investigate and clear ALL alerts of possible ransomware
   a. IDS/IPS
   b. Antivirus/EDR
   c. Threat intelligence
   d. Deception technology

(C) Containment

1. Inventory (enumerate & assess)
2. Detect | Deny | Disrupt | Degrade | Deceive | Destroy
3. Observe -> Orient -> Decide -> Act
4. Locate and isolate the assets responsible for encrypting files
5. Isolate impacted file sharing systems
6. Close the attack vector
7. Fortify non-impacted file sharing systems
8. Fortify non-impacted critical assets
9. Issue perimeter enforcement for known threat actor locations
10. Deploy EDR hunter/killer agents and terminate offending processes

(E) Eradication

1. Close the attack vector
2. Patch asset vulnerabilities
3. Re-image impacted assets
4. Inspect all assets for IOC consistent with the attack profile
5. Inspect user activity for IOC consistent with the attack profile
6. Inspect backups for IOC consistent with the attack profile PRIOR to systems recovery
7. Implement newly obtained threat signatures

(R) Recovery

1. Restore to the RPO within the RTO
2. Restore from known clean backups
3. Address collateral damage

(L) Lessons/Opportunities

1. Perform routine cyber hygiene due diligence
2. Engage external cybersecurity-as-a-service providers and response professionals
3. Avoid opening email and attachments from unfamiliar senders
4. Avoid opening email attachments from senders that do not normally include attachments

References:

1. MITRE ATT&CK Technique T1486: https://attack.mitre.org/techniques/T1486/
2. Paying ransoms is discouraged, but it should be a contingency available to executives (SEE Preparation #4 and #6).

Resources:

- ➔ GuardSight GSVSOC Incident Response Plan: https://github.com/guardsight/gsvsoc_cybersecurity-incident-response-plan
- ➔ IT Disaster Recovery Planning: https://www.ready.gov/it-disaster-recovery-plan
- ➔ Report Cybercrime: https://www.ic3.gov/Home/FAQ

GUARDSIGHT

Incident Response Playbook Template

Incident Type

Ransomware

Introduction

This playbook is provided as a template to customers using AWS products and who are building their incident response capability. You should customize this template to suit your particular needs, risks, available tools and work processes.

Security and Compliance is a shared responsibility between you and AWS. AWS is responsible for “Security of the Cloud”, while you are responsible for “Security in the Cloud”. For more information on the shared responsibility model, please review our documentation (https://aws.amazon.com/compliance/shared-responsibility-model/).

You are responsible for making your own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) references current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. This document is provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Summary

This Playbook

This playbook outlines response steps for handling ransomware incidents. These steps are based on the NIST Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) (Special Publication 800-61 Revision 2) that can be used to:

• Gather evidence • Contain and then eradicate the incident • recover from the incident • Conduct post-incident activities, including post-mortem and feedback processes

Interested readers may also refer to the AWS Security Incident Response Guide (https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/welcome.html) which contains additional resources.

Once you have customized this playbook to meet your needs, it is important that you test the playbook (e.g., Game Days) and any automation (functional tests), update as necessary to achieve the desired results, and then publish to your knowledge management system and train all responders.

Note that some of the incident response steps noted below may incur costs in your AWS account(s) for services used in either preparing for, or responding to incidents. Customizing this playbook and testing it will help you to determine if additional costs will be incurred. You can use AWS Cost Explorer (https://aws.amazon.com/aws-cost-management/aws-cost-explorer/) and look at costs incurred over a particular time frame (such as when running Game Days) to establish what the possible impact might be.

In reviewing this playbook, you will find steps that involve processes that you may not have in place today. Proactively preparing for incidents means you need the right resource configurations, tools and services in place that allow you to respond to an incident.

The next section will provide a summary of this incident type, and then cover the five steps (parts 1 - 5) for handling ransomware incidents.

This Incident Type

Ransomware is malicious code designed by threat actors to gain unauthorized access to systems and data and to encrypt the data to block access by legitimate users. Once ransomware has locked users out of their systems and/or encrypted their sensitive data, the actors demand a ransom. In theory, if the ransom is paid, access to the data is returned (such as by providing an encryption key), but equally, some studies have suggested the victim will subsequently be attacked again. Alternatively, if not paid, the organization risks permanent data loss and/or data leaks to the public, competitors or other malicious actors.

There are usually limited options to mitigate a successful ransomware attack once it has occurred. The best mitigation is to reduce the chance that it can happen in the first place. The AWS Well-Architected security pillar provides a framework to implement AWS best practice, including operating workloads security (security foundations section), protecting compute resources (infrastructure protection section) and others. The security pillar encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security. This playbook covers steps that can be used to deal with ransomware.

Incident Response Process

Part 1: Acquire, Preserve, Document Evidence

1. You become aware that a possible ransomware incident has occurred. This information could come via different means, depending on your configurations in your AWS environment:

2. A colleague reports that an EC2 instance cannot be accessed by SSH or similar, however the instance appears to be correctly configured with appropriate network access in place, and there are no related service issues reported by AWS in the Service Health Dashboard

3. Your ticketing system creates a ticket for unusual metrics or logs from the EC2 instance
4. The instance is reporting network reachability issues in the AWS console, or via Amazon CloudWatch alarms
5. Message from threat actor through alternate communication channel such as email about the ransom demand
6. Findings through services like AWS Security Hub or Amazon GuardDuty.
7. Other alarms or metrics you have configured in your monitoring systems, either internal or external to AWS
8. Once you confirm that an event is a security incident, it is important to determine the scope of impact (quantity of resources as well as sensitivity of data).
9. Determine if there are any known events that could be causing service disruption, or impacting instance metrics (e.g., network CloudWatch metrics increasing due to a sales event, or similar)
10. Use Amazon Detective to investigate any ongoing activity using the time based analysis or a specific period when the incident was identified to identify any deviations from a “normal” operating baseline.
11. Obtain the application’s documented baseline and locate the metrics for standard application performance from the CloudWatch or other application performances monitoring tool used in the organization to compare baseline behavior to anomalous behavior as a result of the incident.
12. Determine the classification level of any data that resides in the EC2 instance, S3 bucket, Amazon Workspaces instance, etc.
13. Confirm a ticket/case has been raised for the incident. If not, manually raise one.
14. If you received an abuse notification from AWS, determine if any cases are already open for the resource that can be correlated to the abuse notification. This may provide indications relating to prior unauthorized activity.
15. If there is a ticket/case already opened, determine what internal alarms/metrics are currently indicating an issue (if automated, what caused the ticket to be created?) If the ticket/case creation was not initiated automatically by an alarm or metric, document the alert/notification that led to identification of the issue if there was one (for example, a ransom demand popping up on the screen, or metrics that indicate the device is no longer on the network). If the incident was identified by an indicator that does not conclusively identify a ransomware incident as the cause, then verify the service disruption is not due to any planned (or other) event and document the actual vector.
16. Identifying the ransomware strain is key to recovery. For example, if objects in S3 buckets are inaccessible with an error of not having encryption key access, the first step would be to review the S3 object properties section to understand the encryption key applied. A similar approach can be leveraged with the Amazon Elastic Block Store (EBS)volumes in situations involving crypto ransomware.
17. Using your preferred monitoring tool, access AWS CloudTrail and search for any API actions which indicates any credential compromise attack vector and refer to the playbook, “Credential Leakage/Compromise”.
18. Determine when the infection occurred using log search. CloudWatch can help you to review logs such as application logs, operating system logs, database logs, etc.

19. Determine the business impact:

a. Identify application(s) impacted; this may be achieved via Resource Tags, or by an internal Configuration Management Database (CMDB)
b. Identify business owner and workload classification (example: mission critical, high risk, etc.)

12. Determine and begin to document end-user impact/experience of the issue. This should be documented in the ticket/case related to the incident. If there are impacted users, determine from them the steps that led to the incident. This will assist you to establish the attack vector used to execute the ransomware. Mitigations against this vector should be placed in later steps of this process.
13. Internal Communications:

a. Identify stakeholder roles from your organization's incident response plan, the application entry in the Configuration Management Database CMDB (if one exists), or via the application's risk register
b. Open an Incident Response bridge to have a regular communication channel about the incident.
c. Notify identified stakeholders including (if required) legal personnel, technical teams and developers and add them to the ticket and the war room, so they are updated as the ticket is updated

14. External Communications:

i. Ensure your organization's legal counsel is informed and is included in status updates to internal stakeholders and especially in regards to external communications.

ii. For colleagues in the organization that are responsible for providing public/external communication statements, ensure these internal stakeholders are added to the ticket so they receive regular status updates regarding the incident and can complete their own requirements for communications within and external to the business.
iii. If there are regulations in your jurisdiction requiring reporting of such incidents, ensure the people in your organization responsible for notifying local or federal law enforcement agencies are also notified of the event. Consult your legal advisor and/or law enforcement for guidance on collecting and preserving the evidence and the chain of custody.
iv. There may not be regulations, but either open databases, government agencies or NGOs may track this type of activity. Your reporting may assist others

Part 2: Contain the Incident

Early detection of anomalous user behavior or network activity is key to reducing the impact of ransomware incidents. The below steps can be taken to help to contain the incident. If applicable, work with the legal and compliance team of your organization on any required response and continue the incident response process outlined here.

1. If possible, determine the type of ransomware used in the incident:

a. Crypto Ransomware - Objects/files will be encrypted
b. Locker ransomware - Locks out access to the device
c. A different type, or previously not observed type

2. For identified AWS resources associated with your impacted workloads, isolate network or internet connectivity by modifying Security groups, S3 bucket Policies or relevant identity and access management policies as applicable to minimize opportunities for the infection to be spread, or for threat actors to have access to those resources.

Keep in mind that sometimes modifying security groups may not have the intended impact, due to connection tracking.

3. Determine whether the EC2 instance actually needs to be recovered, or not. For example, if the impacted instance is part of an AWS Application Auto Scaling group, removing the instance from the group will trigger a scaling action. If the incident is linked to a vulnerable package on the host's operating system, updating the AMI used in the Launch configuration and confirming the vulnerability has been patched (check the Mitre CVE database) will also be required.
4. Check your CloudTrail log for unauthorized activity such as creation of unauthorized IAM users, policies, roles or temporary security credentials. Delete any unauthorized IAM users, roles, and policies, and revoke any temporary credentials.
5. If you're dealing with this incident as part of a broader security incident in the account, a drastic approach could be to use AWS Organizations Service Control Policies (SCPs) to restrict any API call to be made from that AWS account (assuming it is not the master account of the Organization). Please note this may impact other running workloads as SCPs applied at the account level will be enforced on all the IAM entities associated in it. This may prevent malicious actors from inflicting further damage on the account's resources and data.
6. If the attack vector was made possible by un-patched software, operating system updates, out-of-date malware/anti-virus tools, ensure that all EC2 instances are either updated to the latest version of operating system, all software packages and patches are up-to-date and virus signatures and definition files on all EC2 instances are up-to-date. This may be done by several methods:

a. Patch-in-place for mutable architectures
b. Re-deploy for immutable architectures

7. Depending on what occurred in Step 6 above, remove any remaining resources that are identified as being at risk of infection (that may have accessed the same vector that downloaded the ransomware, whether that be via email, visiting an infected website, or something else). If it is part of a larger fleet managed by Auto Scaling, containment efforts may be better focused on establishing the attack vector and then placing mitigations that will prevent other resources in the fleet from becoming infected via the same vector.

Part 3: Eradicate the Incident

1. It is important to understand if the impact from the incident is contained to a subset of the environment. If there is an ability to restore the ransomed data from backups/snapshots, you can refer to the recover from the incident section. Note that there may still be value in exploring the incident under an isolated environment to run the root cause analysis and use controls to avoid situation in the future.
2. Investigate potential use of up-to-date antivirus or anti-malware software to clean the ransomware. Refer to this step with caution as it may alert the actor (see earlier steps to remove network access from the impacted EC2 instance). You can review the locked/encrypted objects in an isolated forensic environment.
3. Review any GuardDuty findings if there are any high or medium severity alerts that can help to reduce the additional effort required to search application level logs. GuardDuty findings provide recommendations on how to remediate the finding.
4. Remove any malware that was identified during the forensic analysis and identify Indicators of Compromise.
5. If the ransomware strain has been identified, determine if any 3rd party decryption tools are available, or if any other online resources may help

Part 4: Recover from the Incident

1. Identify the restore point for any restore operation performed from backup.
2. Review the backup strategy and see if you can recover all the objects and files. This will depend on the lifecycle policies applied on the resources.
3. Restore the data from your backup, or revert to an earlier snapshot of the EC2 instance's volumes. Apply forensic methods to confirm that data is clean before restoring it. Ensure any spread vectors are identified & resolved.
4. Alternatively, if you have been successful in using any open source de-crypter tool to retrieve the data, remove that data from the instance and perform any required analysis to ensure the data is clean. Then, recover the instance, terminate it or quarantine it and create a new one, and restore the data to a new instance.
5. If restoring from a backup and de-crypting the data is not an option, consider whether to start from entirely new environment is a possibility .

Part 5: Post-Incident Activity

1. Documenting and cycling lessons learned during simulations and live incidents back into "new normal" processes and procedures allows organizations to better understand how an incident occurred with their configurations and processes – such as where they were vulnerable, where automation may have failed, or where visibility was lacking – and the opportunity to strengthen their overall security posture.
2. If you identified the initial attack vector or point of entry, determine how best to mitigate the risk of a re-occurrence. For example, if the malware gained initial entry due to an un-patched public-facing EC2 instance, and assuming you applied the missing patch to all current instances, how can you improve your patching process to ensure that patches are tested and applied sooner and with more consistency and reliability?
3. If you've developed set technical steps to take for a given threat, assess opportunities to automate those actions upon detection to mitigate the threat as quickly as possible to minimize scope and severity of impact.
4. Ensure you collect lessons learned from all stakeholders and update your incident response plan, disaster recovery plans, and this playbook as necessary. And where appropriate, consider priorities and funding for new technical capabilities and personnel skills to fill any gaps.

Appendix A

Preparation

As with other incident response scenarios, mitigating ransomware threats requires a strong preventative strategy and preparation is very important. More so than others though, mitigation techniques rely on adequate preparation prior to a ransomware incident. Implementing best practices based on the AWS Well-Architected Framework will help you in your preparation. If key preventative measures are not already in place, these must be considered as part of any post-incident activity including any tools or techniques that failed during the incident response process itself, such as automation, integration with partner offerings, application and systems observability, etc. The below points cover some key preparation steps.

1. Adopt foundational best practices: Leverage AWS Cloud Adoption Framework (CAF) and AWS Well-Architected best practices to your organization's cybersecurity framework such as the NIST CyberSecurity Framework for

AWS, a framework focused on security outcomes organized around five functions (Identify, Protect, Detect, Respond, Recover) and foundational activities that map to existing standards, accreditations and frameworks.

2. Training: Cybersecurity awareness training for your employees. Social engineering is one of the common methods used to induce end users to download an infected file.
3. Deep dive on assets and configurations: Identifying your IT assets is a vital component of governance and security. You must have visibility into all your data storage services and resources in order to evaluate their security posture and effectively configure them. Reduce potential attack surface, for instance, by analysing your public data footprint. If you use Amazon Simple Storage Service (S3), ensure that your S3 buckets use the correct policies and are not publicly accessible. Implement the idea of least privilege enterprise-wide. With S3 Versioning, existing versions of your data are immutable: actors cannot change existing objects, and any modification is going to result in a new version. Use MFA delete to require a second element of authentication for S3 data deletion. In addition, S3 includes a number of security controls to consider when developing and implementing your own security policies; for more information, please see security best practices for Amazon S3 (https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html).
4. Stay up-to-date with system patches: Ransomware often relies on exploit kits to gain access to a system or network using known threats. Amazon Elastic Compute Cloud (Amazon EC2) resources can use AWS Systems Manager to automatically collect software inventory, apply OS patches, create system images, and configure Windows and Linux operating systems. These capabilities enable automated configuration and ongoing management of systems at scale, and help maintain software compliance for instances running in EC2.
5. Continuous monitoring:

a. Use Amazon Inspector to assess your deployed EC2 instances for CVEs and deviation from best practice. Build a CI/CD pipeline to remediate security findings automatically & periodically. Amazon Inspector finds applications by querying the package manager or software installation system on the operating system where the agent is installed. This means that software that was installed through the package manager is assessed for vulnerabilities. You can also leverage AWS Security Competency Partner offerings to help inspect your application deployments for security risks and vulnerabilities, while providing priorities and advice to assist with remediation.
b. AWS developed a new open source Self-Service Security Assessment tool (with ransomware analysis modules) that provides customers with a point-in-time assessment to quickly gain valuable insights into the security posture of their AWS account. For continuous monitoring of your security posture, AWS recommends enabling AWS Security Hub's Foundational Security Best Practices standard, which also provides automated security checks.

6. Data back-up: Create secure backups of your data on a regular basis. AWS Backup is a fully managed backup service that makes it easy to centralize and automate the backup of data across AWS services. If backups are not a requirement, ensure that there are regular snapshots or an up-to-date AMI that can be used either for recovery or replacement of the impacted EC2 instance. Amazon S3 and Amazon Glacier are durable, low-cost storage platforms. Both offer unlimited capacity and require no volume or media management as backup data sets grow. Backup and Recovery Approaches Using AWS.
7. Testing: Implement, review and test disaster recovery scenarios for your organizational needs. This will help you determine the path for implementing recovery mechanisms and mitigate risks. Disaster recovery is about preparing for and recovering from an event that has a negative impact on your business goals. You can use CloudEndure Disaster Recovery to quickly recover your environment, minimizing data loss and downtime in the case of a ransomware incident.

