RANSOMWARE: EXTORTING ORGANIZATIONS IN THE FINANCIAL SECTOR AND BEYOND

Digital Security
Progress. Protected.

Author: **Ondrej Kubovič**
Contributor: **Phil Muncaster**
March 2023

Table of Contents

Introduction

Ransomware is a number one cyber-threat to organizations operating in many verticals. But, according to the G7, it is "one of the most significant challenges that financial entities currently face"– posing potentially "unacceptable risk" to the sector.

Why? Because firms in the financial sector are a top target for threat actors. Even mid-tier banks are perceived either to be flush with cash themselves, or a valuable repository of personal customer and account information. It's no coincidence that 95% of attacks on the sector last year were financially motivated. For a cybercrime economy fueled by the profit motive, it just makes good business sense for avaricious threat actors to target financial institutions.

They are doing so with gusto. While overall ransomware detections dropped between 2021 and 2022, in financial services they rose by 41%, according to one estimate. The same report also cites a 55% year-on-year increase in malicious intrusion attempts in the sector. A separate study claims that the finance vertical is in the top three for extortion-based attacks.

Being a persistently popular target for cyber-criminals is taking its toll on many US financial institutions. Modern ransomware actors usually employ "double extortion" tactics, whereby data is stolen before a ransomware payload is delivered to encrypt data. Either of those alone would be enough to cause significant financial and reputational damage. Together they can be catastrophic – potentially leading to class action lawsuits from breached customers, regulatory fines, punitive IT consulting fees, downtime and customer churn.

Nearly three-quarters (73%) of financial services organizations say their company suffered significant revenue losses following a successful ransomware attack, while over a fifth (23%) claim these attacks have led to layoffs. Some ransomware actors are even asking for details of their victims' insurance policy in order to optimize their demands. According to IBM, financial services has the second highest breach costs, averaging nearly $6m per incident, whereas the average across verticals is $4.4m. Around a quarter of these costs accrue several years after the initial breach, highlighting a "long tail" of negative financial impacts.

ON THE FRONT FOOT

It should come as no surprise why many banks are struggling to manage the surging risk of ransomware. Complex heterogeneous IT environments often mix legacy with more modern, cloud-based systems. Siloed data creates security coverage gaps which threat actors are only too willing to exploit. Technical debt accrued from historic M&A activity may also create security blind spots and extra risk. That's not to mention the relatively new risks stemming from hybrid working. The top infection vector in the sector last year was spear phishing attachments, used in 53% of attacks.

However, help is at hand. ESET has designed this report with your business in mind. It picks apart the ransomware threat so you can better understand the threat, how it works, and where IT infrastructure is likely to be targeted. Most importantly, we offer some step-by-step defense strategies – to help you protect systems in the first instance, but then also rapidly detect and respond. This means that if any threats sneak through, it's possible to minimize their impact.

Ransomware is on the rise in the financial sector. But it doesn't need to pose an unmanageable risk.

Introductory note

Please note that this is an updated version of the white paper Ransomware: A look at the criminal art of malicious code, pressure, and manipulation *originally written in August 2021. This new version contains some recent insights covering the finance sector and provides some recent statistics from both ESET telemetry and external resources.*

The previous version was based on the fundamental contribution made by Stephen Cobb in 2018 as well as contributions by author's colleagues Rene Holt, James Shepperd, Nick FitzGerald, Hana Matušková, and Klára Kobáková.

Huge business and a cyberthreat at its worst

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 is probably one of the most serious cyberthreats your organization might face. Why? Because in the past few years criminal gangs creating this type of malware and running ransomware as a service have been improving a different, more targeted approach to these kinds of attacks — for which metrics are still hard to obtain.

Cybercriminals are also coming up with new approaches to ensure that they receive the sum they ask for, usually by increasing the pressure on the victim. In 2019, they started to rely on double extortion, which combines the "usual" data encryption with data exfiltration. In this way, they not only prevented access to the victim's valuable, critical, or otherwise sensitive files, but could also leak or sell them to other malicious actors. Double extortion remains the most used scheme to compromise an organization which could afford to pay ransom up until today.

Upping the ante further, some ransomware operators have adopted triple extortion, adding the further step of contacting business partners or customers of victims that have not paid the ransom demand.

The cybercriminals inform the victim's partners or customers that their sensitive data has been accessed as part of the ransomware attack, suggesting these partners or customers pressure the ransomware victim to pay up to prevent this data being released. In some cases, the attackers even demand payment from these partners or customers.

Recent years have seen a shift away from victimizing large numbers of random people while requesting ransom demands of modest sums, toward a targeted approach making much larger ransom demands from a smaller victim pool. That group features deeper pockets and members who can ill afford to lose access to their data or control over it. Another recent, slowly emerging trend is the "big shame ransomware" that stands for an incident where "an attacker threatens to leak sensitive data without encrypting it". Reputational damage can be caused by spreading such shame even via social media – and targeting large organizations without exception.

No one really knows how much ransomware operators make, as the circumstances and details are usually not publicly disclosed. According to Palo Alto Networks, the average ransomware payment during the first five months of 2022 reached $925,162, "approaching the unprecedented $1 million mark as they rose 71%" compared to 2021.

Latest IBM's Cost of a Data Breach Report 2022 showed that "the average cost of a ransomware attack—not including the cost of the ransom itself—went down slightly, from USD 4.62 million in 2021 to USD 4.54 million in 2022."

According to one recent report on crypto crime, the total sum extorted from victims in 2022 reached $456.8 million. Another report on data breaches shows that "ransomware accounted for 25% of breaches" in 2021. When speaking about losses from ransomware, the FBI's Internet Crime Complaint Center (IC3) identified that these reached "more than $34.3 million" in 2022. According to the same report, finance sector remains in the top five sectors victimized by ransomware.

There are several notable cases in history when a large amount of ransom was paid. Researchers also add that the most brazen groups usually ask for tens of millions of dollars — Sodinokibi (aka REvil), for instance, demanded $50 million apiece from Acer and Quanta back in 2021. Other sums worth mentioning include:

$144 million from 2013–2019 in payouts to Ryuk, according to the FBI;

$40 million in 2021 paid to Phoenix Locker by CNA Financial — the highest reported single payout yet;

$17.5 million in 2021 paid to Darkside before "retreating" after the Colonial Pipeline attack;

$70 million in 2021 demanded by Sodinokibi for a universal decryptor after the Kaseya VSA attack;

$50 million in 2022 demanded by Lockbit for stolen data from German giant Continental;

$100 million hauled in by Hive in 2022.

How ransomware does it psychologically

Ransomware uses pressure as its core tactic, and while there are many approaches to ransomware, the primary threat it demonstrates is encrypting sensitive and valuable data and putting it out of the victim's reach.