8. Automation: Where you identify fixed technical procedures that don’t deviate or require a human to make a decision, explore the opportunity to automate protections and response actions to mitigate the threat as quickly as possible to minimize scope and severity of impact. Communication channels: Identify communication channels such as an Incident Response bridge that you will need to use during the incident to communicate with the internal and external stakeholders.

Incident response plan

2022-04-26

This Incident Response Plan (IRP) has been prepared to support the Digital Transformation Agency (DTA) CloudSystem. The document provides guidance for responding to cyber security incidents that may occur in relation to an Agency's operation of the CloudSystem.

Purpose

The purpose of this IRP is to provide guidance to Agencies operating the CloudSystem including how to detect cyber security incidents, how to respond and remediate them, along with how to reduce the risk of an incident re-occurring in the future.

Scope

The scope of this IRP is specific to the use of Microsoft 365 services as part of the CloudSystem. As such it is termed a system-specific IRP and is designed to be subordinate to an Agency's overarching IRP. As a result, this IRP does not directly address topics that it is reasonable to assume are discussed in an Agency-level IRP.

The CloudSystem IRP is a living document. It is anticipated that, over time, amendments and updates will be applied to the CloudSystem IRP specific to agency business needs and lessons learnt from cyber incidents.

Incident response plan

This IRP is based on the four step National Institute of Standards and Technology (NIST) incident response life cycle as documented in Special Publication 800-61 Revision 2. The four steps of the process are illustrated in Figure 1 and are:

- Preparation
- Detection & Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity.

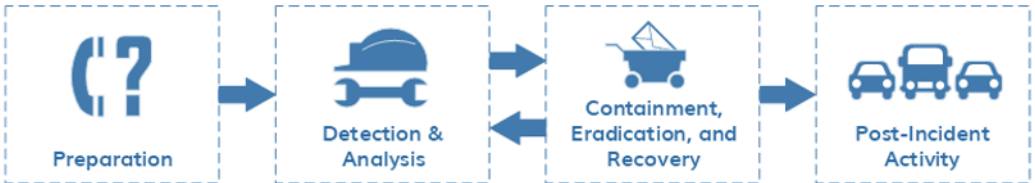


Figure 1 Incident Response Process

Each of the four incident response phases are detailed in the following sections of this document.

Preparation

The preparation phase of the incident response life cycle is a shared responsibility between the project team and Agency cyber security personnel. The project team is responsible for the design, implementation, and security assessment of the solution. This includes performing a risk assessment and determining which specific Information Security Manual (ISM) controls to implement to reduce and manage the risk of security incidents. The following documentation has been produced for the CloudSystem and it is

recommended that the Agencies cyber security personnel familiarise themselves with the content to aid them in their preparation to manage an incident:

- DTA – Blueprint – Solution Overview which describes the solution, which features have been enabled/disabled for the Agency, and how the solution has been structured.
- DTA – Blueprint – Platform Design which describes the technologies used that make up the 'platform' portion of the solution and how they are implemented.
- DTA – Blueprint – Client Devices Design which describes the technologies used that make up the Windows 10 portion of the solution and how it is implemented.
- DTA – Blueprint – Office 365 Design which describes the technologies used that make up the Office 365 portion of the solution and how it is implemented.
- DTA – Cloud-Only Blueprint – Security Risk Management Plan (SRMP) which includes the details of the risk assessment performed and the recommended treatments.
- DTA – Cloud-Only Blueprint – System Security Plan (SSP) which describes how controls identified in the SSP Annex are implemented by the system.
- DTA – Cloud-Only Blueprint – System Security Plan Annex (September 2021) which states the compliance of the solution with the September 2021 version of the ISM.
- DTA – Cloud-Only Blueprint – Security Standard Operating Procedures which describe the steps required to perform multiple operational tasks within the environment.

In addition to having ongoing access to the above documentation it is assumed that Agency cyber security personnel have access to tools and resources as described in the Agency IRP.

Specific resources that are also required by Agency cyber security personnel to detect and respond to security incidents include:

- Access to the various Microsoft management portal required to administer the CloudSystem, as listed below in Table 1
- Membership of the role(s) required to perform any actions related to the incident

Table 1 Microsoft Management Portals

Portal	URL
Microsoft 365 Defender portal	https://security.microsoft.com
Defender for Cloud Apps portal	https://portal.cloudappsecurity.com
Azure portal (including Azure AD)	https://portal.azure.com
Microsoft 365 compliance portal	https://compliance.microsoft.com
Microsoft 365 admin center	https://admin.microsoft.com/

Detection and analysis

Multiple detection methods are available to the Agency's cyber security personnel to aid them in discovering and categorising security incidents. These detection methods include:

- Alerts from Azure AD (including Azure AD Identity Protection) including risky sign-ins and users flagged for risk.
- Azure AD logs stored in Azure and available via the portal, including the audit log for all administrative activities relating to Azure AD.
- Defender for Office 365 alerts and reports for each of the configured capabilities including Safe Attachments, Safe Links, Safe Attachments for SharePoint, OneDrive and Microsoft Teams, and Anti-phishing in Defender for Office 365 protection.
- Microsoft Defender for Endpoint including the Security Operations, Incidents, and Alerts Queue dashboards which provide tailored information and actions for cyber security personnel.
- Microsoft Defender for Cloud Apps Threat Detection, Privileged Accounts, and Access Control dashboards spanning the whole Microsoft 365 deployment, along with configurable email alerts and automatic response capabilities.
- Local Windows 10 events logs written to each Windows 10 endpoint including authentication attempts, firewall activities, and Windows Defender Application Control (WDAC) events.

Due to its containment, eradication and recovery capabilities in addition to its detection and analysis functionality, Microsoft Defender for Endpoint is the primarily incident response tool for the CloudSystem and is described in further detail in the section below.

Microsoft Defender for Endpoint

The CloudSystem leverages Microsoft Defender for Endpoint to monitor, detect, investigate, and respond to threats targeting Windows 10 endpoints. When an alert is triggered of sufficient severity, an email is automatically sent to a specified recipient email address (typically the Agency cyber security team mailbox or similar). Additional email recipients can be configured as required.

Recommendation Agency should ensure a recipient email address (typically the Agency cyber security team mailbox or similar) shared with multiple users is created and monitored.

The majority of alerts generated within the Microsoft 365 Defender portal – which include Microsoft Defender for Endpoint alerts – relate to automatically detected issues and are informational in nature. This means that they are not necessarily harmful to the system but must be reviewed and accounted for. Alerts are organised by severity as they enter the 'Alerts queue', the severity of which is detailed below in Table 2.

Table 2 Microsoft 365 Defender Alert Severities

Severity	Description
High	Threats marked as 'High' have the potential to cause severe damage to the system and devices using it. These alerts must be treated with urgency.
Medium	Threats marked as 'Medium' must be treated with some importance but typically will indicate anomalous behaviour within the environment such as the execution of suspicious files, un-sanctioned registry changes, or observed behaviours typical of a cyber threat or attack.
Low	'Low' urgency threats will typically be identified as commercial/known malware or hacking tools, their function is generally well understood and the ability to stop it is high.
Informational	'Informational' alerts are those that might not be considered harmful to the network but are good to track.

Figure 2 shows an example of an alert from Defender for Endpoint which detected a suspicious sequence of activities and automatically generated an incident detailing the severity, timestamps, devices affected, applications called, and more.

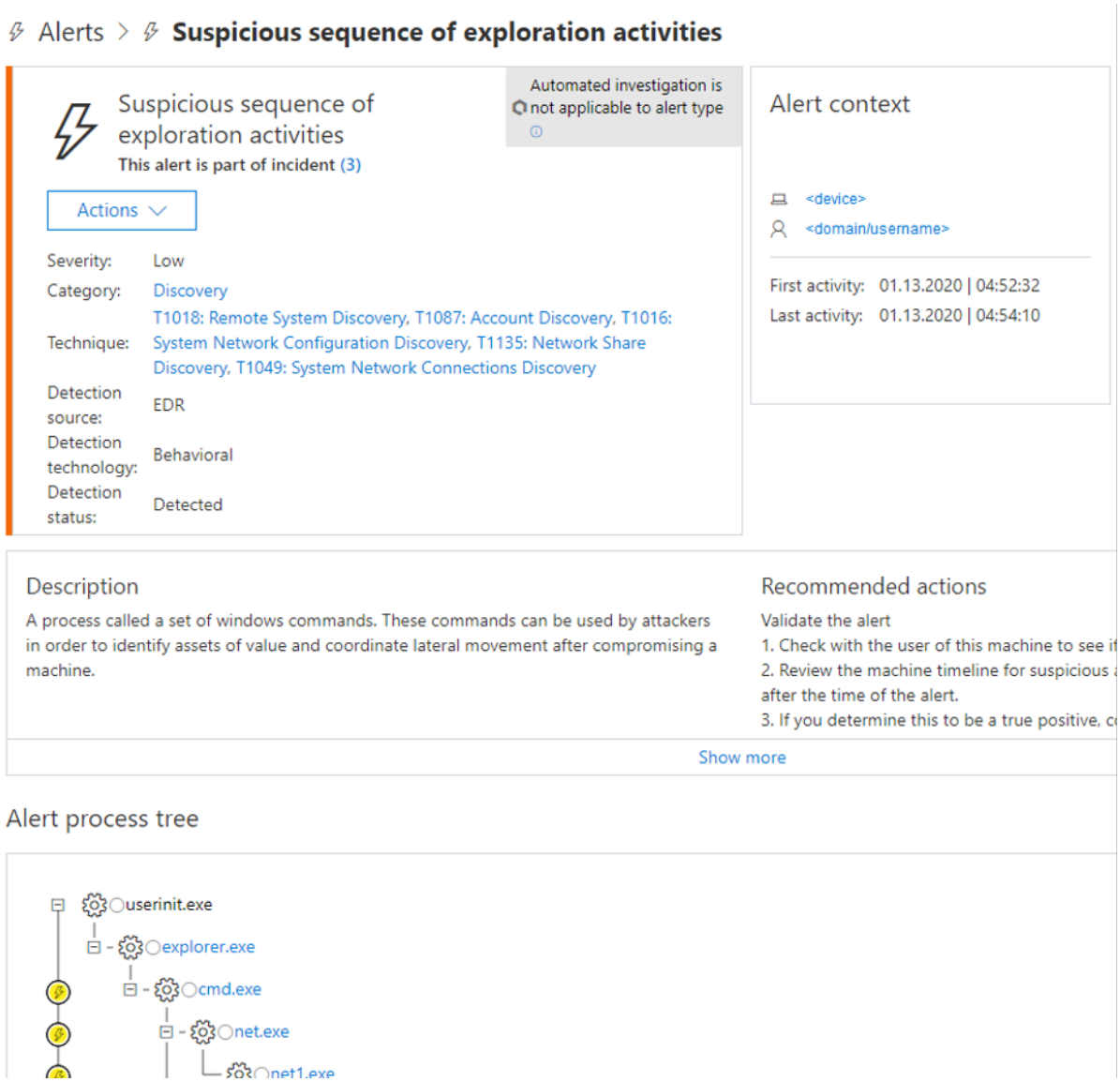


Figure 2 Suspicious sequence of activities

When the Agency's cyber security personnel receive an alert, they should perform analysis to determine the cause and any potential impact, including recommended actions within the Microsoft 365 Defender portal. If an alert occurs during an approved change window and relates directly to the contents of the change, for example an unapproved/not allowed executable runs during an application deployment, then it is unlikely that a security incident has occurred. However, if an alert is triggered outside of a change window and without an obvious cause then the probability of the event being a security incident probable.

Note, Microsoft assign a criticality to each alert based on an internal rating system. It is up to the Agency's cyber security team to make their own assessment of the criticality of all potential security incidents in accordance with the Agency's overarching IRP.

The assignment of criticality to an incident is an important step and due care must be applied to avoid the risks associated with both under and over classifying an incident. If there is ever any doubt, cyber security personnel should always investigate further.

The alerts captured in the Microsoft 365 Defender portal should be leveraged by Agency cyber security personnel to detect and analyse potential security incidents. The Microsoft 365 Defender portal provides far deeper detail than is available from the email alerts, these emails should only serve as a cursory notification, not an in-depth analysis of the incident.

Within the Microsoft 365 Defender portal there are two capabilities that should be utilised by Agency

cyber security personnel for the purpose of detection and analysis of incidents on a day-to-day basis.

- Incidents lists all automatically generated incidents detected by Defender for Endpoint - along with Defender for Office 365 and Defender for Cloud Apps, including the severity of the incident, the machines and users involved, last activity, assignment of the incident, et cetera. All incidents should be assigned as they are generated and managed based on the Agency's operating procedures by cyber security personnel.
- Alerts queue lists all alerts based on the alert type not the incident case that is generated, this can be supremely helpful when attempting to identify patterns of behaviour. This alerts queue will also sort by severity, which incident it is related to, status, and investigation state.

For both the Incidents and Alerts queue Agency cyber security personnel can select individual records to access detailed information on the specific activity.

Incident criticality assignment Regardless of the detection source for a potential incident, all incidents should be assigned a criticality in a consistent manner. In accordance with guidance issued by the Agency's Chief Information Security Officer (CISO) or other personnel responsible for the daily operational information security of the Agency, all incidents should be assigned a system specific criticality. The criticality ratings for incidents have been developed from a number of Federal Government Agencies' overarching risk frameworks, specifically the consequence definitions. These definitions are listed below.

Note, if incident criticality definitions are included in the Agency IRP cyber security personnel should use those in preference to the criticalities defined below. The Business Impact Levels (BILs) defined in the Protective Security Policy Framework (PSPF) should also be considered in the assessment of incident criticalities.

Table 3 Incident Criticality Definitions

Incident Criticality	Performance Metrics	Reputational Metrics
Extreme	Major impact on departmental outcomes and performanceRequires major additional management effort by Senior Executive to control the impactUnavailability of agency mission critical systems including the delivery of Government outcomes (e.g. a public facing system that is used in emergency procedures, a grants systemCatastrophic breach and or loss and or destruction of agency information containing sensitive and personal information of Australian citizens and or classified information	Significant adverse publicityLoss of stakeholder confidence requiring intervention by SecretaryReporting to accountable authorities outside of the Agency e.g. Privacy Commissioner, Minister of Department etc
High	Moderate impact on achievement of outcomes and performanceRequires additional management effort by business area, Senior Executive to control the impact	Substantial adverse publicityLoss of stakeholder confidence requiring intervention at Executive level
Medium	Minor impact on achievement of outcomes and performanceRequires additional management effort within the business area to control the impact	Some adverse publicityMinor loss of stakeholder confidence

Incident Criticality	Performance Metrics	Reputational Metrics
Low	Insignificant impact on achievement of outcomes and performance	Some adverse publicityMinor loss of stakeholder confidence

Agency cyber security personnel should use the above table to define the criticality of incidents based on the data available to them at the time of detection and analysis. If this data is updated or found to be inaccurate Agency cyber security personnel should re-assess the criticality of the related incident(s). The criticality of an incident should be used to determine the resources, timeframes and reporting requirements related to it.

Azure service outages An additional data source that can be leveraged by Agency cyber security personnel when analysing potential security incidents is the Azure status dashboard. This dashboard is published by Microsoft and reports on the current status of all Azure-based services, including any current warnings or errors. An example of the dashboard is shown below in Figure 3.

The Azure status dashboard is available at https://status.azure.com/ and does not require the user to be logged into Azure to view the current status.

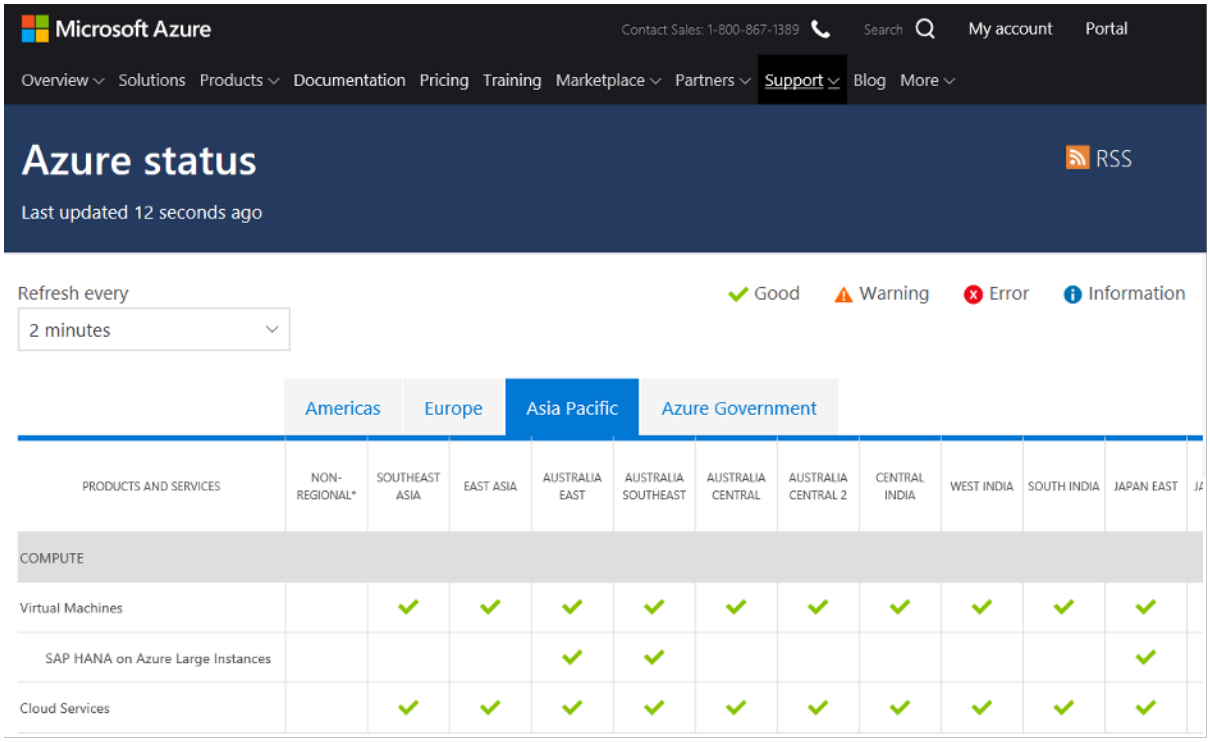


Figure 3 Azure Status Dashboard

Agency cyber security personnel can use the dashboard to determine if a potential incident is local to the Agency's system or is a widespread issue affecting the underlying Azure service(s).

Recommendation It is recommended that at least one Agency cyber security personnel member is subscribed to the provided Rich Site Summary (RSS) feed to receive updates whenever an Agency-leveraged service is affected.

Microsoft 365 service outages Agency cyber security personnel should review the Microsoft 365 service status (including all Office 365 services) when investigating an incident relating to availability. The following resources are available from Microsoft to identify the status of Microsoft 365 services:

- Microsoft 365 Service health status
- Microsoft 365 Status Twitter

In the first instance the Microsoft 365 Service health status page should be consulted, followed by the Microsoft 365 Status Twitter account. If no issues are identified by either of these resources, then Agency-specific scenarios should be explored such as loss of Internet connect, Local Area Network (LAN) outage, etc.

As an example of how to navigate the Microsoft 365 Service health status page, please refer to Figure 4 below.

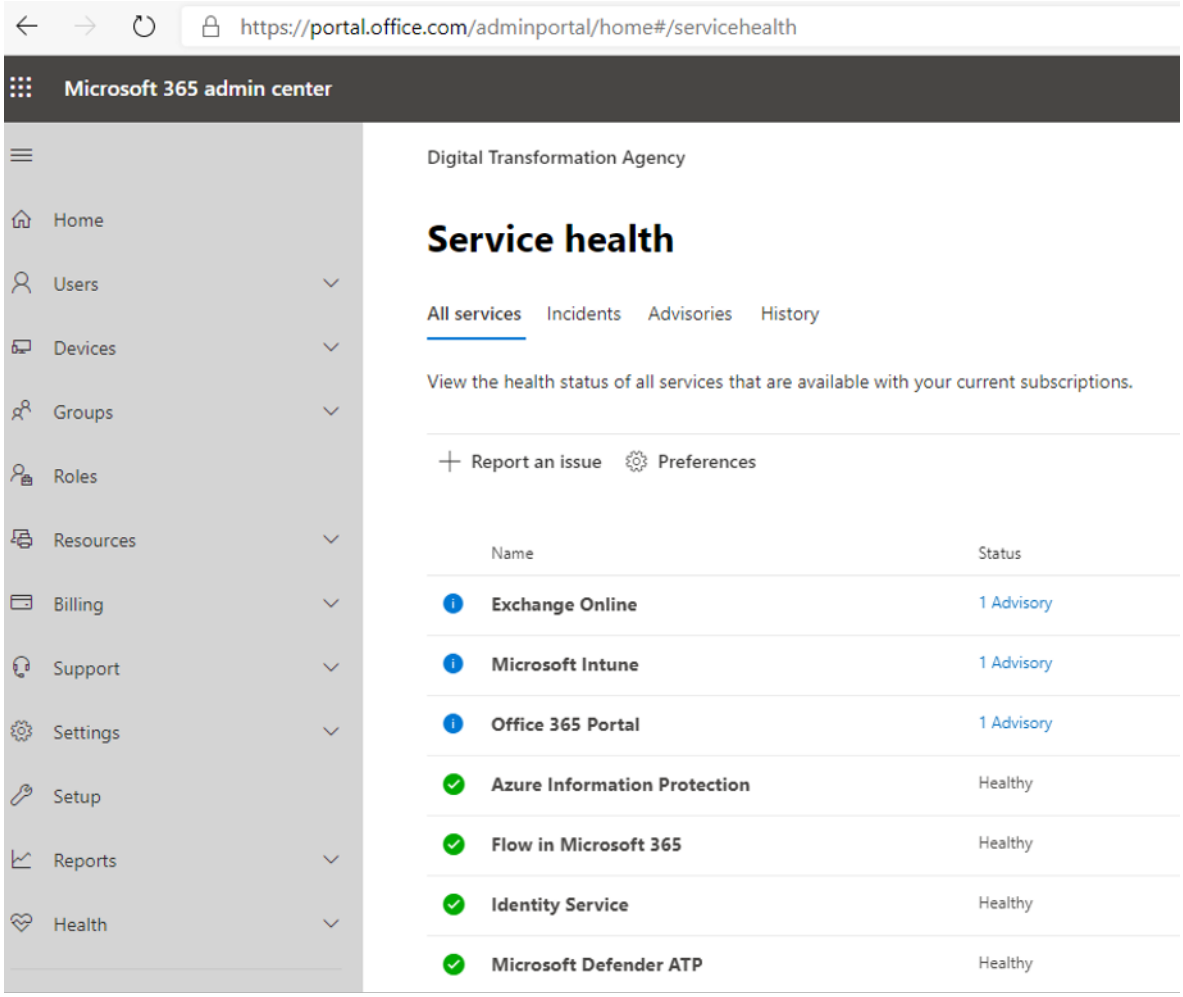


Figure 4 Office 365 Service Outages

Agency cyber security personnel can use the dashboard to determine if a service is down, whether the issue is widespread and affecting the underlying services, or whether there is no identified outage. This page can also be used to review ongoing service advisories such as those identified below in Figure 5.

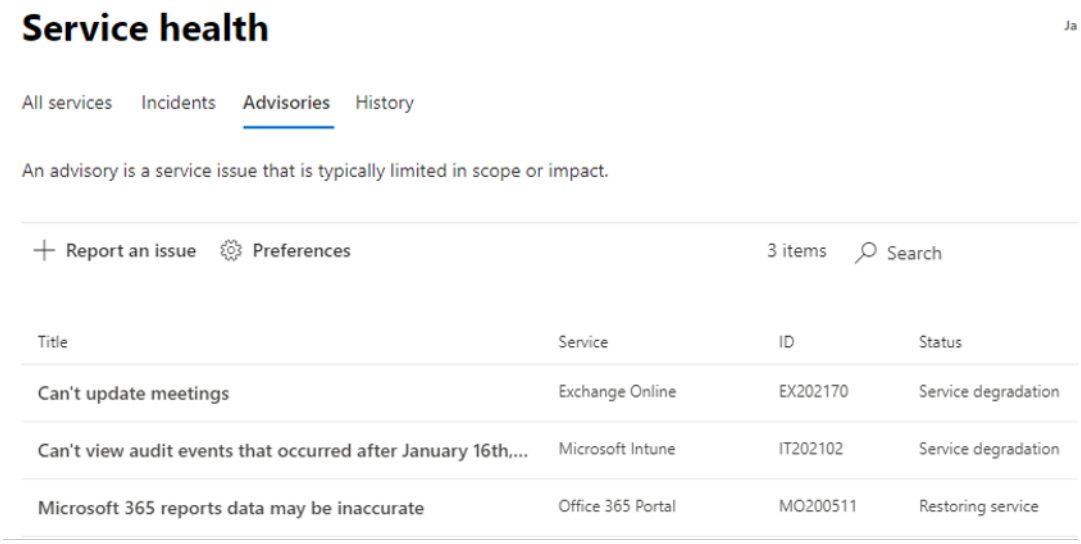


Figure 5 Office 365 Service Health Advisories

Recommendation It is recommended that at least one Agency cyber security team member, or another person assigned with cyber security responsibilities, review these services daily to ensure there are no ongoing service outages that will affect the availability.

Containment, eradication, and recovery

The Agencies cyber security teams' approach to containment, eradication, and recovery – particularly in relation to resource allocation and priority – should be based on the category of the incident as previously described. However, regardless of the criticality of an incident the basic actions that are required to address the incident are dependent on the specific incident type.

This IRP defines specific incident types that are directly related to the solution, namely:

- Violation of confidentiality of Agency data stored in Office 365 (including Exchange Online)
- Violation of integrity and/or confidentiality of Azure AD accounts
- Violation of integrity of Azure AD configuration
- Violation of integrity of Office 365 configuration
- Loss of availability of Agency data stored in Office 365

The following table provides recommendations for the containment, eradication, and recovery activities associated with the above incident types:

Table 4 Incident Containment, Eradication, and Recovery Activities

Incident type	Containment, Eradication, and Recovery Activities
Violation of confidentiality of Agency data stored in Office 365(For example, sensitive information is sent outside the organisational boundaries – data spill)	**Containment** – Data Loss Prevention (DLP) policies are in place across Microsoft Teams, Exchange Online, SharePoint Online, and Outlook. All data stored in these corporate data locations is backed by policies to block the egress of what is identified as 'sensitive'. Note, if DLP policies have been disabled or modified they should be re-enabled and verified by referring to the relevant ABAC.**Eradication** – DLP policies automatically block messages from being sent or redacts and obfuscates data attempting to leave organisational boundaries.**Recovery** – Recovery of sensitive information is automated by DLP. User notifications are linked to DLP policies upon creation. The Agency cyber security team should review DLP policies often to ensure they align with business needs. New policies should be created based on commonly used applications within the organisation.
Violation of integrity and/or confidentiality of Azure AD account(s)(For example, user or administrative account compromised)	**Containment** – Compromised account credentials can result in catastrophic damage to the system if the account in question has administrative privileges, and breaches of sensitive data. To contain this, Conditional Access and Multi-Factor Authentication (MFA) are employed to control access to all accounts, even if account credentials are compromised. Agency cyber security personnel can perform a global account sign-out and password reset if an account is suspected of being compromised.**Eradication** – Compromised accounts can be disabled from log-ins, passwords reset, and global sign-outs initiated. Agency cyber security personnel should review Azure AD logs to identify the source of the breach from an identity perspective. They should also review sharing audit logs against SharePoint Online and OneDrive for Business prior to the user being given their account credentials back. Additionally, a full audit of the user's log-in habits should be performed to ensure they comply with Agency security requirements.**Recovery** – Once the incident has been remediated the users account should be re-enabled, password reset, and access granted. Simultaneous to this, the Agency cyber security team are to review all appropriate logs dependant on the breach.

Incident type	Containment, Eradication, and Recovery Activities
Violation of integrity of Azure AD configuration(For example, unapproved changes are made to Conditional Access policies)	**Containment** – Unauthorised changes to Conditional Access policies can result in gaps within the approved authentication process. To prevent these changes Privileged Identity Management should be utilised to only grant temporary permissions to perform privileged tasks.**Eradication** – Agency cyber security personnel should revert any changes made to the configuration in alignment with the configuration outlined in the 'DTA – Platform – Detailed Design' and 'DTA – Conditional Access – ABAC' documents.**Recovery** – Ensure all changes have been reverted, to ensure this has been completed successfully refer to the design and ABAC documents. Once the change(s) have been reverted any further authentication attempts will need to pass the conditional access policies. Measures should be in place to record any security incidents and unexpected changes to the configuration due to lack of knowledge.
Violation of integrity of Office 365 configuration(For example, DLP or retention policies are disabled or modified without authorisation)	**Containment** – DLP and retention policies are in place to ensure sensitive data does not improperly leave organisational boundaries. DLP is controlled by Azure AD permissions, as such, all access to it should be controlled by Privileged Identity Management (PIM). In the event of an incident PIM can be used to restrict administrative privileges to prevent further changes and provide an audit log of previous actions.**Eradication** – Agency cyber security personnel should revert any changes made to the configuration in alignment with the configuration in the 'DTA – Office 365 – Detailed Design' document. The Azure AD and PIM logs should be scrutinised to review by whom the unapproved change was made.**Recovery** – Ensure all changes have been reverted, to ensure this has been completed successfully refer to the design and ABAC documents. Agency cyber security personnel should review the last modified time of the affected policy and align it with PIM logs. A review of all privileged users and groups is recommended.

Incident type	Containment, Eradication, and Recovery Activities
Loss of availability of Agency data stored in Office 365(For example, the Microsoft Teams service is unavailable, and critical corporate data cannot be accessed)	**Containment** – Service availability within the Office 365 and Azure environments is very high, if however, a service is offline or otherwise inaccessible, the Agency cyber security team should ensure the status of the service via the Microsoft 365 Service Health Status portal (see: Microsoft 365 Service Outages). If Microsoft Teams is inaccessible, secondary pathways to the data should be explored, for example, accessing the Teams back-end SharePoint Online site.**Eradication** – Not applicable for availability incidents.**Recovery** – The service is controlled by Microsoft and its availability is backed by Microsoft service level agreements.

Note, the activities listed above are designed to aid Agency cyber security personnel in responding to the specific incident types defined. However, this is not an exhaustive list of all possible responses. Agency cyber security personnel should use their judgement to determine if they are appropriate to a specific incident or if other actions should be taken.

Defender for Endpoint threat remediation Defender for Endpoint provides the ability to automate responses to detected threats, reducing the total response time for an incident and eliminating the need for manual actions to be taken by the Agency's cyber security team. Five levels of automation are available as listed below:

- No automated response – automated investigations are not run, and all activities must be performed by the Agency's cyber security team.
- Semi (any folder) – approval is required from the cyber security team for all remediation activities suggested as part of an automated investigation.
- Semi (non-temp folders) – remediation occurs automatically for temporary folders including users' download folders, remediation for other locations requires approval.
- Semi (core folders) – remediation occurs automatically for all folders other than operating system directories (e.g. Program Files and Window).
- Full – all remediation activities are performed automatically.

The CloudSystem uses the default Defender for Endpoint configuration for automated investigations, namely Full automation. Therefore, Agency cyber security personnel will not be prompted to approve remediation activities that are recommended as part of Defender for Endpoint automated investigations. The automation level can be adjusted if required based on the specific requirements of the Agency's cyber security personnel.

Note, prior to early 2021, the default configuration was Semi (any folder).

Automated remediation notification Depending on the nature of the initial alert, if Microsoft Defender for Endpoint detects a threat and it is resolved automatically it will notify administrators by sending a follow up email. An example of an alert resolution email is shown below in Figure 6.

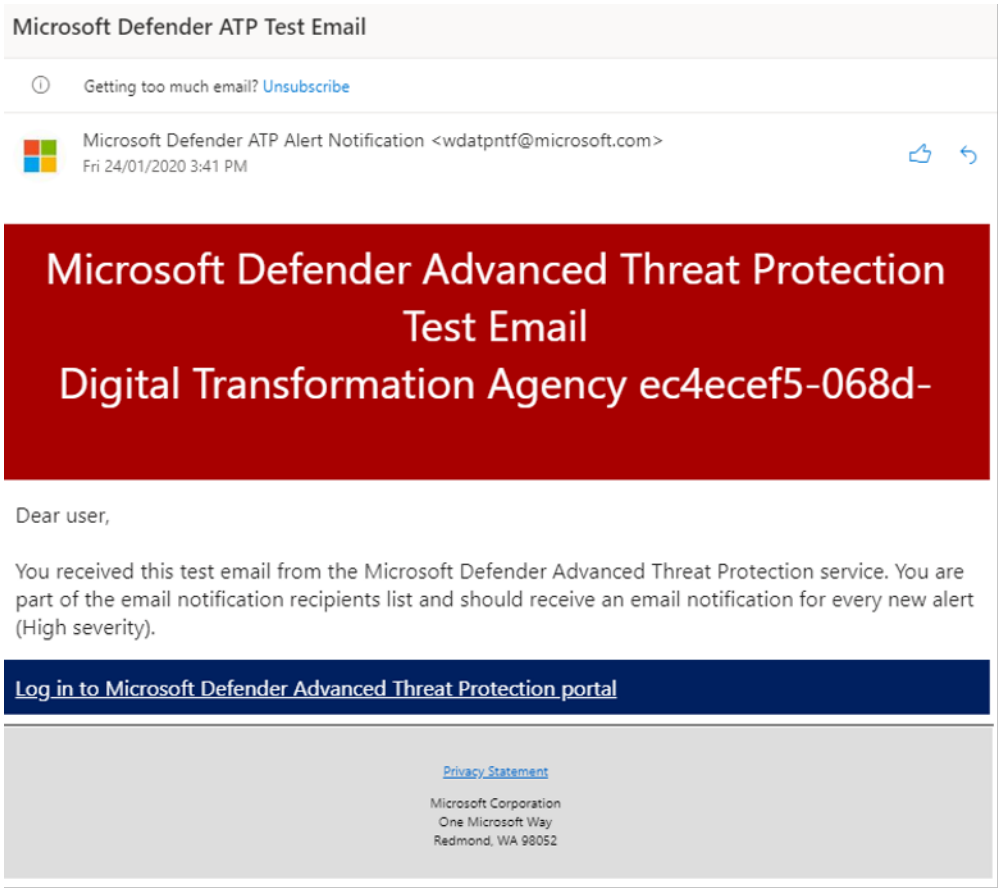


Figure 6 Alert Resolution Email

Agency cyber security personnel should be aware of these notifications but should not rely on them as a trigger to cease investigation and/or recovery activities.

Recommendation It is recommended that Agency cyber security personnel verify that an incident resulting from alert is actually resolved before moving to the post-incident phase.

Post-incident activity

In accordance with the Agency's overarching IRP recommendation, 'lessons learnt' meetings should be held after all major incidents. However, for incidents it is recommended that one of these meetings is held after every incident. This provides an opportunity to assess the current controls in place and evaluate if additional controls can be applied to prevent or minimise the effect of a similar incident occurring again.

Due to the regular update cadence for Azure and Office 365, new features are made available monthly. This often includes Preview features in Azure that provide enhanced capabilities but are still under development by Microsoft. One of the goals of the post-incident meetings should be to assess newly released and preview features for their potential to reduce the risk of the incident re-occurring. This may require specialist resources to attend to present newly available features and discuss how implementing them may reduce the risk to the system.