Pressure points expand when individuals or organizations can sustain reputational damage, business outages, or even legal and financial penalties. The risk of such damage has been exacerbated by doxing employed by multiple ransomware gangs, wherein they comb through their victims' systems looking for sensitive data that they will then threaten to release unless an additional fee on top of the ransom is paid — a type of double extortion. The Maze gang, which started the doxing trend back in November 2019, even improved on its original approach by creating its own underground leak site, making it very difficult for the victims to have their leaked data taken down.

With the pressure applied and — as a rule increasing, manipulation is sure to follow. Victims often see multiple facets of their digital touchpoints affected, from DDoS attacks on their websites to obnoxious demonstrations of criminal presence on a network. Some of these include shock-inducing approaches like print bombing, in which multiple printers on a network are commanded to print a ransom note — threatening management's ability to control internal and external communication about an incident. Pressure might also be applied more directly; for example by accessing a business's customer data and

then getting in touch, possibly even cold-calling the victims, with further threats and publicly goading the victims while their IT departments struggle to mitigate impacts from an attack. The attackers may use various methods to contact the victim, such as phone calls, emails, or instant messaging. This is an aggressive tactic, as it directly targets the victim and puts additional pressure on them to pay the ransom.

These are just some of the calling cards that accompany today's ransomware campaigns. Simply put, ransomware can turn an unfortunate malware incident into psychological warfare that aims to force victims to act against their own will and best interest. While criminals involved in physical abductions typically start their pressure campaigns with some ace up their sleeves but can run short on options later, cybercriminals have an even wider variety of methods they can pursue to gain leverage and crush any hope of seamless recovery.

To achieve their malicious aims, cybercriminals use a vast number of approaches that potentially allow them to gain remote access, monitor their victims' activities, and then apply surgical, pinpoint pressure. This demonstrates how much power they can achieve over their victims' data, networks, business continuity, and reputation. Indeed, these attacks don't have to come via custom malware, zero-day exploits, or long-term persistence campaigns. They can simply be the result of poor security practices by employees, poor configuration of RDP or other remote access tools, or gaps in practices and processes, within both organization and service providers, or other gaps in the supply chain.

How ransomware does it technically

While ransomware has been a nuisance for more than a decade, the scope for ransomware has expanded throughout the period of digital intensification brought by the COVID-19 pandemic. A clear correlation rapidly emerged between COVID-19 lockdowns and phishing emails that were often based on topical fears of negative business impacts and lost opportunities.

Another manifestation of this phenomenon was employees suddenly working from home and (often for the first time) accessing internal company systems and services via Remote Desktop Protocol (RDP). This became a wildly popular vector to deliver ransomware. With the admin rights that accompany some cases of RDP use, ransomware can appear alongside a number of other security concerns in a network.

We can also see that wielding ransomware as a tool for digital crime is very much a game of ambition and scale. Less skilled actors can dabble, coding imperfect malicious scripts that will impact a very limited number of victims via spam. Others may try their luck by propagating malicious payloads — including ransomware — via downloaders or botnets. More ambitious actors may pay a fee to use a fully tuned ransomware product and deploy it to earn profit for themselves, becoming affiliates of the ransomware developers through a ransomware as a service (RaaS) business model.

Advanced criminal actors running the RaaS schemes often leverage vulnerabilities to gain access to a machine, then move laterally to a server and on-to the wider network, only later deciding on the use of ransomware. If resource rich, these gangs may purchase zero-day exploits or even develop their own, allowing them to bypass many types of proactive mitigation technologies. Finally, whether through luck, skill, or significant investments of human and financial resources, attackers can conduct supply chain attacks to access entire IT ecosystems. For example, by commandeering popular managed service provider (MSP) platforms and productivity tools, threat actors can unleash ransomware across multiple networks (and thus organizations) at scale. Leveraging a supply-chain attack to position ransomware is yet another fearsome scenario for businesses to contend with.

An appreciation for the ever-growing variety of approaches and speed with which ransomware can evolve is critical to understanding the security posture necessary to avoid business outages. Innovation in ransomware moves quickly; case in point is when researchers observed Sodinokibi (aka REvil) ransomware demonstrating file encryption within a PC's Safe Mode that flew under the radar yet required additional user login. Within a month, this novel capability had been improved by changing the login password to the attacker's choice and configuring the PC to automatically reboot and log into Safe Mode, making it a viable vector for a full-scale campaign.

Network-attached storage (NAS) devices, which are commonly used to share files and make backups, have also earned the attention of ransomware gangs. In 2021, the NAS appliance maker QNAP alerted its customers that eCh0raix ransomware was attacking its NAS devices, especially those with weak passwords. The eCh0raix continued targeting vulnerable NAS devices also in 2022, although berely reaching the peak of its activity from the end of January that year. Also ESET telemetry from the last third of 2022 showed that NAS devices remained interesting for the ransomware scene.

Generally speaking, the year-over-year detection trend for ransomware attacks was considerably more dynamic, dropping by 20% between 2021 and 2022. Several factors could have contributed, including increased international law enforcement cooperation and activity, disruptions caused by the war in Ukraine, and increased regulation limiting ransom payments and thus diminishing the financial return for the attackers.

Affecting the infrastructure

RANSOMWARE VIA RDP

An RDP endpoint is a Windows device that is running Remote Desktop Protocol (RDP) software so that it can be accessed over a network, such as the internet. RDP enables an organization's Windows devices to be accessed remotely as if their keyboards and displays were on your desk. The benefits of deploying RDP can be several, from managing or troubleshooting employee devices to serving up centralized resources such as desktops that can run heavy workloads, applications, or databases.

Company systems that employees need to access remotely must have RDP enabled, and ideally, mandate platform access via two-factor authentication (2FA). Employees then connect to these systems by running RDP 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 remote system (the default port for RDP is 3389, although that can be changed). The remote system presents a login screen that asks for a username and password. You can see what this looks like on a Windows system in *Figure 1*.

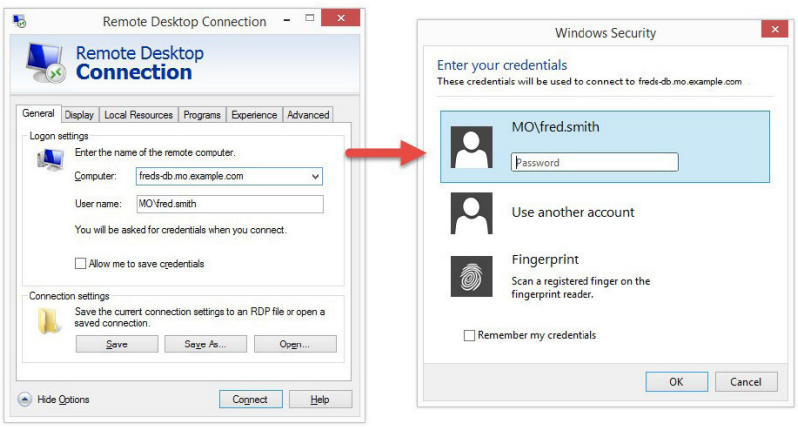


Figure 1 RDP login screen

There are two main ways in which organizations use RDP:

1. The first is to manage programs running on a server; for example a website or back-end database. In this scenario, the simplest configuration has a system administrator open port 3389 to the outside world to allow remote management.