Note, new capabilities and services – including all Preview features – should be assessed by Agency cyber security personnel before being enabled.

Figure 7 illustrates how a preview feature is presented in the Azure portal using the "… (Preview)" suffix to the feature/service name.

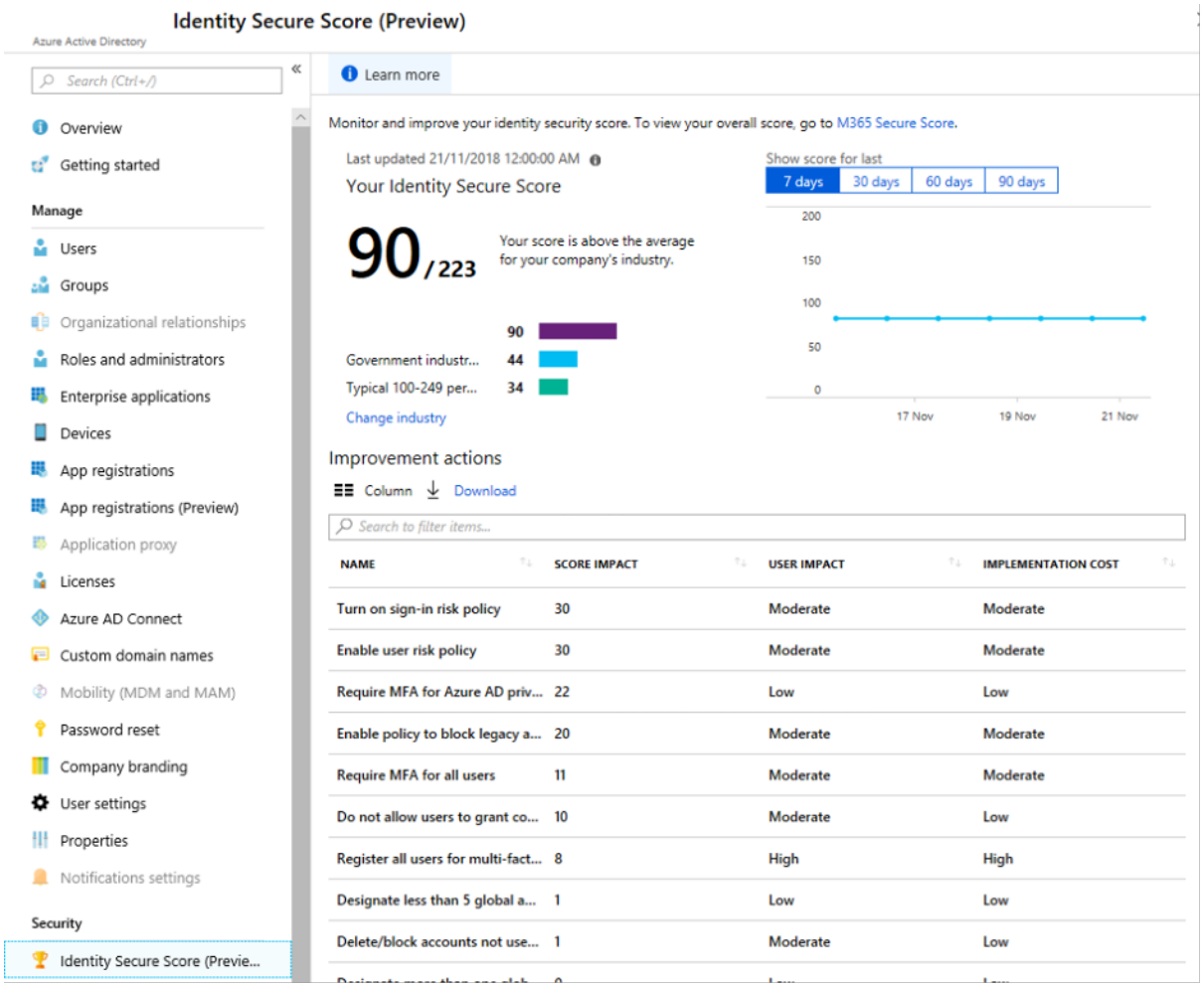


Figure 7 Azure AD Preview Feature

Note, as of the time of writing the Azure AD Identity Secure Score feature is no longer in preview and is generally available for all tenants.

The outcomes of all post-incident meetings should be recorded in the report prepared for each incident. This ensures there is a document chain of events for the incident including tasks that will now be undertaken due to the analysis of the incident, but potentially not directly related (for example applying an additional control to prevent a future incident). This report may be the subject of an internal or external audit in accordance with the Agencies reporting requirements and therefore should be treated as a formally controlled document and stored in accordance with existing policies. Additionally, any information collected as part of the incident response should be either be directly included in the report, or its storage location referenced, as applicable.

All other aspects of the 'lessons learnt' meetings and reporting requirements should be undertaken in accordance with the recommendations provided in the Agency's overarching IRP.

Coordination with external resources

In some cases, Agency cyber security personnel may require the assistance of additional external resources to aid in one or more phases of the Incident Response Life Cycle. When this is required, Agency cyber security personnel should follow existing Agency policies and procedures to appropriately engage and communicate with external resources to assist with incident management and response.

Microsoft support requests

With the introduction of Azure AD an additional external resource becomes available to assist Agency cyber security personnel manage and respond to security incidents. Microsoft Support Requests can be made from within the Azure Portal to report issues and access assistance with all Azure hosted services,

including Azure AD, Azure MFA, and Conditional Access. Support Requests are associated with Azure Subscriptions, and a user must have 'write permissions' for the subscription to raise a support request.

The New support request wizard provides a three-step process to detail and submit new support requests via the Azure Portal. The three steps are:

- Basics – which includes the issue type (most likely to be technical if raised in relation to a security incident), the subscription affected and the specific service. This is illustrated below in Figure 8.
- Problem – which includes a technical description of the issue/incident including severity, problem type, category, title, and details. It also provides fields to identify when the problem started and provide the option for the user to upload a file.
- Contact information – which includes contact details for a Microsoft engineer to use to assist with the support request. Depending on the reported severity of the issue the Preferred contact method and Response may be auto-filled (for example, high severity requests default to phone and 24x7 respectively).

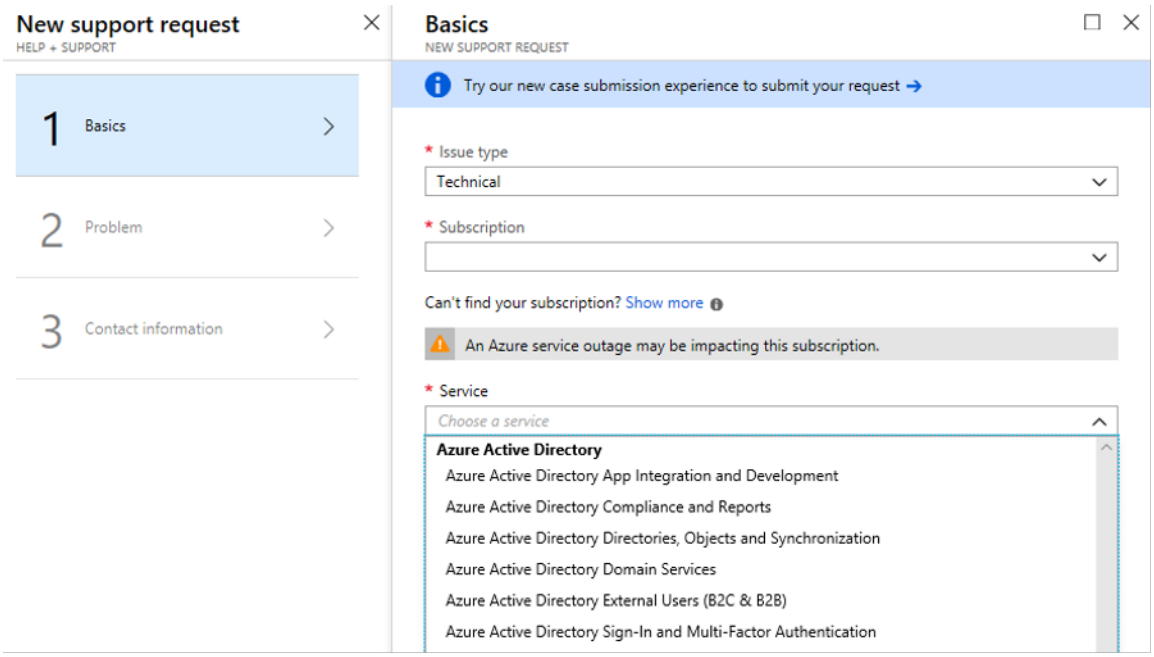


Figure 8 New Support Request

The progress of support requests can also be tracked from within the Azure Portal under the Help + support page. This is illustrated below in Figure 9.

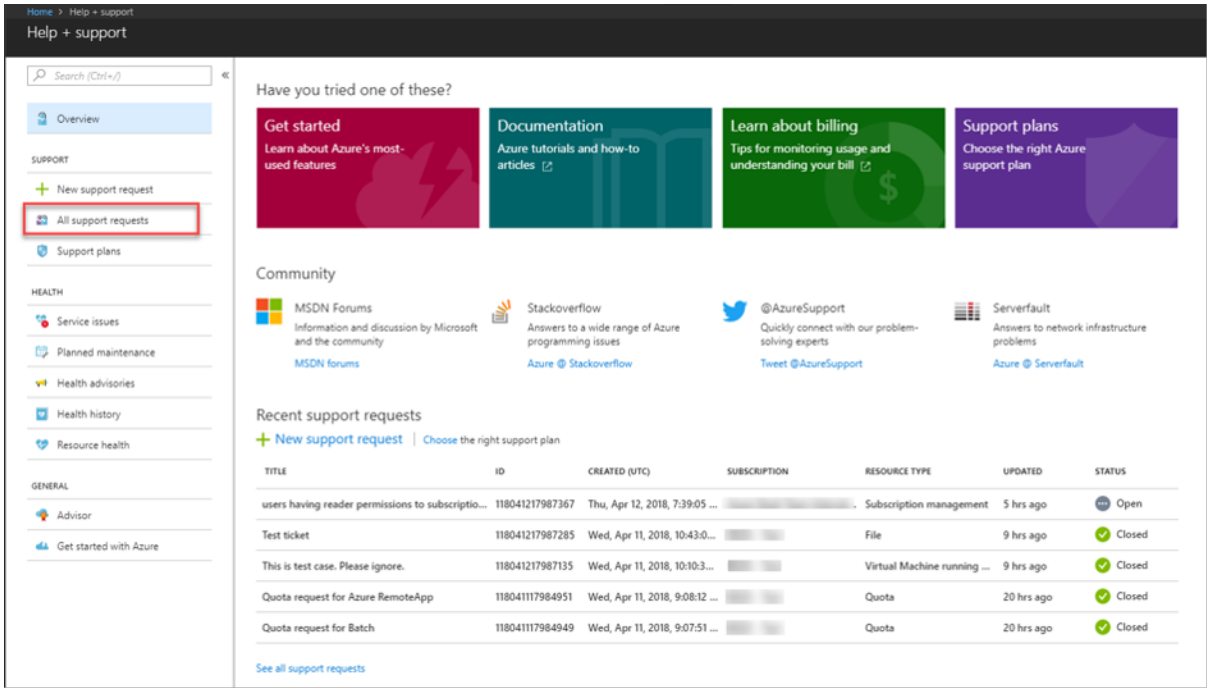


Figure 9 All Support Requests

For more information on creating Azure support requests, including any updates to the process, refer to Create an Azure support request.

Australian Cyber Security Centre

In the case where an incident has not been able to be resolved using the steps defined previously, the ACSC may be engaged by agency approved staff as per the Agency's overarching IRP.

An incident can be reported to the ACSC via the following methods:

- Website - https://www.cyber.gov.au/contact
- Phone number – 1300 CYBER1 (1300 292 371)
- Email – asd.assist@defence.gov.au

Note, reporting an incident via the phone is preferred when the incident is considered urgent by the Agency.

Playbook: Ransomware

Investigate, remediate (contain, eradicate), and communicate in parallel! Containment is critical in ransomware incidents, prioritize accordingly.

Assign steps to individuals or teams to work concurrently, when possible; this playbook is not purely sequential. Use your best judgment.

Investigate

`TODO: Expand investigation steps, including key questions and strategies, for ransomware.`

1. **Determine the type** of ransomware (*i.e.,* what is the family, variant, or flavor?)[1]
    1. Find any related messages. Check:
        - graphical user interfaces (GUIs) for the malware itself
        - text or html files, sometimes opened automatically after encryption
        - image files, often as wallpaper on infected systems
        - contact emails in encrypted file extensions
        - pop-ups after trying to open an encrypted file
        - voice messages
    2. Analyze the messages looking for clues to the ransomware type:
        - ransomware name
        - language, structure, phrases, artwork
        - contact email
        - format of the user id
        - ransom demand specifics (*e.g.*, digital currency, gift cards)
        - payment address in case of digital currency
        - support chat or support page
    3. Analyze affected and/or new files. Check:
        - file renaming scheme of encrypted files including extension (*e.g.*, `.crypt`, `.cry`, `.locked`) and base name
        - file corruption vs encryption
        - targeted file types and locations
        - owning user/group of affected files
        - icon for encrypted files
        - file markers
        - existence of file listings, key files or other data files
    4. Analyze affected software or system types. Some ransomware variants only affect certain tools (*e.g.*, databases (https://www.bleepingcomputer.com/news/security/mongodb-apocalypse-professional-ransomware-group-gets-involved-infections-reach-28k-servers/)) or platforms (*e.g.*, NAS products (https://forum.synology.com/enu/viewtopic.php?f=3&t=88716))
    5. Upload indicators to automated categorization services like Crypto Sheriff (https://www.nomoreransom.org/crypto-sheriff.php), ID Ransomware (https://id-

ransomware.malwarehunterteam.com/), or similar.

2. **Determine the scope:**
    1. Which systems are affected? `TODO: Specify tool(s) and procedure`
        - Scan for concrete indicators of compromise (IOCs) such as files/hashes, processes, network connections, etc. Use endpoint protection/EDR, endpoint telemetry, system logs, etc.
        - Check similar systems for infection (*e.g.*, similar users, groups, data, tools, department,configuration, patch status): check IAM tools, permissions management tools, directory services, *etc.*
        - Find external command and control (C2), if present, and find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, netflow or router logs, *etc.*
    2. What data is affected? (*e.g.*, file types, department or group, affected software) `TODO: Specify tool(s) and procedure`
        - Find anomalous changes to file metadata such as mass changes to creation or modification times. Check file metadata search tools
        - Find changes to normally-stable or critical data files. Check file integrity monitoring tools
3. **Assess the impact** to prioritize and motivate resources
    1. Assess functional impact: impact to business or mission.
        - How much money is lost or at risk?
        - How many (and which) missions are degraded or at risk?
    2. Assess information impact: impact to confidentiality, integrity, and availability of data.
        - How critical is the data to the business/mission?
        - How sensitive is the data? (*e.g.*, trade secrets)
        - What is the regulatory status of data (*e.g.*, PII, PHI)
4. **Find the infection vector.** Check the tactics captured in the Initial Access tactic (https://attack.mitre.org/tactics/TA0001/) of MITRE ATT&CK[4]. Common specifics and data sources include:
    - email attachment: check email logs, email security appliances and services, e-discovery tools, *etc.*
    - insecure remote desktop protocol (RDP): check vulnerability scanning results, firewall configurations, *etc.*
    - self-propagation (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, *etc.*)
    - infection via removable drives (worm or virus)
    - delivered by other malware or attacker tool: expand investigation to include additional attacker tools or malware

Remediate

- **Plan remediation events** where these steps are launched together (or in coordinated fashion), with appropriate teams ready to respond to any disruption.
- **Consider the timing and tradeoffs** of remediation actions: your response has consequences.

Contain

`TODO: Customize containment steps, tactical and strategic, for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

In ransomware situations, containment is critical. Inform containment measures with facts from the investigation. Prioritize quarantines and other containment measures higher than during a typical response.

Quarantines (logical, physical, or both) prevent spread *from* infected systems and prevent spread *to* critical systems and data. Quarantines should be comprehensive: include cloud/SaaS access, single-sign-on, system access such as to ERP or other business tools, *etc.*

- Quarantine infected systems
- Quarantine affected users and groups.
- Quarantine file shares (not just known-infected shares; protect uninfected shares too)
- Quarantine shared databases (not just known-infected servers; protect uninfected databases too)
- Quarantine backups, if not already secured
- Block command and control domains and addresses
- Remove vector emails from inboxes
- Confirm endpoint protection (AV, NGAV, EDR, *etc.*) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, *etc.*).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs

`TODO: Consider automating containment measures using orchestration tools.`

Eradicate

`TODO: Customize eradication steps, tactical and strategic, for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

- Rebuild infected systems from known-good media
- Restore from known-clean backups
- Confirm endpoint protection (AV, NGAV, EDR, *etc.*) is up-to-date and enabled on all systems.
- Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, *etc.*).
- Deploy custom signatures to endpoint protection and network security tools based on discovered IOCs
- **Watch for re-infection:** consider increased priority for alarms/alerts related to this incident.

Reference: Remediation Resources

`TODO: Specify financial, personnel, and logistical resources to accomplish remediation.`

Communicate

`TODO: Customize communication steps for ransomware`

`TODO: Specify tools and procedures (including who must be involved) for each step, below, or refer to overall plan.`

1. Escalate incident and communicate with leadership per procedure
2. Document incident per procedure

3. Communicate with internal and external legal counsel per procedure, including discussions of compliance, risk exposure, liability, law enforcement contact, *etc.*
4. Communicate with users (internal)
    1. Communicate incident response updates per procedure
    2. Communicate impact of incident **and** incident response actions (e.g., containment: "why is the file share down?"), which can be more intrusive/disruptive during ransomware incidents
    3. Communicate requirements: "what should users do and not do?" See "Reference: User Actions for Suspected Ransomware," below
5. Communicate with customers
    1. Focus particularly on those whose data was affected
    2. Generate required notifications based on applicable regulations (particularly those that may consider ransomware a data breach or otherwise requires notifications (*e.g.*, HHS/HIPAA (https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf))) `TODO: Expand notification requirements and procedures for applicable regulations`
6. Contact insurance provider(s)
    1. Discuss what resources they can make available, what tools and vendors they support and will pay for, *etc.*
    2. Comply with reporting and claims requirements to protect eligibility
7. Communicate with regulators, including a discussion of what resources they can make available (not just boilerplate notification: many can actively assist)
8. Consider notifying and involving law enforcement (https://www.nomoreransom.org/en/report-a-crime.html)
    1. Local law enforcement
    2. State or regional law enforcement
    3. Federal or national law enforcement
9. Communicate with security and IT vendors
    1. Notify and collaborate with managed providers per procedure
    2. Notify and collaborate with incident response consultants per procedure

Recover

`TODO: Customize recovery steps for ransomware.`

`TODO: Specify tools and procedures for each step, below.`

> ***We do not recommend paying the ransom:*** *it does not guarantee a solution to the problem. It can go wrong (e.g., bugs could make data unrecoverable even with the key). Also, paying proves ransomware works and could increase attacks against you or other groups.*[2, paraphrased]

1. Launch business continuity/disaster recovery plan(s): *e.g.*, consider migration to alternate operating locations, fail-over sites, backup systems.
2. Recover data from known-clean backups to known-clean, patched, monitored systems (post-eradication), in accordance with our well-tested backup strategy.

- Check backups for indicators of compromise
- Consider partial recovery and backup integrity testing

3. Find and try known decryptors for the variant(s) discovered using resources like the No More Ransom! Project's Decryption Tools page (https://www.nomoreransom.org/en/decryption-tools.html).
4. Consider paying the ransom for irrecoverable critical assets/data, in accordance with policy `TODO: Expand and socialize this decision matrix`
    - Consider ramifications with appropriate stakeholders
    - Understand finance implications and budget
    - Understand legal, regulatory, and insurance implications
    - Understand mechanisms (*e.g.*, technologies, platforms, intermediate vendors/go-betweens)

Resources

Reference: User Actions for Suspected Ransomware

`TODO: Customize steps for users dealing with suspected ransomware`

1. Stay calm, take a deep breath.
2. Disconnect your system from the network `TODO: include detailed steps with screenshots, a pre-installed tool or script to make this easy ("break in case of emergency"), consider hardware network cut-off switches`
3. Take pictures of your screen using your smartphone showing the things you noticed: ransom messages, encrypted files, system error messages, *etc.*
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. Every little bit helps! Document the following:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. Where were you when it happened, and on what network? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are you using? (operating system, hostname, *etc.*)
    7. What account were you using?
    8. What data do you typically access?
    9. Who else have you contacted about this incident, and what did you tell them?
5. Contact the help desk and be as helpful as possible
6. Be patient: the response may be disruptive, but you are protecting your team and the organization! **Thank you.**

Reference: Help Desk Actions for Suspected Ransomware

`TODO: Customize steps for help desk personnel dealing with suspected ransomware`

1. Stay calm, take a deep breath.
2. Open a ticket to document the incident, per procedure `TODO: Customize template with key questions (see below) and follow-on workflow`

3. Ask the user to take pictures of their screen using their smartphone showing the things they noticed: ransom messages, encrypted files, system error messages, *etc.* If this is something you noticed directly, do the same yourself.
4. Take notes about the problem(s) using the voice memo app on your smartphone or pen-and-paper. If this is a user report, ask detailed questions, including:
    1. What did you notice?
    2. Why did you think it was a problem?
    3. What were you doing at the time you detected it?
    4. When did it first occur, and how often since?
    5. What networks are involved? (office/home/shop, wired/wireless, with/without VPN, *etc.*)
    6. What systems are involved? (operating system, hostname, *etc.*)
    7. What data is involved? (paths, file types, file shares, databases, software, *etc.*)
    8. What users and accounts are involved? (active directory, SaaS, SSO, service accounts, *etc.*)
    9. What data do the involved users typically access?
    10. Who else have you contacted about this incident, and what did you tell them?
5. Ask follow-up questions as necessary. **You are an incident responder, we are counting on you.**
6. Get detailed contact information from the user (home, office, mobile), if applicable
7. Record all information in the ticket, including hand-written and voice notes
8. Quarantine affected users and systems `TODO: Customize containment steps, automate as much as possible`
9. Contact the security team and stand by to participate in the response as directed: investigation, remediation, communication, and recovery

Additional Information

1. "Ransomware Identification for the Judicious Analyst" (https://www.gdatasoftware.com/blog/2019/06/31666-ransomware-identification-for-the-judicious-analyst), Hahn (12 Jun 2019)
2. No More Ransom! (https://www.nomoreransom.org) Project, including their Crypto Sheriff (https://www.nomoreransom.org/crypto-sheriff.php?lang=en) service and their Q&A (https://www.nomoreransom.org/en/ransomware-qa.html)
3. ID Ransomware (https://id-ransomware.malwarehunterteam.com/) service
4. MITRE ATT&CK Matrix (https://attack.mitre.org), including the Initial Access (https://attack.mitre.org/tactics/TA0001/) and Impact (https://attack.mitre.org/tactics/TA0040/) tactics

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

RANSOMWARE EMERGENCY RESPONSE GUIDE

RECOVER FROM A RANSOMWARE ATTACK

cyber.gov.au

What to do if you're held to ransom

A guide to remove ransomware, recover your files and protect yourself against future attacks.

Ransomware is a common and dangerous type of malware. It works by locking up or encrypting your files so that you can no longer access them.

A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files, or to prevent data and intellectual property from being leaked or sold online.

This guide has simple steps to follow if you are a victim of ransomware. The first section will show you how to respond if one of your devices is infected with ransomware. The second section will help you to recover your files and restore your devices.

NEVER PAY A RANSOM.

There is no guarantee your files will be restored, nor does it prevent the publication of any stolen data or its sale for use in other crimes. You may also be targeted by another attack.

Call the Australian Cyber Security Centre 24/7 Hotline on **1300 CYBER1** (1300 292 371) if you need cyber security assistance.

Not all ransomware attacks are the same so some of the steps in this guide may not apply to your situation. Use the actions that best suit your case.

Table of Contents

Here are the simple ways you can remove ransomware, recover your files and protect yourself against future attacks. **If you get stuck, find a professional to help you work through a ransomware attack or call the Australian Cyber Security Centre's 24/7 Hotline on 1300 CYBER1 (1300 292 371).**

RESPOND TO A RANSOMWARE ATTACK

RECOVER FROM A RANSOMWARE ATTACK

PREVENT FUTURE ATTACKS

Respond to a ransomware attack

Start here if you are experiencing a ransomware attack.

Work through the steps below as quickly as you can. Acting quickly could stop the ransomware from spreading.

If you get stuck, seek professional help. Ransomware attacks can cause serious damage. It is hard to tackle and overcome them on your own. Consider finding a professional to help you work through a ransomware attack and get back on your feet.

Step 1: Record important details

It is important to record important details about the ransomware attack to help you:

- ask for help from a professional
- make an insurance, bank or legal claim that may follow after the attack
- make a report to the ACSC through ReportCyber
- tell your family, colleagues or authorities that there has been an issue.

Complete this step as quickly as possible, as the ransomware could still be spreading through your device and network.

What to record

The details you should try to record are:

- if the files that have been affected by ransomware have a new extension
- the name of any new file extension
- the ransom note
- anything else that has changed since the attack.

A quick way to record the information you need is to take a photo of your screen. It's okay if you can't record everything, but you should try to capture as much as possible, as quickly as you can.

Step 2: Turn off the infected device

As soon as you have recorded details about the ransomware attack, turn off the infected device by holding down the power button or unplugging it from the wall. For most people, this is the best way to stop the ransomware from spreading.

Step 3: Disconnect your other devices

Ransomware can spread across networks. If there are other devices on your network, you should turn them off too. Start with the devices that are most important to you. Important devices typically include things like Network Attached Storage (NAS) devices, servers, computers, phones, tablets, and any other devices that store valuable information.

Step 4: Change your important passwords

Some forms of ransomware steal your passwords. It can be difficult to know what information ransomware has accessed so, as a precaution, you should change the passwords for your accounts as soon as possible. Start with your most important accounts first.

What's important will be different for everyone, but important accounts typically include:

- cloud storage accounts
- email accounts
- bank accounts
- business accounts.

The ACSC has published guidance on using password managers and guidance on creating passphrases (a strong type of password). These resources are available at **cyber.gov.au/passphrases**.

As you change your passwords, consider enabling multi-factor authentication on supported accounts. Multi-factor authentication makes it harder for cybercriminals to get access to your accounts. The ACSC has published guidance on enabling multi-factor authentication. This is available at **cyber.gov.au/mfa**.

Recover from a ransomware attack

Now that you've responded to a ransomware attack, it's time to recover your information, restore your infected devices and report the incident.

Note: At the end of this guide, you will be given guidance on reporting the incident. In some cases you may need to make reports urgently, for example, to meet obligations to your customers or your insurance company. Consider if you have any urgent reporting requirements before you begin the next step.

Step 5: Recover your information

Check your backups

The ACSC recommends you keep backups of your information as a precaution against things like ransomware attacks.

If you have backups, make sure they are free from ransomware to avoid re-infecting your device. Your backups may be infected with ransomware if they are saved on your infected device or were on the same network as your infected device at any point since the infection. Your backups should be secure if they were never connected to the infected device or to the same network as the infected device.

If you think your backups may be infected with ransomware, don't try to access them, ask an IT professional for support.

If you have backups that are free from ransomware, make sure you don't connect them to your infected device or network. Remove the ransomware from the infected device or network first using the guidance in Step 6.

What to do if you don't have a secure backup of your information

If you do not have a secure backup, it may still be possible to recover your information but you will likely need professional help. Consider how important the affected information is to you and how much you are willing to pay for professional help to restore it.

Remember, never pay a ransom. There is no guarantee your files will be restored, nor does it prevent the publication of any stolen data or its sale for use in other crimes. You may also be targeted by another attack.

Step 6: Remove ransomware from affected drives and devices

Ransomware can be difficult to remove. For most people, the best way to remove ransomware is to wipe all infected drives and devices and reinstall their operating systems. **Be aware that this step will permanently delete all of your information so make sure you've completed Step 5 and recovered what information you can first.**

Remember that ransomware can spread across a network. We recommend following this step for all drives and devices that were on the same network as the infected device at any point since the infection.

The steps to wipe your drives and devices vary across manufacturers. The manufacturer of your drive or device will have guidance on their website. We've listed some resources below.

Apple iPhone, iPad or iPod: support.apple.com/HT201252
Apple Mac devices: support.apple.com/HT212749
Microsoft Windows devices: support.microsoft.com (Search for the article "Recovery options in Windows")
Samsung phones: samsung.com/au/support/mobile-devices/factory-data-reset-samsung-phone/
Google Pixel phones: support.google.com/pixelphone/answer/4596836

Step 7: Restore your information

Now that you have removed the ransomware from affected drives and devices, it is safe to connect them to your backups and restore your information. Remember the guidance in Step 5; only restore information from a backup if you are confident that it is free from ransomware.

The ACSC's guidance on backups includes information on restoring your information. This is available at **cyber.gov.au/backups**.

Step 8: Notify and Report

Report the incident to the ACSC through ReportCyber at **cyber.gov.au/acsc/report**. Submitting a report helps to disrupt cybercrime operations and make Australia the most secure place to connect online. Include the information you recorded in Step 1.

Additional reporting responsibilities for businesses

If you're a business, depending on the severity of the ransomware compromise, you may have to notify your customers of the attack.

If your business holds sensitive information (such as financial or personally identifiable information), or is part of a government supply chain, you may also need to report the incident to regulators.

If you think you need to make a report, consult with the Office of the Australian Information Commissioner at **oaic.gov.au** or seek legal or government support.

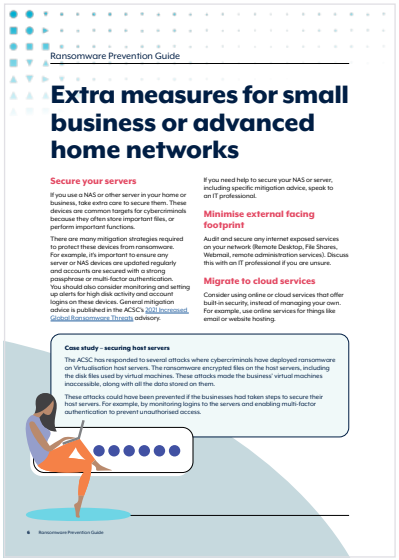
Prevent future attacks

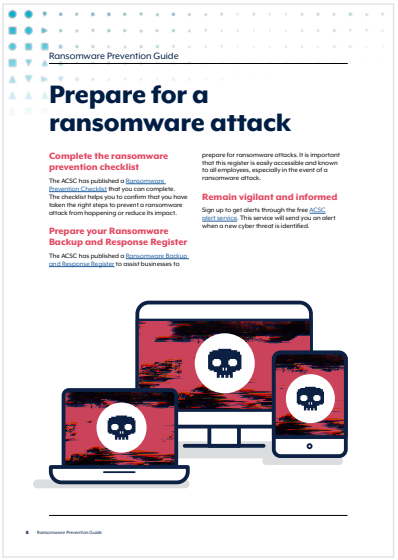
Step 9: Prevent future attacks

Take some time to consider how your device was infected with ransomware so you can prevent the same thing from happening again.

The ACSC has published advice to help you protect yourself against ransomware attacks at **cyber.gov.au/ransomware**.

This advice outlines precautions you can take to reduce the impact of ransomware attacks or prevent them from happening in the first place.





Notes

Notes

Notes

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Anti-Ransomware Guide

Christopher M. Frenz & Christian Diaz

Version 1.7
12 March-2018

Executive Summary

Open up any newspaper or news site and an increasingly common headline is becoming "hospital held for ransom". While hospitals and other organizations often have downtime procedures that let them revert back to paper for dealing with power outages and other disasters, it is still a nightmare scenario to find your entire organization's IT infrastructure screeching to a halt all because someone clicked on a malicious link or opened a questionable email attachment. Moreover, many organizations have a significant number of legacy systems that make security a challenge and beyond very basic security provisions often do not have a corporate culture that is heavily focused on information security. This has left many organizations struggling with how to handle ransomware attacks. The below is meant to serve as a comprehensive defense in depth based checklist and guide to preventing ransomware from taking a foothold in your organization as well as ensuring the proper procedures are in place to deal with an actual ransomware outbreak in your environment. Given the prevalence of Windows systems as ransomware targets, the guide is geared towards a Windows environment but is designed to be product agnostic. Please note that the list is designed to be comprehensive and as such not all controls may be applicable to all environments.

Perimeter Protections:

These are your first line of defense as stopping a threat before it gains access to any of your systems or employees is always ideal.

Firewall:

While a firewall at the perimeter is probably already in place for most organizations, it is important to verify that your firewall is configured for egress filtering as well as ingress filtering. Ingress filtering controls what communications are allowed into the organization's network, while egress filtering controls what communications are allowed to leave the organization's network. Both egress and ingress access controls should be based on a least privilege model. Systems that do not need access to external information sources and systems should be blocked from communicating with external entities. A system without access to any external entities is far less likely to become an entry point for malware than an internet connected system. Moreover, in the event that a ransomware infection takes place it will not be able to phone home if proper egress filtering is in place. Logging should also be turned on on the firewall as repeated access attempts being logged to known malicious IP addresses can serve as an indicator of a problem. Organizations may also want to consider blocking the domains contained in the Ransmoware Trackers Domain Blocklist in their firewall - https://ransomwaretracker.abuse.ch/downloads/RW_DOMBL.txt

Proxy Server/Web Filter:

As mentioned above, cutting systems off from the internet completely is a great defense where feasible, but the reality is that completely blocking internet on all systems is likely not feasible and would be a hindrance to business operations. Internet connected systems should be configured to go through a proxy server that allows for Web content to be filtered, with firewall rules ensuring that proxied Web access is the only means of egress for http and https connections. While a whitelisting approach to Web access is most ideal, organizations should at a minimum use their filtering appliance to block access to known malicious sites, spam/phishing sites, proxy avoidance sites, pornography, and all other categories of sites deemed unnecessary for normal business operations. It is also recommended, where feasible, that any website yet uncategorized by the vendor be blocked as there is a higher chance of such a site being malicious in nature than being a new valid business site. While it may be politically unpopular within many organizations, it is also strongly recommended to block access to personal

email, file sharing sites, social media, instant messaging, and advertising networks at this level. Special exemptions for file sharing sites, social media, etc, can be added on an as needed basis. Prohibiting the download of executable files (e.g. .exe, .scr, etc) onto endpoints should also be put in place. Many proxy servers/Web filtering appliances also have the ability to scan incoming web content with an AV engine. Where this is supported it is recommended that it be turned on and that where feasible a different AV engine than the one used internally used to enhance the likelihood that a signature exists for a relatively new threat. Web filters should be updated regularly to ensure that categorizations for malicious and other sites are always current.