2. A second use of RDP is to allow remote access to corporate desktops or virtual machines that have access to resources not accessible outside the corporate network. Accessing such systems via RDP means there is no need to directly open sensitive internal servers to the internet. It may also be that desktops in the office have extra processing power needed for many processes or have expensive specialist software needed for staff to complete some (or in some cases most) of their tasks. Again, when this is done over the internet, often port 3389 is opened to the outside world.

For the criminally inclined, finding systems accessible from the outside world and then abusing them for malicious purposes is straightforward because:

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

Systems 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 March 27, 2023, Shodan indicated that there were nearly 4 million systems on the internet with port 3389 open (registration may be required to view filtered Shodan queries). As you can see from the Shodan interface in *Figure 2*, over 1 million of those systems were in the US.

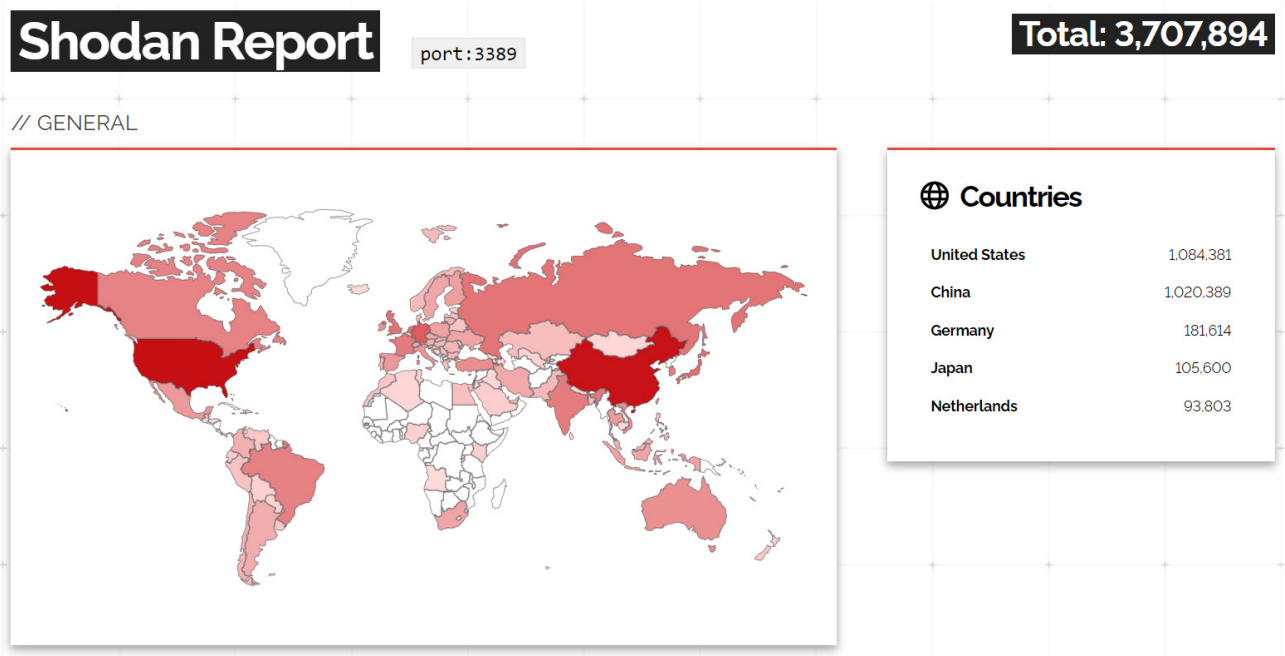


Figure 2 Nearly 4 million systems on the internet using port 3389 (Source: Shodan Report, port 3389)

Using a different query, over 3.1 million machines were found to be explicitly running RDP. For an attacker, all of these machines are potential targets to be explored. While logging in to an RDP system typically requires a username and password, these can be surprisingly easy for attackers to guess and many will lead to success.

One shortcut for attackers who have sufficient funding is to simply purchase access to compromised RDP systems. Such credentials are available in marketplaces on the dark web. Note that ransomware is not the only reason for buying hacked RDP credentials. Other uses for a compromised RDP system include 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.

If only username and password are required to remotely access the device, then an attacker, having identified such endpoint as a target, can make repeated attempts to guess these credentials. Doing so at a high rate, via use of a database of plausible credentials, is referred to as brute-force attack. Absent any mechanism to limit multiple bad guesses, such attacks can be very effective and even lead to a network- wide compromise.

ESET telemetry shows that the number of detections reached almost 300 billion in 2021 which stands for the highest figures yet.

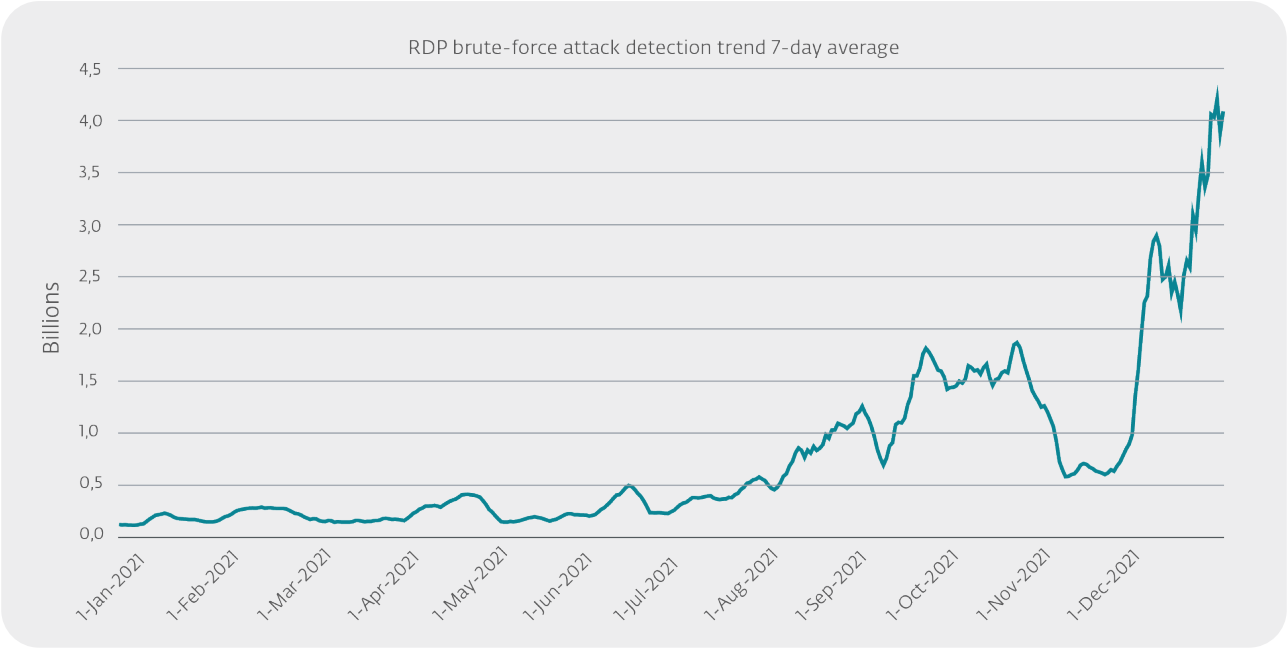


Figure 3 Trend of RDP connection attempts in 2021, seven-day moving average. (Source: ESET telemetry)

However, there was a sharp drop in January 2022, and the detections continued dropping ever since.

Gaining unauthorized access from the internet to devices running RDP may require more upfront effort than email-based ransomware, but the RDP vector offers threat actors significant benefits, like misuse of legitimate access, the potential to evade endpoint protections, and the ability to rapidly compromise multiple systems — or even the whole network — within a single organization.

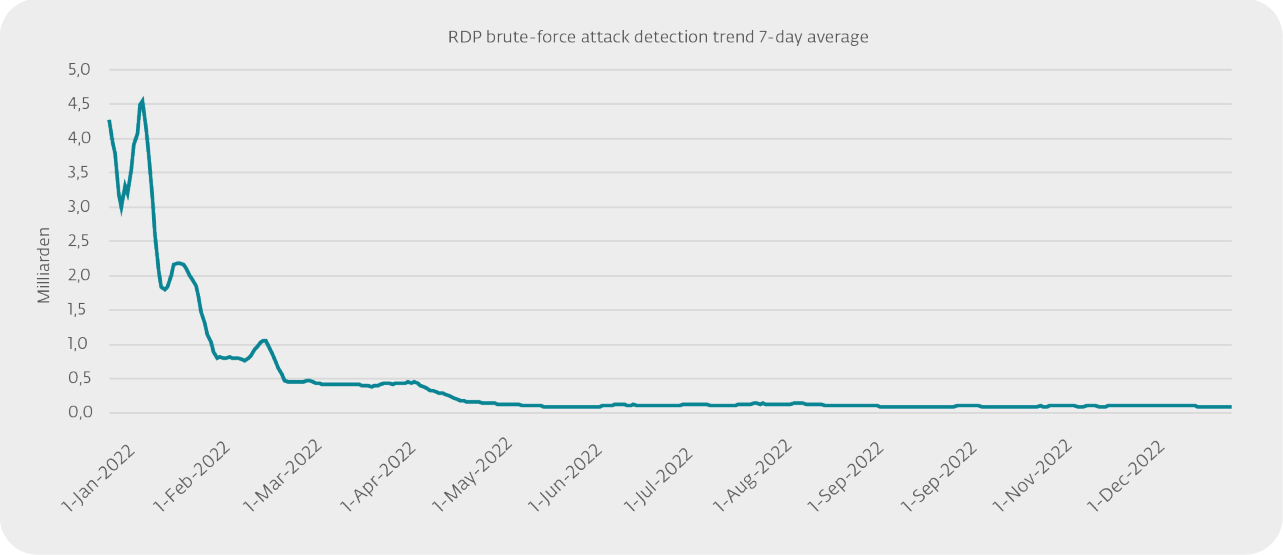


Figure 4 Trend of RDP connection attempts in 2022, seven-day moving average. (Source: ESET telemetry)

"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 malicious websites propagating ransomware. However, if an attacker with system administrator privileges on a compromised server turns off the endpoint protection software before deploying their ransomware, that attack may well elude typical malware metrics.

Lateral movement and living off the land

For the ransomware attacker, a compromised RDP system can mean much more than extorting money to decrypt the files on that machine. That's especially true if that system can provide an entry point to an entire network of devices, potentially enabling large-scale encryption or theft 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 try to 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 in the following text 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, often used by the system's actual administrators, and even standard tools installed with the base operating system, to extend network penetration. For example, PsExec and Windows Management Instrumentation Command-line (WMIC) are often misused 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. For more information on how to detect them see the discussion of endpoint detection and response (EDR) tools below.

The term lateral movement is used to describe the strategy of gaining a foothold on one system and using that to compromise other devices that can be reached from there. For example, attackers can utilize compromised credentials to target a server not even present in the targeted organization and use its connection to the main infrastructure to deliver the ransomware payload.

In addition to living off the land, ransomware attacks may take advantage of unpatched vulnerabilities in legitimate system software. Perhaps one of the most archetypal examples was WannaCryptor ransomware, which propagated via EternalBlue exploit, misusing high-severity vulnerability in Microsoft's implementation of Server Message Block. Despite patches having been publicly available for approximately two months prior to the WannaCryptor campaign on May 12, 2017, attackers still found and compromised over 200,000 vulnerable machines. Even in the latter stages of this outbreak, infected devices continued to pose threats as, for example, users may have unknowingly brought compromised laptops into what admins felt to be a secure perimeter.

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 stealing data, encrypting and ransoming the files used by that one asset. However, a lot can be gained via persistence, so many ransomware operators are likely to continue to perform recon even after the data has been stolen and before encrypting it — just to make sure they have enough leverage.

Defending against RDP ransomware attacks

It is possible to defend systems running RDP against unauthorized access and thus deny criminals this attack vector—which is not as popular as it used to be in previous years, although password guessing remains the most prevalent intrusion 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 the section "Securing RDP against ransomware."

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 MFA (multi-factor authentication), limited to specific roles, on specific systems that are configured securely, patched promptly, monitored constantly, firewalled appropriately, and backed up regularly.

However, even if you have such rules in place or are working toward 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 make an inventory of 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 that the organization's security staff were not aware of 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.

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, require long passwords for the accounts that will have such access. How long? Passwords of 15 characters or more may seem prohibitively long but are easily remembered if passphrases are used, and passwords that length need not have complexity rules, which research shows tend to push people into poor password practices. After setting stringent password length requirements on the accounts, determine whether or not it is feasible to limit those systems to the internal network and access them remotely 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 MFA so that you are not relying on passwords alone for protection. However, be sure to use an MFA 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 MFA has been used for many years to confirm banking transactions).