In addition to the blocks stated above it is advised that Web traffic to the following top level domains be completely blocked as results from Spamhaus (https://www.spamhaus.org/statistics/tlds/) and BlueCoat (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems/) suggest that the majority of sites hosted on these TLDs are suspicious in nature:

Top Level Domain
.accountant
.biz
.click
.country
.cricket
.download
.gdn
.gq
.kim
.link
.party
.review
.review
.science
.stream
.tk
.top
.trade
.win
.work
.zip

Organizations may also want to consider blocking the URLs contained in the Ransmoware Trackers URL BlockList in their Web filtering appliance - https://ransomwaretracker.abuse.ch/downloads/RW_URLBL.txt

SPAM Filter:

As a perimeter defense we are discussing SPAM filters that filter email before they hit your corporate mail server or if you are using hosted email ensuring that the SPAM filtering made available by your hosting provider is turned on. It is far better to block at the perimeter known SPAM, mail containing

malicious links, and mail containing malicious attachments, that to let other internal layers of defenses handle it. It is also recommended to block any message that contains executable attachments such as .exe or .vbs files. For institutions that do not have any international presence it may also be advisable to block all emails coming from locations outside of North America and whitelisting any necessary exceptions. As with Web filtering software, SPAM filters should always be kept up to date to ensure they have the latest block lists and that their AV engines have the latest signatures for analyzing attachments. Where feasible the AV engine used in the SPAM filter should be different than the AV engine used on endpoints where email will be accessed.

VPN/Remote Access:

The SamSam ransomware is commonly reported as being spread through attempts to connect to organizations remotely through poorly secured publicly facing RDP services. It is advised that organizations limit remote access to just necessary accounts and that an account lockout policy is in place the help prevent the brute forcing of credentials. Remote access should also make use of two-factor authentication wherever feasible to mitigate the damage that can be caused by a lost or stolen access credentials.

Network Defenses:

Defenses than can be deployed on the LAN to help detect and mitigate malware outbreaks.

DNS Sinkhole:

While connectivity to malicious sites is ideally blocked at the perimeter, an extra layer of defense against establishing connections to malicious sites can be added by creating a DNS sinkhole which will prevent connections to certain domains by giving out false information when a DNS request comes in for one of the domains in the sinkhole. As with perimeter defenses, preventing any system or person from accessing malicious content is always far preferable to mitigating it once it has been downloaded to or accessed by an endpoint. Ideally your sinkhole domain list will be from a different source than the one used on your Web filter to ensure more comprehensive coverage of malicious domains. A tutorial on creating DNS sinkholes on Windows DNS servers can be found at: https://cyber-defense.sans.org/blog/2010/08/31/windows-dns-server-blackhole-blacklist

Network Segmentation:

Network Segmentation via VLANs and ACLs that control traffic between VLANs will not work to prevent a ransomware attack from gaining access to your systems, but will be invaluable if a malware infection is able to gain a foothold within your organization. Network segmentation can help to ensure that a malware infection, or other security issue, stays isolated to just the network segment the infected endpoint is on and does not spread through the entirety of the organization. It is particularly important for organizations that maintain legacy systems which are no longer able to receive security updates.

Virtual Machine Segmentation:

Just as the network segmentation discussed above is key in ensuring that the number of systems a malware infection can spread to is minimized, it is important to remember that many virtual machine communications take place across the back plane of a server and do not transverse standard network equipment like switches. For heavily virtualized environments it is advisable to deploy virtual machine segmentation technologies, such as VMware's NSX or Microsoft's HNV, to ensure that virtual machine communications can be controlled with network security mechanisms that are equivalent to that of physical systems.

Network Intrusion Detection System (NIDS):

Having a network IDS in place will likely not be a highly effective way of preventing malware from gaining access to your system as most are geared more towards detecting exploit attempts than malware, but a NIDS system can be used to alert to potential outbreaks since they can be used to alert if communication attempts are being made to malicious IP addresses such as command and control centers for botnets and key generation sites for ransomware tools. The earlier IT and infosec staff are alerted to the presence of malware outbreak, the better the chance there is at successfully containing the incident, and this is one such avenue of detection that can be employed. Depending on the deployment, NIDS systems may also help to pinpoint a system within the organization that is attempting to infect other systems.

Endpoint Protections:

Protections that exist on desktop PCs and other systems that users interface with.

Fully Patched and Updated:

Ransomware and other malware often use a variety of exploits to gain a foothold onto systems and ensuring that the OS and all applications on the system are fully patched and updated will minimize the number of ways that endpoints can be successfully exploited. With regards to ransomware keeping your email client, browser, and Flash fully updated is of critical importance. Organizations should have robust procedures in place for ensuring proper patch management and the routine patching of software.

No Unnecessary Applications and Services:

If an application does not exist on the system it cannot be exploited so ensuring that endpoint configurations also follow a least privilege model is an effective way of reducing the attack surface of endpoints. It is particularly advisable to not run Java and Flash on computers that do not require it.

No Administrative Rights:

Administrative rights should only be used for administrative tasks and normal computer usage should never be performed from an account with administrative privilege. This will prevent many types of malware from gaining a foothold as they users account may simply not have the proper permissions to "install" the malware.

Antivirus (AV):

Antivirus should be run on all endpoints and configured for on access scanning of files and other resources. Antivirus should be kept up to date and alerting should be configured to notify IT staff on any possible infections. It is important to remember that AV is largely signature based and, as such, can only effectively detect known threats. AV may not provide any protection against a novel virus or a new malware variant. Ideally this is a different vendor than one used to scan for viruses at the perimeter defense level.

Next Generation AV:

Antivirus solutions that signature-less in nature and as such have the potential to detect zero-day attacks and novel strains of malware. Next-gen AV uses methods like behavioral detection, machine

learning, and cloud based file execution to try to identify exploit attempts and malware. Some Next-gen AV packages are certified under PCI-DSS as AV replacements but not all are. In many cases they can be used as a potential compliment to traditional AV.

Host Based Intrusion Detection/Prevention Systems (HIDS/HIPS):

These systems could be standalone or integrated into an endpoint protection solution from an AV vendor. They work to detect suspicious changes to critical system files, potential buffer overflows, and other potentially suspicious activity on endpoints. They may help to provide earlier insight into a possible outbreak and some have a limited ability to mitigate certain exploit attempts.

Web Filtering:

Many endpoint protection packages provide an additional means of filtering malicious Web content and it is advisable to turn these filters on as well, particularly if the recommended practice of using a different vendor for internal systems vs. the perimeter is followed. This will increase the chance that malicious Web content is blocked before a system or user has the ability to access it.

SPAM Filtering:

As with Web filtering, SPAM filtering is also possible at the endpoint level and having a different filtering solution in place on endpoints can help to increase the odds that SPAM and malicious emails that bypass perimeter defenses are detected. This is critical since certain ransomware variants like Locky are commonly spread through malicious email attachments.

Disable Support for Macros:

Macros and other executable content can be embedded in documents used within office applications and PDF files. Odds are that most users in your organization have no legitimate need for such features and support for such features should be turned off by default.

Software Restriction Policies/AppLocker:

GPO policies can be set to blacklist certain applications from running and to blacklist applications from running in certain locations such as the AppData folder of a user's profile, which is a common malware target. Organizations can develop their own policies or use the anti-ransomware policies made available by organizations like Third Tier. As an alternative to GPO blacklists, the free CryptoPrevent utility can also be used to deploy software restriction policies to endpoints. Such policies are a nice compliment to AV software as they are not signature based and may prevent event novel malware variants from running successfully. Just be sure to test any such policies to ensure they do not interfere with any legitimate applications that are used within your environment. A better approach than blacklisting would be an application whitelisting approach, but this is more challenging and time consuming project in order to ensure that no critical applications are broken once only whitelisted applications are allowed to run.

Hosts file:

Hosts files are checked prior to DNS to resolve IP addresses and like DNS sinkholes can be used to prevent malicious domains from being properly resolved. In addition to other Web filtering mechanisms this could provide another layer of defense against a user or system potentially connecting

to a malicious site.

Disable USB Access:

While not as common as Web and email based transmission vectors there have been variants of the CryptoLocker ransomware that have been known to spread via USB drives. Wherever feasible, USB drive access should be blocked.

Virtual Desktop Infrastructure:

If the organizations endpoints are virtualized an additional option for malware defense is to ensure that all VDI desktops are non-persistent and that the systems revert back to a predefined state after each session. This ensures that any malware that infected a VDI desktop is eliminated once the users sessions ends, since the system reversion will restore the desktop to a "like new" pre-infection state.

Enhanced Mitigation Experience Toolkit (EMET):

EMET is a free utility released by Microsoft that helps to detect and prevent exploits that seek to take advantage of memory corruption. EMET is also a nice addition to techniques like AV, because it is not signature based and as such has a chance at stopping even novel malware and exploit attempts. Be sure to test EMET thoroughly before deploying though to ensure it does not interfere with any of the legitimate applications used in your enterprise. More information about EMET can be found at - https://technet.microsoft.com/en-us/security/jj653751 EMET is being made EOL in upcoming months, but will be replaced by Exploit Protection mechanisms built into the Windows Defender Security Center in Windows 10.

Local Administrator Password Solution (LAPS):

While the authors are not aware of any known ransomware variants that spread to other systems using pass the hash techniques, it is a common exploitable vulnerability present in many windows environments since the local admin password for each machine is common across all systems. LAPS randomizes the local admin password of systems and stores the passwords in Active Directory. It further allows for access controls to be put into place to control who can lookup these AD stored local admin passwords. LAPS thus makes it harder for attackers and potential worm like malware to move laterally through a breached organization. More information about LAPS can be found at - https://technet.microsoft.com/en-us/library/security/3062591.aspx

Application Sandboxing:

Application sandboxing is a method of isolating applications so that they only have access to a strict set of tightly controlled resources such as memory and disk space. Typically sandboxed applications are prevented from permanently committing any changes to disk. As such sandboxing application such as web browsers and their respective plugins can help to prevent certain forms of ransomware from impacting your system as the sandbox has the potential to keep the ransomware from accessing the files on your hard drive or network shares.

Disable SMBv1:

Many ransomware variants, including WannaCry, exploit vulnerabilities in the SMBv1 protocol. Modern versions of windows are capable of using the newer SMBv2 and/or SMBv3

protocols and in many cases SMBv1 can be safely disabled within your environment. In case other security vulnerabilities are discovered in the SMBv1 protocol having it disabled may provide a proactive security defense against future ransomware attacks. Microsoft has a guide for disabling SMBv1 available at https://blogs.technet.microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/. Please be sure to test this thoroughly before applying domain wide as older version of Windows and other legacy equipment may require SMBv1 to function properly.

Controlled Folder Access

A new feature being introduced in Windows 10 that will block unauthorized applications from making any changes to the contents of a protected folder.
https://blogs.windows.com/windowsexperience/2017/06/28/announcing-windows-10-insider-preview-build-16232-pc-build-15228-mobile

Rename vssadmin.exe
Shadow copies are commonly used within Windows to create snapshots of previous versions of files and vssadmin.exe is a utility used to administer these shadow copies. Many ransomware variants also use this same utility to delete all of your shadow copies and make it more difficult to recover your files. A tutorial on renaming vssadmin can be found at https://www.bleepingcomputer.com/news/security/why-everyone-should-disable-vssadmin-exe-now/.

PayBreak

An interesting research project which has the potential to reverse the effects of a ransomware attack by recording the encryption keys used by the ransomware to encrypt each file. More information about the technique and tool developed by the researches is available at
https://eugenekolo.com/static/paybreak.pdf.

NAS Server:

Most organizations have shared drives hosted on some form of NAS device that can have shares that are affected by ransomware. The protection mechanisms listed below are in addition to all of the protection mechanisms, such as fully patched, AV, etc, described under endpoint protection.

File Permissions:

A common principle in information security is that of least privilege whereby individuals should only have access to what is required to do their jobs and no more. Unfortunately with regards to network shared drives it is not uncommon for many organizations to experience scope creep with regards to permissions over time. IT is not always properly informed when an employee is transferred to a new department or in some other ways changes roles within an organization. This often results in permissions being added for the new role, but the no longer needed permissions of the old role remaining in place. While it is a good security practice in general to remove unnecessary access permissions, given the spike of ransomware attacks now is a very pertinent time for organizations to audit access permissions on all file shares and ensure that least privilege is being enforced. It is will be significantly more difficult for a malware infection to encrypt files if the user does not have access to the files in the first place. Thus, while this control may not help prevent a ransomware attack, it can go a long way towards mitigating how much data in your organization is impacted.

Shadow Copies:
While some newer ransomware variants have some ability to prevent data restoration from shadow copies having point in time snapshots of your data can provide a quick way of restoring data in many cases. Windows supports taking point in time snapshots of storage data and the ability to roll back to previous point in time versions of files.

Virtual Machine Snapshots:
Virtualization of server infrastructure is quite common and it is also possible to protect against ransomware by taking regularly scheduled virtual machine snapshots that will allow you to roll the virtual machine state back to a previous point in time. This can provide an alternate recovery option in the case a ransomware attack hits.

Data Inventory:
Having a data inventory which maps out what type of data is present in each share is highly beneficial at it can help you to triage your recovery and remediation priorities. Moreover, strains of malware that threaten to dox victims are also appearing. Having a clear sense of what data was encrypted or otherwise effected by the malware, will help the organization to better assess the threat of doxing.

SIEM and Log Management:
Firewalls, servers, IDS devices, Web filters, endpoints, etc all generate log data which may provide clues to a malware outbreak. Having a SIEM solution monitor and process these logs may help to provide an early indication of a possible malware outbreak and as such may help to improve upon response times. Having this data centrally collected may also help in the analysis of it if a root cause analysis later needs to be performed.

Backup:
In case an attacks hits, recovering from a ransomware attack will take the presence of proper backup and recovery plans.

Backup and Recovery Plan:
The organization should have a well-defined recovery point and recovery time objective for each asset, which will help them to determine the proper backup technologies and procedures for their particular environment. There should be clearly documented policies and procedures in place for describing backup schedules, how data is supposed to be backed up or recovered, who is responsible for backups and recovery, etc. It also pays to have employees cross trained in this area.

Storage Snapshots:
In most large environments, server storage is often housed on a SAN and most modern SAN appliances let you retain one or more snapshots of your storage volumes. Storage snapshots should be configured so that if necessary a volume can be rolled back to a previous state that was snapshotted prior to the outbreak. The frequency of snapshots should be determined according to your organizations predetermined recovery point and recovery time objectives.

Offline Backups:
While technologies like real time replication between SANs or data centers are great for business

continuity purposes, they are not much use in recovering from a ransomware attack as the encrypted versions of files will be rapidly replicated to other locations as well. To successfully restore data from backup following a ransomware event backups should be taken in a pull only manner and stored offline to ensure that backup data does not become encrypted and unrecoverable as well. While not as sexy as many newer disk based backup systems, tape can still serve as an ideal backup medium for storing multiple historical point in time snapshots of data from within an environment. Backup frequency should be determined according to your organizations predetermined recovery point and recovery time objectives.

Testing of Backup and Recovery:

Disaster recovery plans are often put to the wayside until disaster actually strikes which can be a big mistake. Backup and recovery should be successfully tested on a routine schedule to ensure that all systems are working properly and that staff members are knowledgeable enough to actually operate the systems. You do not want to wait to find out that a critical server was not being backed up properly after a ransomware attack or other disaster occurs. Routine testing will also improve the recovery time in the event that a disaster actually does strike.

Awareness Training:

Despite many protection mechanisms, the reality is that it is still possible for a malicious email or malicious link to get through and find itself presented to a user. In this case, while AV, software restriction policies, and other endpoint defenses may still protect you the best defense is a well-educated user capable of recognizing a suspicious email and reporting it to the IT department for investigation in a timely manner. The sooner such suspicious communications are reported, the sooner they can be blocked at the perimeter, AV companies contacted to create signature, and other defenses deployed to help stop the spread of the threat throughout the organization.

IoT Malware:

IoT malware like Mirai and Brickerbot have illustrated the potential for IoT devices to be compromised the same as any other network enabled computing device. The following controls are not a comprehensive list of IoT security controls, but a list of the security controls most likely to aid in the prevention, mitigation, and remediation of a ransomware attack. This section will just cover controls that apply to the IoT devices themselves. Network controls, etc., such as network segmentation, are critical to proper IoT security, but are covered in other sections.

No Default Credentials:

To date the most common vector for the compromise of IoT devices has been the use of default credentials, such as in the case of Mirai where a list of 62 username and password pairs was used to compromise hundreds of thousands of devices. Simply put, changing the password of your IoT device from the default will help to prevent many current malware strains that target IoT devices.

Account Lockout:

Given the prevalence of IoT malware that uses password guessing attacks, configuring account lockout

policies, wherever possible, can help stop many IoT malware variants. Access should be restricted after 3 or more failed attempts.

Spare Copy of Firmware:

In case a device is infected having a spare copy of the devices firmware or a way to reset the device to a like new state can be essential to returning the device to a functional state.

Backup Configuration:

Related to the above control, having all custom configurations and settings backed up can be critical to speedily restoring a device to a functional state.

Restricted Management Interface: Management interfaces should be separate from any Internet facing interfaces wherever possible and the management interface placed on an isolated network segment. Admin access should be restricted to the management interface wherever feasible.

Update Mechanisms: All IoT devices should be configured to regularly receive updates and to ensure that the devices are always running the latest firmware version available.

Vulnerability Management:

All organizations should implement a comprehensive vulnerability management program that is designed to identify all information systems (endpoints, servers, IoT, etc) that are not fully patched and that do not comply with organizationally defined security policies. The program should include provisions for performing corrective actions within a finite period of time with the goal of reducing the organizations attack surface as time goes on. Vulnerability management initiatives should include provisions for continuous monitoring so vulnerabilities can be identified and mitigated as they arise.

Incident Response:

While hopefully all of the above defenses keep incidents to a minimum, organizations need to be prepared for the reality that no matter how controls are in place a ransomware incident is always a possibility.