If you are forced to rely on passwords because MFA is not available — possibly due to short-sighted budgetary policy — at least stop would-be intruders making repeated attempts to guess credentials. Set a threshold of three invalid login attempts, after which no login attempts are recognized for a set period of time; for example, three minutes. In Figure 5 you can see what this looks like in Windows.

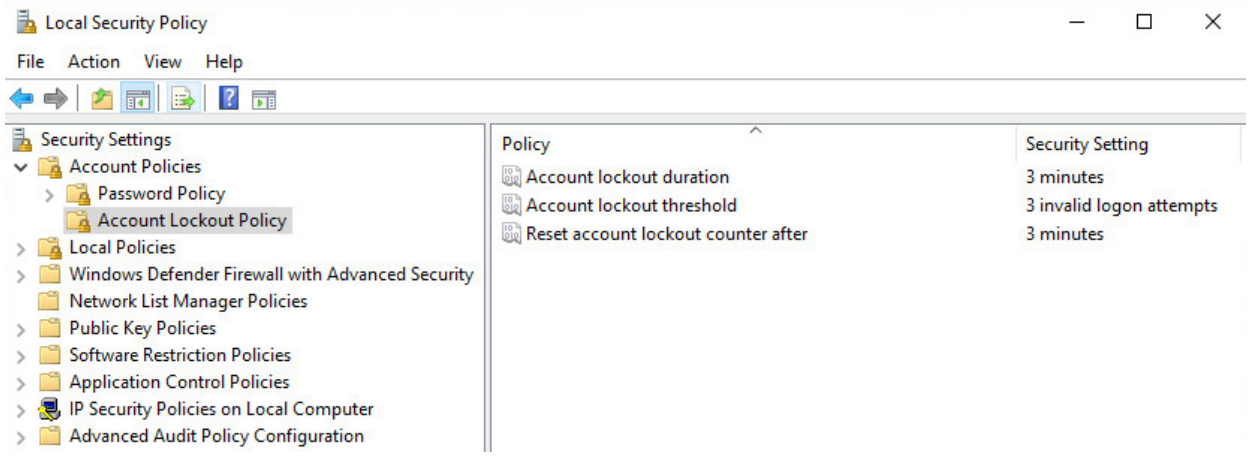


Figure 5 Account lockout policy

You can also change the RDP listening port from 3389 to something else to make accessible machines slightly 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 the section "Securing RDP against ransomware" for more details).

Hardening and patching should be performed for all remotely accessible devices. 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, which are sometimes used by malware.

You can also use AppLocker to control which apps and files employees can run on their machines. Of course, the last line of defence 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 three more vectors, email, supply-chain, and vulnerabilities are considered.

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 with securing 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 directly from the internet unless they have been approved for use in that manner and configured appropriately. Question why access to the asset cannot be provided via VPN. Disable RDP whenever it is not required (these articles show how on different versions of Microsoft Windows: Server 2019; Server 2016; Server 2008/R2; Windows 10; Windows 8; Windows 7).

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 password to the user account you are connecting to on the remote machine regularly. Make sure that you change the default password that is sometimes automatically generated for cloud instances.

b. Enforce password complexity (a long passphrase containing 15+ characters with no phrases related to the business, product names, or users is mandatory).

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 – three invalid attempts with three-minute lockout durations are reasonable choices.

d. Test and deploy patches for all known vulnerabilities and make sure that the most obvious culprits, such as BlueKeep and EternalBlue, are among the fixed flaws. If a computer cannot be patched, plan for its timely replacement.

e. Use Network Level Authentication to enhance Remote Desktop Session Host security by requiring that the user be authenticated to the Remote Desktop Session Host server before a session is created.

f. 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 value (WARNING: do not try this unless you are familiar with the Windows Registry and TCP/IP): HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber.

g. 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.

h. Use more than one authentication factor. There are three possibilities: things you know, like usernames and passwords; things you are, like fingerprint or voiceprint; something you have, like your phone, which can receive a one-time passcode or run an authenticator app to generate one for you.

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 MFA solutions that leverage the ubiquity of phones but do not communicate via SMS (such as ESET Secure Authentication).

i. 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).

j. To access servers, use unique passwords for local accounts with admin rights (e.g., by using LAPS or a robust password manager service). In addition, restrict server access rights to a limited group of users. This reduces the attack surface of servers by limiting the number of users that can access them.

k. Set the RDP client connection's encryption level to "high," if possible. If not, use the highest encryption level available for connections.

l. Install a VPN gateway to broker all RDP connections from outside your local network.

m. 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).

n. Enable exploitation blocking in endpoint security software, which is a non-signature-based anomaly detection technology that monitors the behavior of commonly targeted applications.

o. Isolate any insecure computer that needs to be accessed from the internet using RDP.

p. If all staff and vendors are in the same country, or among a short list of countries, consider blocking access from excluded countries by instituting GeoIP blocking at the VPN gateway in order to prevent connections from foreign attackers.

RANSOMWARE VIA EMAIL

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 malware that serves as the initial stage of a compromise, which ends with ransomware.

They may use this vector to deliver downloaders that install malware 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 steal valuable data and encrypt files throughout the organization, prior to making a very large ransom demand, as is often the case of targeted ransomware attacks via RDP.

In particular, email is one of the primary vectors for botnets, such as Trickbot, Qbot, and Dridex, which commonly use Microsoft Office documents with malicious macros for initial intrusion and ransomware as the final payload. Some of the previously seen relations between botnet and ransomware families include Emotet with Qbot, Trickbot, Ryuk, and Conti; Dridex with FriedEx (aka BitPaymer); Nemucod with Avaddon, Dridex, Ursnif, and Trickbot; and SmokeLoader and Zloader with LockBit and Crysis.

Law enforcement took down Emotet at the start of the year 2021, which consequently saw a very strong decline of downloaders being spread via email. We describe the impacts of Emotet's campaigns, both before and after its takedown, in the T1 2021 ESET Threat Report, in the Q4 2020 ESET Threat Report, and in the Q3 2020 ESET Threat Report.

Despite the significant decline of downloaders, malicious actors using compromised macros remained the top email threat in 2021. January even saw a spike of emails delivering malicious Office documents that led to Dridex and Emotet downloaders.

Another popular botnet, Trickbot, faced a disruption in October 2020, yet it seems to have been only a temporary setback, as its operators launched a new phishing campaign as early as January 2021 aimed at legal and insurance companies in North America. It seems that further efforts will be necessary in the future to dispose of Trickbot for good.

Protecting against ransomware via email

When it comes to protecting your organization against ransomware attacks via email, the first line of defence 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 expect to receive via email; 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 need to adopt a secure file sharing solution or collaboration framework first, and transition staff to using that before being able to rigorously implement stricter email attachment filtering.

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 from visiting 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 endpoint 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 cloud component ESET LiveGuard Advanced.

You can find best practices to configure your system to protect against ransomware here.

Prompt and comprehensive patching of operating systems and applications will help to prevent ransomware entering via email attachments or drive-by downloads. 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 on the threat scape. As stated in 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 defences.

RANSOMWARE VIA THE SUPPLY CHAIN

A ransomware attack vector that warrants close attention these days is the software supply chain. 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.

In 2017 ESET discovered that a legitimate accounting software 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 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 what became the most devastating cyberattack in history. The first line of defense against this type of attack is a good endpoint protection product, backed up by EDR tools.

Thus, due to the complex impacts and mitigations these attacks can unleash and subsequently require, researchers and security admins are on the lookout. July 2, 2021 saw a set of events transpire with Kaseya's IT management software for MSPs that demonstrated the characteristics of a supply-chain ransomware attack leveraging the Win32/Filecoder.Sodinokibi.N trojan. Subsequent investigation has shown that the incident was based on exploitation of a zero-day vulnerability, yet the supply-chain label elicited a quick reaction. Kaseya, for its part, has rushed to triage the incident and pushed out notifications to those potentially affected with the advice to shut potentially affected on-premises VSA servers down immediately.

The growing intensity of supply-chain attacks is also documented by the number of published ESET research articles where this attack vector was used. Between November 2020 and February 2021 there were four supply-chain attack cases discovered exclusively by ESET — a very high number compared to previous years.

Defending against this type of attack involves keeping up with patches, using endpoint protection software, leveraging EDR solutions, and educating users about unsolicited emails that encourage them to visit unfamiliar websites.

RANSOMWARE VIA EXPLOITING VULNERABILITIES

While cybercriminals can benefit from both known and unknown vulnerabilities, laying hands on zero-day vulnerabilities generally belongs to the world of APT groups and state-sponsored actors. Despite the threat of zero days, known vulnerabilities provide more than enough headache for security admins, researchers, and business owners alike.

Case in point is the fact that almost all cybersecurity vendors still detect the EternalBlue exploit (2017) and its many variants, as well as ongoing exploitation based on Microsoft's SMBv1 file-sharing protocol. The long shelf life of the vulnerabilities and threats like WannaCryptor (aka WannaCry) usually trace to poor updates and patch management at businesses and institutions.

In parallel, the increasing complexity of the threatscape has yielded new tools to fight more modern threats, but these too come with additional technical burdens — looking out for product vulnerabilities and pursuing careful patch management.

The huge rise in use of, and dependence on, VPNs in business and for personal use stands out. Here, two cases spring to mind where vulnerabilities identified in Pulse Secure's and Fortinet's VPN services allowed for the proliferation of ransomware among customers. The use of VPN at large institutions and businesses, while highly effective, adds an additional responsibility with regard to updating the product as required. This focus on timely updates should be pursued with employment of multi-factor authentication when signing in to their respective VPN services. Where suspicions of credential abuse arise, organizations should pursue comprehensive account resets.

These challenges are also echoed in the global upsurge in use of large productivity and collaboration platforms. In March 2021, a frenzy of activity erupted among threat actors, leading software vendors, and the wider cybersecurity industry when it was discovered that Microsoft rushed out emergency updates to address four zero-day flaws affecting Microsoft Exchange Server versions 2013, 2016, and 2019. Subsequently, threat actors were observed exploiting the vulnerabilities in the wild to access on-premises Exchange servers, which allowed them to steal emails, download data, and compromise machines with malware for long-term access to the victim networks.

This large-scale event ultimately saw Exchange servers under siege from at least 10 APT groups. ESET researchers' thoughts quickly turned to understanding how many organizations would have been probed and infiltrated for future attacks including ransomware. The likely mechanism? With a foothold on a Microsoft Exchange server, attackers would have very privileged access to a company — possibly admin rights — and then, in time, plan an upcoming attack.

As previously mentioned in the section on supply-chain attacks above, the Kaseya VSA ransomware attack affected over 50 MSPs with impacts on over 1,000 end customers. The attackers used a number of zero-day vulnerabilities — including CVE-2021-30116 — to compromise the Kaseya VSA IT

management software, a popular tool among MSPs. The attackers claimed to have hit over a million systems, which could an exaggeration. ESET telemetry revealed victims in 17 countries, including the United Kingdom, South Africa, Canada, Germany, and the United States.

While the early indications of Kaseya's troubles being a supply-chain attack were not borne out, a zero-day attack of this sort is very serious and indeed did produce downstream supply chain effects. In short due to the popularity of Kaseya systems, impacts were recorded to businesses only tangentially connected to their VSA platform for MSPs. As of July 2, Scandinavian supermarket chain Coop took steps to shut down approximately 500 stores due to the fact that the third-party payment processor and supplier of their checkout/POS system was based on Kaseya-hosted systems. So, while Coop was not directly affected, it was still significantly impacted through its dependence on another service that was shut down due to the Kaseya attack.

IT Admins, CISOs, and C-suite managers should have taken notice at the scale and impact of both the Microsoft Exchange and Kaseya incidents, to refresh their focus on both the threat environment and business impact that ransomware can have. For further reference, please see some of the most frequently mentioned vulnerabilities in public reports:

- **Kaseya VSA**
- **Pulse Connect Secure**
- **Citrix Hypervisor**
- **Fortinet VPN**
- Microsoft Exchange Server — See the featured story in one of our **threat reports.**
- **Citrix Application Delivery Controller and Gateway**
- **Microsoft Office Common Controls**
- **Windows Win32k**
- **Accellion File Transfer Appliance**

Ransomware defense strategies

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, possibly impacting all of your company's operations. 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?"

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. 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. 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

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 from getting into your organization — or if it does get in, reduce the damage it can do.

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 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 is a vital defense mechanism and crucial for your recovery efforts.

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 of 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.

These days there are more options than ever for backup and recovery, notably cloud storage, whether remote, on-premises, 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. Ransomware simply adds to the long list of reasons your organization should not skimp on this part of the IT program. However, 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.

To avoid ransomware from traversing it, opt for off-site storage that:

- 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; and
- protects the customer by spelling out the provider's legal/contractual responsibilities, what happens if the provider goes out of business, and so on.

Don't underestimate the usefulness of write-once media for archiving data too. 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.

EXTENDED DETECTION AND RESPONSE

There is one category of security software that can help limit the impact of ransomware attacks andstrengthen your response to them: extended detection and response tools, or XDR for brevity. Either as a collection of internally developed tools or an integrated security product, XDR can be used to assist manual threat-hunting efforts on your networks as well as automate a wide range of defensive measures.