Incident Response Plans:

One of the worst things an organization can do is wait until an incident occurs to begin to think about how to deal with one. Organizations should have a clear cut plan in place that defines how they will react to an incident and who will be responsible for what actions during the detection, containment, eradication, and recovery phases. It is also important all staff are made aware of the plan and are trained to respond appropriately and effectively. For organizations without any sort of incident response plan in place, a good starting resource is https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Mock Incidents:
When an incident occurs the best way to mitigate the damage is to detect and contain the incident as quickly as possible. The best way to do this is to routinely test your incident response plan to see how people within your organization respond to a mock incident. While there are many mock incidents that could be conducted some recommended starting ones would include a phishing campaign against employees and a simulated malware outbreak, which can be safely done using an EICAR test string.

Data Recovery:
If disaster hits it is better to be able to recover your data and applications from a pre-incident backup than via decryption since this will better help to ensure a clean system going forward, but that may not always be possible. If you find yourself the victim of ransomware, and are stuck without a backup, it may pay to check out the site nomoreransom.org which offers ransomware variant detection based on the upload of a sample file and also hosts the decryption keys for the variants Wildfire, Chimera, Teslacrypt, Shade, Coinvault, Rannoh, and Raknhi.

Insurance:
An increasing number of companies are transferring some of their cyber risks to insurance carriers by taking out policies against data breaches. Some insurance companies now provide policies or provisions within policies that particularly deal with ransomware attacks. Companies in heavily targeted industries may want to consider taking out policies that cover such attacks or determining if their existing policies will cover ransomware attacks.

Indicators of Compromise:
Indicators of compromise can be useful in determining if a system has been exposed to or effected by malware. A nice resource on indicators of compromise for various ransomware variants can be found here: http://goo.gl/b9R8DE

Acknowledgements
Thanks to Adrian Sanabria for raising awareness of PayBreak.

Changelog:
Version 1.1 – Added Sections on Data Recovery, Insurance, and Indicators of Compromise
Version 1.2 – TLD block recommendations added to Proxy Server/Web Filter section
Version 1.3 – Sections on Next-Gen AV and Data Inventory added
Version 1.4 – Added sections on IoT Security and Vulnerability Management
Version 1.5 – Added sections on disabling SMBv1
Version 1.6 – Updated EMET section and added sections on Controlled Folder Access and Paybreak.
Version 1.7 – Added section of VPN/Remote Access and a section on renaming vssadmin.exe. Firewall and Web filter sections expanded to include Ransomware Tracker Blocklists.

RANSOMWARE GUIDE

SEPTEMBER 2020

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Overview

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increased, with some demands exceeding US $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small.

These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

This *Ransomware Guide* includes two resources:
Part 1: Ransomware Prevention Best Practices
Part 2: Ransomware Response Checklist

CISA recommends that organizations take the following initial steps:

- Join an information sharing organization, such as one of the following:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC): **https://learn.cisecurity.org/ms-isac-registration**
  - Election Infrastructure Information Sharing and Analysis Center (EI-ISAC): **https://learn.cisecurity.org/ei-isac-registration**
  - Sector-based ISACs - National Council of ISACs: **https://www.nationalisacs.org/member-isacs**
  - Information Sharing and Analysis Organization (ISAO) Standards Organization: **https://www.isao.org/information-sharing-groups/**
- Engage CISA to build a lasting partnership and collaborate on information sharing, best practices, assessments, exercises, and more.
  - SLTT organizations: **CyberLiaison_SLTT@cisa.dhs.gov**
  - Private sector organizations: **CyberLiaison_Industry@cisa.dhs.gov**

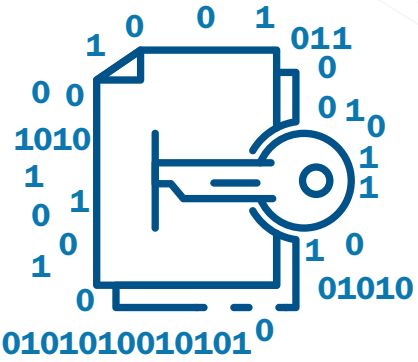
Engaging with your ISAC, ISAO, and with CISA will enable your organization to receive critical information and access to services to better manage the risk posed by ransomware and other cyber threats.

Part 1: Ransomware Prevention Best Practices

Be Prepared

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
  - Maintain regularly updated "gold images" of critical systems in the event they need to be rebuilt. This entails maintaining image "templates" that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server.
  - Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred.
    - Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
  - In addition to system images, applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.). It is more efficient to rebuild from system images, but some images will not install on different hardware or platforms correctly; having separate access to needed software will help in these cases.
- Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.
  - Review available incident response guidance, such as the *Public Power Cyber Incident Response Playbook* (**https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf**), a resource and guide to:
    - Help your organization better organize around cyber incident response, and
    - Develop a cyber incident response plan.
  - The Ransomware Response Checklist, which forms the other half of this *Ransomware Guide*, serves as an adaptable, ransomware-specific annex to organizational cyber incident response or disruption plans.



Ransomware Infection Vector: Internet-Facing Vulnerabilities and Misconfigurations

- Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface.
  - CISA offers a no-cost Vulnerability Scanning service and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.
- Regularly patch and update software and OSs to the latest available versions.
  - Prioritize timely patching of internet-facing servers—as well as software processing internet data, such as web browsers, browser plugins, and document readers—for known vulnerabilities.
- Ensure devices are properly configured and that security features are enabled. For example, disable ports and protocols that are not being used for a business purpose (e.g., Remote Desktop Protocol [RDP] – Transmission Control Protocol [TCP] Port 3389).
- Employ best practices for use of RDP and other remote desktop services. Threat actors often gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware. See CISA Alert AA20-073A, Enterprise VPN Security (**https://us-cert.cisa.gov/ncas/alerts/aa20-073a**).
  - Audit the network for systems using RDP, close unused RDP ports, enforce account lockouts after a specified number of attempts, apply multi-factor authentication (MFA), and log RDP login attempts.
- Disable or block Server Message Block (SMB) protocol outbound and remove or disable outdated versions of SMB. Threat actors use SMB to propagate malware across organizations. Based on this specific threat, organizations should consider the following actions to protect their networks:
  - Disable SMBv1 and v2 on your internal network after working to mitigate any existing dependencies (on the part of existing systems or applications) that may break when disabled.
    - Remove dependencies through upgrades and reconfiguration: Upgrade to SMBv3 (or most current version) along with SMB signing.
  - Block all versions of SMB from being accessible externally to your network by blocking TCP port 445 with related protocols on User Datagram Protocol ports 137–138 and TCP port 139.

Ransomware Infection Vector: Phishing

- Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents. Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- Implement filters at the email gateway to filter out emails with known malicious indicators, such as known malicious subject lines, and block suspicious Internet Protocol (IP) addresses at the firewall.
- To lower the chance of spoofed or modified emails from valid domains, implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed sender policy framework and Domain Keys Identified Mail protocols, adding a reporting function that allows senders and receivers to improve and monitor protection of the domain from fraudulent email.
- Consider disabling macro scripts for Microsoft Office files transmitted via email. These macros can be used to deliver ransomware.

Ransomware Infection Vector: Precursor Malware Infection

- Ensure antivirus and anti-malware software and signatures are up to date. Additionally, turn on automatic updates for both solutions. CISA recommends using a centrally managed antivirus solution. This enables detection of both "precursor" malware and ransomware.
  - A ransomware infection may be evidence of a previous, unresolved network compromise. For example, many ransomware infections are the result of existing malware infections, such as TrickBot, Dridex, or Emotet.
  - In some cases, ransomware deployment is just the last step in a network compromise and is dropped as a way to obfuscate previous post-compromise activities.
- Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.
  - Enable application directory allowlisting through Microsoft Software Restriction Policy or AppLocker.
  - Use directory allowlisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from PROGRAMFILES, PROGRAMFILES(X86), and SYSTEM32. Disallow all other locations unless an exception is granted.
- Consider implementing an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment.

CISA offers a no-cost Phishing Campaign Assessment and other no-cost assessments: **https://www.cisa.gov/cyber-resource-hub**.

For more information on DMARC, see: **https://www.cisecurity.org/blog/how-dmarc-advances-email-security/** and

https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C.pdf.

Funded by CISA, the MS-ISAC and EI-ISAC provide the Malicious Domain Blocking and Reporting (MDBR) service at no-cost to members. MDBR is a fully managed proactive security service that prevents IT systems from connecting to harmful web domains, which helps limit infections related to known malware, ransomware, phishing, and other cyber threats. To sign up for MDBR, visit: **https://www.cisecurity.org/ms-isac/services/mdbr/.**

CISA and MS-ISAC encourage SLTT organizations to consider the Albert IDS to enhance a defense-in-depth strategy. CISA funds Albert sensors deployed by the MS-ISAC, and we encourage SLTT governments to make use of them. Albert serves as an early warning capability for the Nation's SLTT governments and supports the nationwide cybersecurity situational awareness of CISA and the Federal Government. For more information regarding Albert, see: **https://www.cisecurity.org/services/albert-network-monitoring/.**

Ransomware Infection Vector: Third Parties and Managed Service Providers

- Take into consideration the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization relies on to meet its mission. MSPs have been an infection vector for ransomware impacting client organizations.
  - If a third party or MSP is responsible for maintaining and securing your organization's backups, ensure they are following the applicable best practices outlined above. Using contract language to formalize your security requirements is a best practice.
- Understand that adversaries may exploit the trusted relationships your organization has with third parties and MSPs. See CISA's APTs Targeting IT Service Provider Customers (**https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers**).
  - Adversaries may target MSPs with the goal of compromising MSP client organizations; they may use MSP network connections and access to client organizations as a key vector to propagate malware and ransomware.
  - Adversaries may spoof the identity of—or use compromised email accounts associated with—entities your organization has a trusted relationship with in order to phish your users, enabling network compromise and disclosure of information.

General Best Practices and Hardening Guidance

- Employ MFA for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
  - If you are using passwords, use strong passwords (**https://us-cert.cisa.gov/ncas/tips/ST04-002**) and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs. Threat actors often seek out privileged accounts to leverage to help saturate networks with ransomware.
  - Restrict user permissions to install and run software applications.
  - Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network.") and prevent access via an RDP session.

- Remove unnecessary accounts and groups and restrict root access.
- Control and limit local administration.
- Make use of the Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.
- Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly accessible—this includes audits of third-party access given to MSPs.

- Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365 (**https://www.us-cert.cisa.gov/ncas/alerts/aa20-120a**).
- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network (see figure 1). This is useful in steady state and can help incident responders understand where to focus their efforts.
  - The diagram should include depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or MSPs).
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.

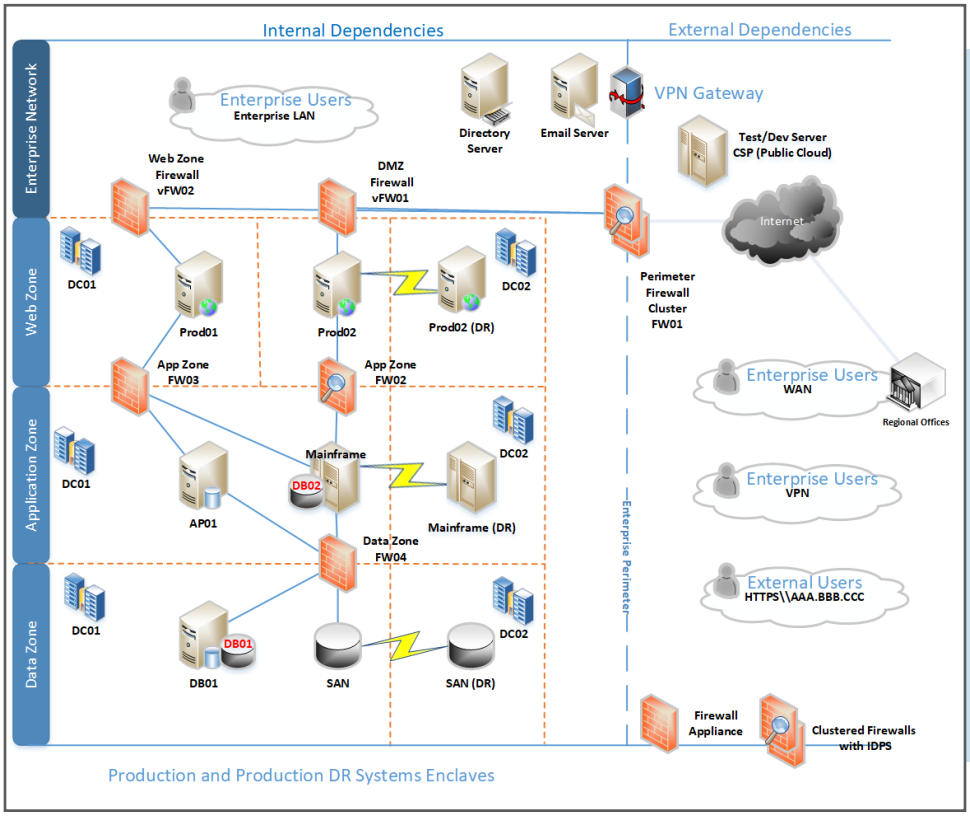


Figure 1. Example Network Diagram

This will help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors. See figures 2 and 3 for depictions of a flat (unsegmented) network and of a best practice segmented network.

- Network segmentation can be rendered ineffective if it is breached through user error or non-adherence to organizational policies (e.g., connecting removable storage media or other devices to multiple segments).

- Ensure your organization has a comprehensive asset management approach.
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware).
  - Understand which data or systems are most critical for health and safety, revenue generation, or other critical services, as well as any associated interdependencies (i.e., "critical asset or system list"). This will aid your organization in determining restoration priorities should an incident occur. Apply more comprehensive security controls or safeguards to critical assets. This requires organization-wide coordination.
  - Use the MS-ISAC Hardware and Software Asset Tracking Spreadsheet: **https://www.cisecurity.org/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet/**.

- Restrict usage of PowerShell, using Group Policy, to specific users on a case-by-case basis. Typically, only those users or administrators who manage the network or Windows OSs should be permitted to use PowerShell. Update PowerShell and enable enhanced logging. PowerShell is a cross-platform, command-line, shell and scripting language that is a component of Microsoft Windows. Threat actors use PowerShell to deploy ransomware and hide their malicious activities.
  - Update PowerShell instances to version 5.0 or later and uninstall all earlier PowerShell versions. Logs from PowerShell prior to version 5.0 are either non-existent or do not record enough detail to aid in enterprise monitoring and incident response activities.
    - PowerShell logs contain valuable data, including historical OS and registry interaction and possible tactics, techniques, and procedures of a threat actor's PowerShell use.
  - Ensure PowerShell instances (use most current version) have module, script block, and transcription logging enabled (enhanced logging).

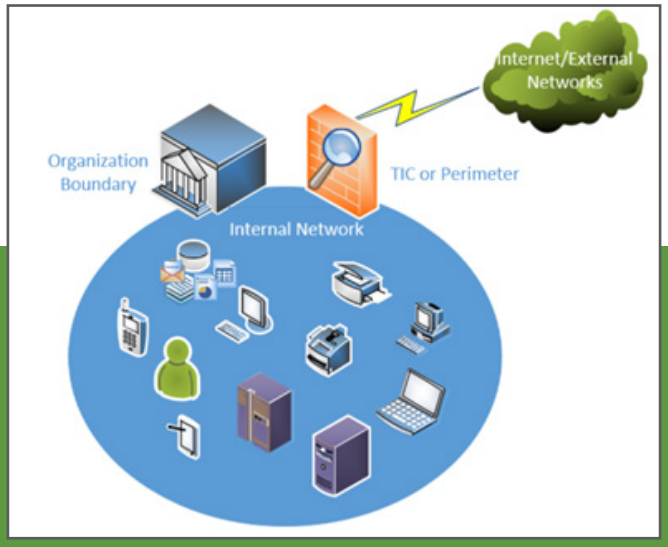


Figure 2. Flat (Unsegmented) Network

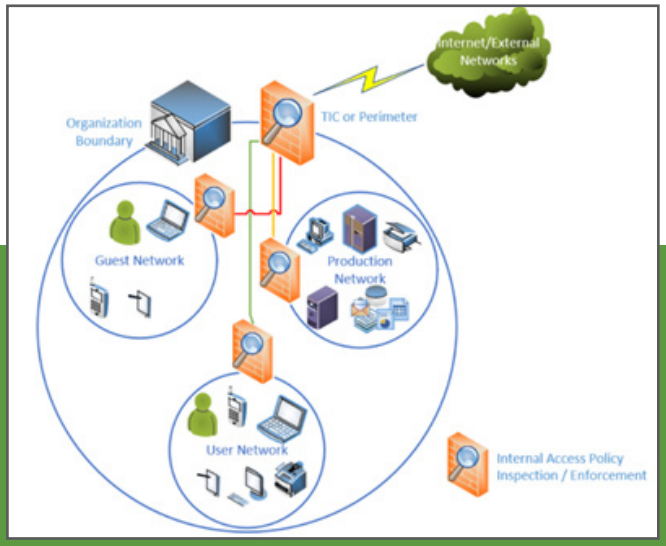


Figure 3. Segmented Network

- The two logs that record PowerShell activity are the “PowerShell” Windows Event Log and the “PowerShell Operational” Log. CISA recommends turning on these two Windows Event Logs with a retention period of 180 days. These logs should be checked on a regular basis to confirm whether the log data has been deleted or logging has been turned off. Set the storage size permitted for both logs to as large as possible.

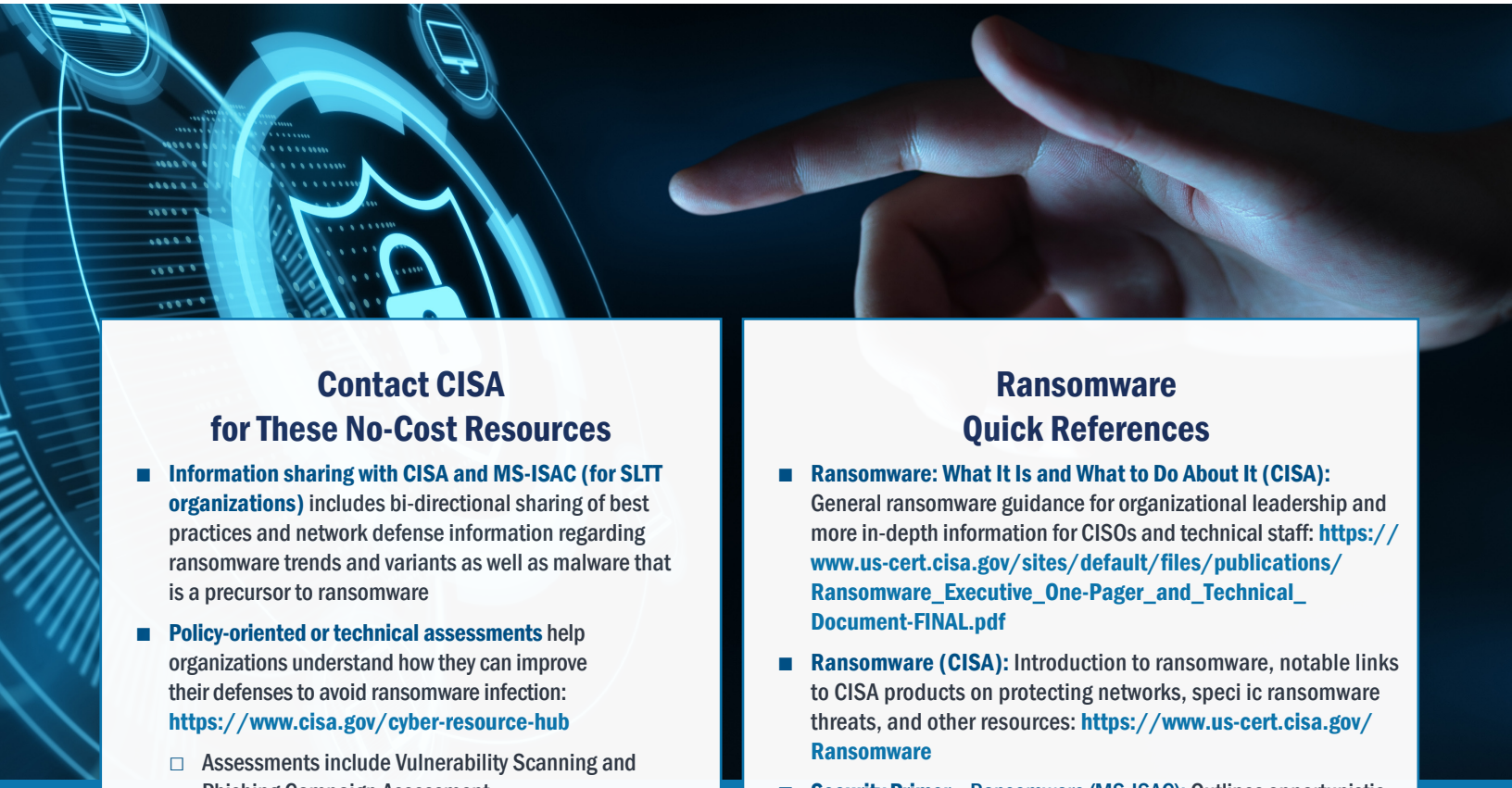
- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware network-wide.
  - The following list contains high-level suggestions on how best to secure a DC:
    - Ensure that DCs are regularly patched. This includes the application of critical patches as soon as possible.
    - Ensure the most current version of the Windows Server OS is being used on DCs. Security features are better integrated in newer versions of Windows Server OSs, including Active Directory security features. Use Active Directory configuration guides, such as those available from Microsoft (**https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory**), when configuring available security features.
    - Ensure that no additional software or agents are installed on DCs, as these can be leveraged to run arbitrary code on the system.
    - Access to DCs should be restricted to the Administrators group. Users within this group should be limited and have separate accounts used for day-to-day operations with non-administrative permissions.
    - DC host firewalls should be configured to prevent internet access. Usually, these systems do not have a valid need for direct internet access. Update servers with internet connectivity can be used to pull necessary updates in lieu of allowing internet access for DCs.
  - CISA recommends the following DC Group Policy settings:

    (Note: This is not an all-inclusive list and further steps should be taken to secure DCs within the environment.)
    - The Kerberos default protocol is recommended for authentication, but if it is not used, enable NTLM auditing to ensure that only NTLMv2 responses are being sent across the network. Measures should be taken to ensure that LM and NTLM responses are refused, if possible.
    - Enable additional protections for Local Security Authentication to prevent code injection capable of acquiring credentials from the system. Prior to enabling these protections, run audits against the lsass.exe program to ensure an understanding of the programs that will be affected by the enabling of this protection.
    - Ensure that SMB signing is required between the hosts and the DCs to prevent the use of replay attacks on the network. SMB signing should be enforced throughout the entire domain as an added protection against these attacks elsewhere in the environment.

- Retain and adequately secure logs from both network devices and local hosts. This supports triage and remediation of cybersecurity events. Logs can be analyzed to determine the impact of events and ascertain whether an incident has occurred.

- Set up centralized log management using a security information and event management tool. This enables an organization to correlate logs from both network and host security devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the organization as a whole.
- Maintain and back up logs for critical systems for a minimum of one year, if possible.

- Baseline and analyze network activity over a period of months to determine behavioral patterns so that normal, legitimate activity can be more easily distinguished from anomalous network activity (e.g., normal vs anomalous account activity).
  - Business transaction logging—such as logging activity related to specific or critical applications—is another useful source of information for behavioral analytics.



Contact CISA for These No-Cost Resources

- **Information sharing with CISA and MS-ISAC (for SLTT organizations)** includes bi-directional sharing of best practices and network defense information regarding ransomware trends and variants as well as malware that is a precursor to ransomware
- **Policy-oriented or technical assessments** help organizations understand how they can improve their defenses to avoid ransomware infection: **https://www.cisa.gov/cyber-resource-hub**
  - Assessments include Vulnerability Scanning and Phishing Campaign Assessment
- **Cyber exercises** evaluate or help develop a cyber incident response plan in the context of a ransomware incident scenario
- **CISA Cybersecurity Advisors (CSAs)** advise on best practices and connect you with CISA resources to manage cyber risk
- **Contacts:**
  - **SLTT organizations:** **CyberLiaison_SLTT@cisa.dhs.gov**
  - **Private sector organizations:** **CyberLiaison_Industry@cisa.dhs.gov**

Ransomware Quick References

- **Ransomware: What It Is and What to Do About It (CISA):** General ransomware guidance for organizational leadership and more in-depth information for CISOs and technical staff: **https://www.us-cert.cisa.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf**
- **Ransomware (CISA):** Introduction to ransomware, notable links to CISA products on protecting networks, speci ic ransomware threats, and other resources: **https://www.us-cert.cisa.gov/Ransomware**
- **Security Primer –** Ransomware (MS-ISAC): Outlines opportunistic and strategic ransomware campaigns, common infection vectors, and best practice recommendations: **https://www.cisecurity.org/white-papers/security-primer-ransomware/**
- **Ransomware: Facts, Threats, and Countermeasures (MS-ISAC):** Facts about ransomware, infection vectors, ransomware capabilities, and how to mitigate the risk of ransomware infection: **https://www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/**
- **Security Primer – Ryuk (MS-ISAC):** Overview of Ryuk ransomware, a prevalent ransomware variant in the SLTT government sector, that includes information regarding preparedness steps organizations can take to guard against infection: **https://www.cisecurity.org/white-papers/security-primer-ryuk/**

Part 2: Ransomware Response Checklist

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the following checklist. Be sure to move through the **first three steps in sequence.**

Detection and Analysis

☐ **1. Determine which systems were impacted, and immediately isolate them.**

- ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- ☐ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

☐ **2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.**

☐ **3. Triage impacted systems for restoration and recovery.**

- ☐ Identify and prioritize critical systems for restoration, and confirm the nature of data housed on impacted systems.
  - Prioritize restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.
- ☐ Keep track of systems and devices that are not perceived to be impacted so they can be deprioritized for restoration and recovery. This enables your organization to get back to business in a more efficient manner.

☐ **4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.**

☐ **5. Using the contact information below, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.**

- ☐ Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.

If extended identification or analysis is needed, CISA, MS-ISAC and local, state, or federal law enforcement may be interested in any of the following information that your organization determines it can legally share:

- ☐ Recovered executable file
- ☐ Copies of the readme file – DO NOT REMOVE the file or decryption may not be possible
- ☐ Live memory (RAM) capture from systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Images of infected systems with additional signs of compromise (use of exploit toolkits, RDP activity, additional files found locally)
- ☐ Malware samples
- ☐ Names of any other malware identified on your system
- ☐ Encrypted file samples
- ☐ Log files (Windows Event Logs from compromised systems, Firewall logs, etc.)
- ☐ Any PowerShell scripts found having executed on the systems
- ☐ Any user accounts created in Active Directory or machines added to the network during the exploitation
- ☐ Email addresses used by the attackers and any associated phishing emails
- ☐ A copy of the ransom note
- ☐ Ransom amount and whether or not the ransom was paid
- ☐ Bitcoin wallets used by the attackers
- ☐ Bitcoin wallets used to pay the ransom (if applicable)
- ☐ Copies of any communications with attackers

Remember: Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC, and federal law enforcement do not recommend paying ransom.

- ☐ Consider requesting assistance from CISA; MS-ISAC; and local, state, or federal law enforcement (e.g., Federal Bureau of Investigation [FBI], U.S. Secret Service [USSS]). See contact information below.
- ☐ As appropriate, coordinate with communications and public information personnel to ensure accurate information is shared internally with your organization and externally with the public.
- ☐ The *Public Power Cyber Incident Response Playbook* (https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf) contains guidance for organizational communication procedures as well as templates for cyber incident holding statements for public consumption. Work with your team to develop similar procedures and draft holding statements as soon as possible, as developing this documentation during an incident is not optimal. This will allow your organization to reach consensus, in advance, on what level of detail is appropriate to share within the organization and with the public, and how information will flow.

Containment and Eradication

If no initial mitigation actions appear possible:

☐ 6. Take a system image and memory capture of a sample of affected devices (e.g., workstations and servers). Additionally, collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise (e.g., suspected command and control IP addresses, suspicious registry entries, or other relevant files detected). The contacts below may be able to assist you in performing these tasks.

- ☐ Take care to preserve evidence that is highly volatile in nature—or limited in retention—to prevent loss or tampering (e.g., system memory, Windows Security logs, data in firewall log buffers).

☐ 7. Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants.

To continue taking steps to contain and mitigate the incident:

☐ 8. Research the trusted guidance (i.e., published by sources such as government, MS-ISAC, reputable security vendor, etc.) for the particular ransomware variant and follow any additional recommended steps to identify and contain systems or networks that are confirmed to be impacted.

- ☐ Kill or disable the execution of known ransomware binaries; this will minimize damage and impact to your systems. Delete other known, associated registry values and files.

☐ 9. Identify the systems and accounts involved in the initial breach. This can include email accounts.

☐ 10. Based on the breach or compromise details determined above, contain any associated systems that may be used for further or continued unauthorized access. Breaches often involve mass credential exfiltration. Securing the network and other information sources from continued credential-based unauthorized access may include the following actions:

- ☐ Disabling virtual private networks, remote access servers, single sign-on resources, and cloud-based or other public-facing assets.

☐ 11. Additional suggested actions—server-side data encryption quick-identification steps:

- ☐ In the event you learn that server-side data is being encrypted by an infected workstation, quick-identification steps are to:

  1. Review Computer Management > Sessions and Open Files lists on associated servers to determine the user or system accessing those files.

  2. Review file properties of encrypted files or ransom notes to identify specific users that may be associated with file ownership.

  3. Review the TerminalServices-RemoteConnectionManager event log to check for successful RDP network connections.

  4. Review the Windows Security log, SMB event logs, and any related logs that may identify significant authentication or access events.

  5. Run Wireshark on the impacted server with a filter to identify IP addresses involved in actively writing or renaming files (e.g., "smb2.filename contains cryptxxx").

☐ 12. Conduct an examination of existing organizational detection or prevention systems (antivirus, Endpoint Detection & Response, IDS, Intrusion Prevention System, etc.) and logs. Doing so can highlight evidence of additional systems or malware involved in earlier stages of the attack.

Upon voluntary request, CISA and MS-ISAC can assist with analysis (e.g., phishing emails, storage media, logs, malware) at no cost to support your organization in understanding the root cause of an incident, even in the event additional remote assistance is not requested:

- CISA – Advanced Malware Analysis Center: **https://www.malware.us-cert.gov/MalwareSubmission/pages/submission.jsf**
- MS-ISAC – Malicious Code Analysis Platform (SLTT organizations only): **https://www.cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/**
  - ☐ Scans a suspicious file or Uniform Resource Locator (URL) against several antivirus vendors to determine if it matches known malicious signatures
  - ☐ Runs a file or URL in a sandbox to analyze behavior
  - ☐ Provides a user with a summary report of malware behavior, including files accessed, tasks created, outbound connections, and other behavioral traits
  - ☐ Users can opt to keep submissions private and make direct requests for assistance from MS-ISAC; users can also mark submissions for sharing with CISA
  - ☐ Email: **mcap@cisecurity.org** to set up an account
- Remote Assistance – Request via CISA Central or MS-ISAC Security Operations Center (see contact information below)

- ☐ Look for evidence of precursor "dropper" malware. A ransomware event may be evidence of a previous, unresolved network compromise. Many ransomware infections are the result of existing malware infections such as TrickBot, Dridex, or Emotet.
  - Operators of these advanced malware variants will often sell access to a network. Malicious actors will sometimes use this access to exfiltrate data and then threaten to release the data publicly before ransoming the network in an attempt to further extort the victim and pressure them into paying.
  - Malicious actors often drop manually deployed ransomware variants on a network to obfuscate their post-compromise activity. Care must be taken to identify such dropper malware before rebuilding from backups to prevent continuing compromise.

☐ 13. Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.

- ☐ Outside-in persistence may include authenticated access to external systems via rogue accounts, backdoors on perimeter systems, exploitation of external vulnerabilities, etc.
- ☐ Inside-out persistence may include malware implants on the internal network or a variety of living-off-the-land style modifications (e.g., use of commercial penetration testing tools like Cobalt Strike; use of PsTools suite, including PsExec, to remotely install and control malware and gather information regarding—or perform remote management of—Windows systems; use of PowerShell scripts).
- ☐ Identification may involve deployment of endpoint detection and response solutions, audits of local and domain accounts, examination of data found in centralized logging systems, or deeper forensic analysis of specific systems once movement within the environment has been mapped out.

☐ 14. Rebuild systems based on a prioritization of critical services (e.g., health and safety or revenue generating services), using pre-configured standard images, if possible.

☐ 15. Once the environment has been fully cleaned and rebuilt (including any associated impacted accounts and the removal or remediation of malicious persistence mechanisms) issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility. This can include applying patches, upgrading software, and taking other security precautions not previously taken.

☐ 16. Based on established criteria, which may include taking the steps above or seeking outside assistance, the designated IT or IT security authority declares the ransomware incident over.

Recovery and Post-Incident Activity

☐ 17. Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.

- ☐ Take care not to re-infect clean systems during recovery. For example, if a new Virtual Local Area Network has been created for recovery purposes, ensure only clean systems are added to it.

☐ 18. Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.

☐ 19. Consider sharing lessons learned and relevant indicators of compromise with CISA or your sector ISAC/ISAO for further sharing and to benefit others within the community.

Contact Information

Consider filling out the following contact information for ready use should your organization become a victim of a ransomware incident. Consider contacting these organizations for mitigation and response assistance or for purpose of notification.

State and Local Response Contacts:		
Contact	**24x7 Contact Information**	**Roles and Responsibilities**
IT/IT Security Team - Centralized Cyber Incident Reporting		
Departmental or Elected Leaders		
State and Local Law Enforcement		
Fusion Center		
Managed/Security Service Providers		
Cyber Insurance		

Federal Asset Response Contacts

Upon voluntary request, federal asset response includes providing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents while identifying other entities that may be at risk, assessing potential risks to the sector or region, facilitating information sharing and operational coordination, and providing guidance on how to best use federal resources and capabilities.

What You Can Expect:

- Specific guidance to help evaluate and remediate ransomware incidents
- Remote assistance to identify the extent of the compromise and recommendations for appropriate containment and mitigation strategies (dependent on specific ransomware variant)
- Phishing email, storage media, log and malware analysis, based on voluntary submission (full-disk forensics can be performed on an as-needed basis)
- Contacts:
  - CISA:
    - **https://us-cert.cisa.gov/report**, **Central@cisa.gov** or (888) 282-0870
    - Cybersecurity Advisor (**https://www.cisa.gov/cisa-regions**): [Enter your local CISA CSA's phone number and email address.]
  - MS-ISAC:
    - **soc@msisac.org** or (866) 787-4722

Federal Threat Response Contacts

Upon voluntary request, federal threat response includes law enforcement and national security investigative activity: collecting evidence and intelligence, providing attribution, linking related incidents, identifying additional affected entities, identifying threat pursuit and disruption opportunities, developing and executing action to mitigate the immediate threat, and facilitating information sharing and operational coordination with asset response.

What You Can Expect:

- Assistance in conducting a criminal investigation, which may involve collecting incident artifacts, to include system images and malware samples.
- Contacts:
  - FBI:
    - **https://www.fbi.gov/contact-us/field-offices**
    - [Enter your local FBI field office POC phone number and email address.]
  - USSS:
    - **https://www.secretservice.gov/contact/field-offices/**
    - [Enter your local USSS field office POC phone number and email address.]

DEFEND TODAY,
SECURE TOMORROW

CISA.GOV

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®