XDR is an evolution of EDR, which optimizes threat detection, investigation, response, and hunting in real time. XDR unifies security relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation. XDR uses behavioral analytics across endpoint, network, cloud, email, and other layers to spot suspicious activity and stop attackers before they can make an impact.

In *Figure 6*, you can see several ransomware-related XDR rules designed to alert security personnel to suspicious activity (this particular XDR is ESET Inspect).

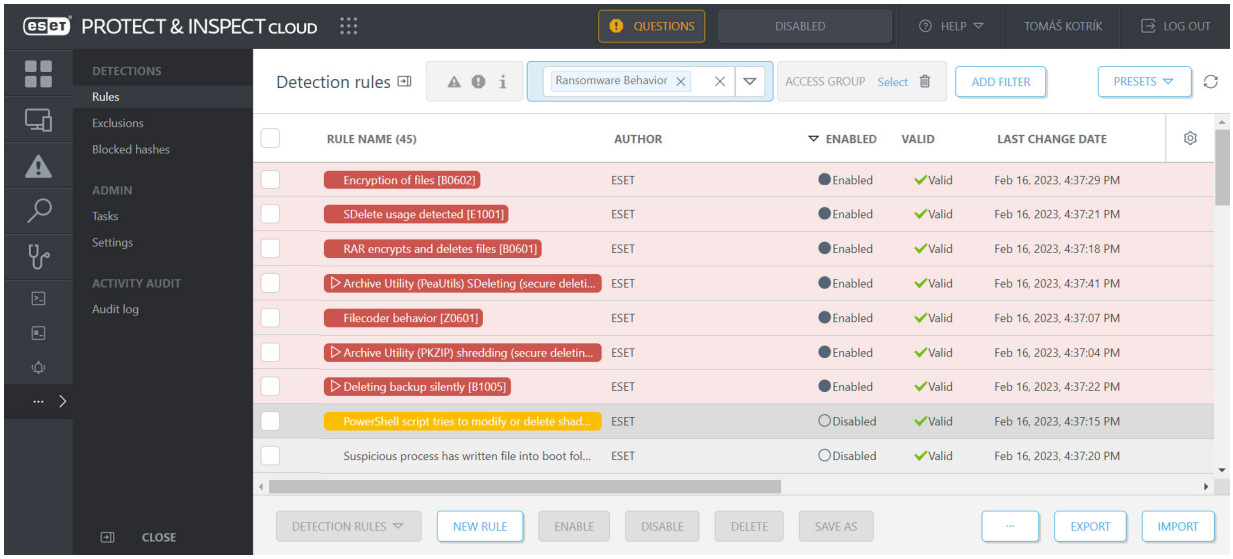


Figure 6 PROTECT & INSPECT Cloud console with some of the ransomware-related rules

An XDR tool can monitor all of your organization's endpoints for anomalous and suspicious activity, like the changing of file extensions typically seen in a ransomware attack. Your security team would definitely like to be alerted to the presence of attack tools like Mimikatz, created to steal user credentials from memory, or Cobalt Strike beacon, often used by attackers to establish a foothold in the system and remotely execute commands.

Early warning signs of intrusion can be coded into rules and alarms. These can be continually refined with fresh data from threat intelligence sources such as lists of indicators of compromise (IoC). A good XDR 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 XDR can increase your security team's ability to thwart attacks, respond to attacks, and perform forensic analysis after an attack.

MANAGED DETECTION AND RESPONSE

MDR is an outsourced version of extended detection and response (XDR), sometimes combined with other tools. Many organizations are turning to MDR—a type of managed security service combining tools, technologies, and cybersecurity experts. While XDR requires the organization to do the monitoring, detection, and response, with MDR, a trusted cybersecurity provider takes care of the heavy lifting—freeing in-house staff to focus on high-value tasks elsewhere.

The benefits of outsourcing detection and response are simple but compelling:

- The MDR provider takes care of all management of the back-end technology, freeing up staff to focus on high-value, strategic tasks rather than drowning in alerts
- The MDR provider may also optimize and manage the backend technology to align with each customer's risk profile and infrastructure
- With detection and response managed by a third party, there will be no need to pay hefty salaries to attract and retain the best SOC talent
- Customers can benefit from their provider's economies of scale, ability to attract the best talent, and insight into other customer organizations and threat environments

THREAT INTELLIGENCE (TI)

According to IDC, threat intelligence (TI) has become a crucial part of the XDR solutions, while standing for a unique tool enhancing prevention and detection in cybersecurity. Speaking about the prevention, TI allows vendors to "find adversarial tactics in the wild or profile what has been exploited." Having the upper hand in this matter "can help populate firewalls or other malware-based detection systems" and therefore anticipate risks. What is crucial to detection is that if there are indicators of compromise (IoC), threat intelligence helps vendors correlate these IoCs "with the threats, tactics, and procedures (TTPs) of the adversary".

There are three main reasons why financial organizations should consider integrating TI feeds into their systems.

OVERCOME INFORMATION OVERLOAD

Ransomware, zero-days, advanced persistent threats, targeted attacks and botnets are all concerns for businesses around the world. The problem is that, due to the volume of different threats, organizations are unable to easily understand which proactive defenses and mitigations are the most important. This ultimately leads to organizations scrambling to try and find meaningful information among limited data sets, such as their own networks, or the extremely large datasets that they find via external sources.

Threat intelligence services help sift through the information overload and provide the most relevant information for specific organizations. Threat intelligence services allow organizations to prioritize emerging threats quickly and easily, which leaves them more time to proactively implement new defenses against them.

FIGHT THREATS PROACTIVELY

Today's cybersecurity landscape is constantly evolving with new attack methods and never before seen threats. When an attack or data breach occurs, organizations are typically surprised that their defenses were compromised, or are completely unaware that the attack even happened. After the attack is finally discovered, organizations rush to reactively implement mitigations to stop this attack from being repeated.

However, this does not protect them from the next attack that might use a brand new vector. Threat intelligence services provide insight on future business risks and unknown threats, which allow organizations to improve the effectiveness of their defenses and implement a proactive cybersecurity posture.

By providing information on the threat actor, attack vectors and indicators of compromise, security teams can reduce incident response time by getting the full picture of the attack and what to look for.

ACCELERATE INCIDENT RESPONSE

When a data breach occurs, security teams typically need to figure out how the incident happened, as well as identify which devices were affected. This process is usually a very long and manual process as engineers sift through their network searching for abnormalities which might indicate that the network was compromised.

Threat intelligence services allow incident response teams to fully understand and quickly respond to data breaches. By providing information on the threat actor, malware behavior, attack vectors and indicators of compromise, security teams can reduce incident response time by understanding the full picture of the attack as well as what to look for.

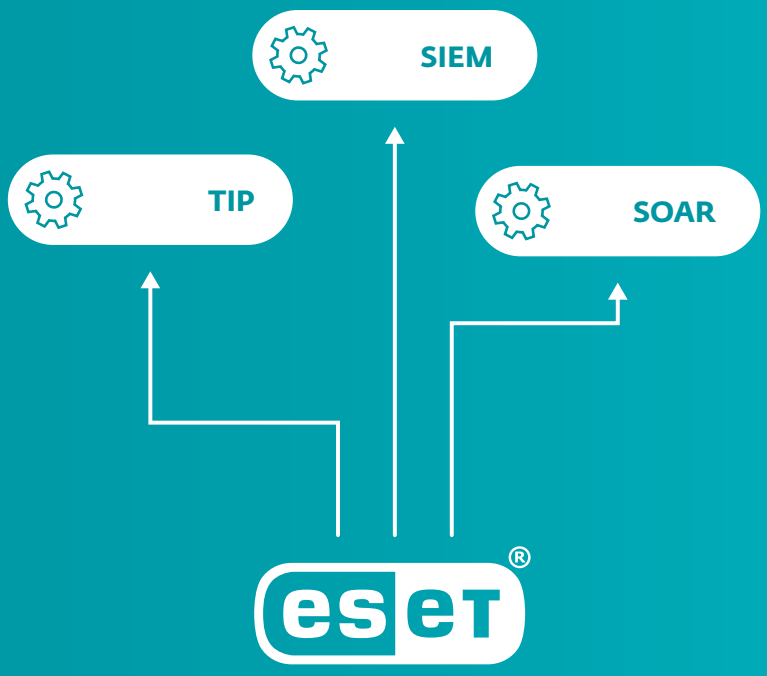
WHAT EXACTLY IS ESET THREAT INTELLIGENCE (ETI)?

ESET's Threat Intelligence service provides global knowledge, gathered by ESET experts, on targeted attacks, advanced persistent threats (APTs), zero-days and botnet activities.

Informed by ESET intelligence feeds, organizations can improve their proactive security posture and enhance their threat hunting and remediation capabilities. ESET's feeds are highly curated and provided several times a day; they are deduplicated, disambiguated, containing only fresh and prevalent IoCs - and delivered with confidence scoring.

ESET's APT Reports package includes in-depth technical reports describing recent campaigns, toolsets and related subjects, providing a very high level of context, and monthly summary overviews ideal for C-level audience. In addition, every customer ordering the APT Reports PREMIUM package will have access to an ESET analyst. This provides an opportunity to discuss topics in greater detail and help resolve any outstanding issues.

ESET threat intelligence can be integrated into company's system
Integrating ESET telemetry is simple and will enrich your TIP, SIEM or SOAR. We have a comprehensive API with full documentation and we supply data in standardized formats, such as JSON and STIX feeds via TAXII, so that integration into any tool is possible. For IBM QRadar, Anomali, and Logpoint we have step-by-step integration manuals for fast and easy implementation – and we're continually adding others.



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 ransom 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.
- What steps are the organization obliged to take in case of a data breach?
- What is company policy on powering down affected machines? Who makes this call? Powering down machines eliminates potential evidence stored in memory and may be considered as not compliant with regulations.

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 Disaster Recovery, Incident/Crisis Response plans are prepared in case of a ransomware attack. Here's an outline of the ground your response plan needs to cover:

- At first signs of attack, notify designated personnel
- Isolate and analyze affected machines
- Powering down: If isolating affected machines is not possible, take a system image and memory capture, then power them down to avoid further spread of the ransomware attack
- Once the attack is confirmed, activate your 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 (e.g., if a key is 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 your business continuity plan
- Collect relevant logs and possible indicators of compromise, such as binaries, ransom demand notes, IP addresses, registry entries, or other files
- Document the initial investigation of the attack and the steps taken to remediate it

It is a good idea to have at least one ransomware scenario in your crisis planning playbook and to go through it in a tabletop 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).

NEVER PAY THE RANSOM

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 further criminal activity
- You are allowing ransomware gangs to research zero-day vulnerabilities and develop new exploits
- You may be hit with future attacks and further demands for money
- 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:
- Some of the data might have been corrupted in the encryption process and is thus not recoverable
- The provided decrypting tool might be bundled with other malware, does not work properly, or is much slower than recovery from backups
- 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 exist but are incomplete or damaged in some way. However, there may be alternatives to paying up. So before you decide to send the money, check with your security software vendor (a) in case this is one of the rare situations where a decryption tool is available, making recovery possible without paying

the ransom, and (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 common 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, the probability of being attacked again after the first payment — after all, you are not dealing with law-abiding citizens — and that you are supporting a criminal exercise and thus making further attacks on others more likely as well.

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. Suppose the attackers have you send them an encrypted file that 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 and, should any personally identifiable information be contained in that data, likely committed an offense under one or more of the burgeoning set of tightened national and regional privacy laws.

Also, bear in mind that removing active ransomware with security software 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 often part of the malware. In other words, if you decide to pay, proceed with caution.

Conclusion

Some of the highest profile ransomware groups make tens of millions of dollars from their efforts – supported by a cybercrime economy that delivers all the tools and services they need to launch successful attacks. These are determined, highly skilled criminal enterprises, with the agility to rebrand and retool when they come under too much scrutiny from law enforcers and government agents. Although law enforcement efforts are improving, the only guaranteed way to stop the ransomware pandemic is if it becomes no longer profitable to engage in attacks.

In the first instance, financial institutions should try to resist the urge to pay their extorters. It has been calculated that just half of those who do pay up get all their data back, and there's still no way of knowing if stolen information will be sold on to fraudsters. Ransomware is also changing, with some experts warning of a growing trend for destructive attacks, which will change the risk calculus again for banks. Russia's invasion of Ukraine may also see a surging threat to this critical infrastructure sector from state-backed or linked groups.

What does this mean for US banks? That they should expand efforts to protect, detect and respond to ransomware threats, using resources like this and partners like ESET to guide them. But it should also encourage the financial sector as a whole to improve the sharing of threat intelligence, via existing networks like Information Sharing and Analysis Centers.

Ransomware actors are past masters at collaborating to achieve their goals. It's time industry players took the same approach, to defend their own interests.

Protect your enterprise against ransomware.

LEARN MORE

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to deliver comprehensive, multilayered protection against cybersecurity threats for businesses and consumers worldwide.

ESET has long pioneered machine learning and cloud technologies that prevent, detect and respond to malware. ESET is a privately owned company that promotes scientific research and development worldwide.

Digital Security
Progress. Protected.