RANSOMWARE WHITE PAPER // 2018 // Author: Stephen Cobb

TLP: WHITE

RANSOMWARE:
an enterprise perspective

Digital Security
Progress. Protected.

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

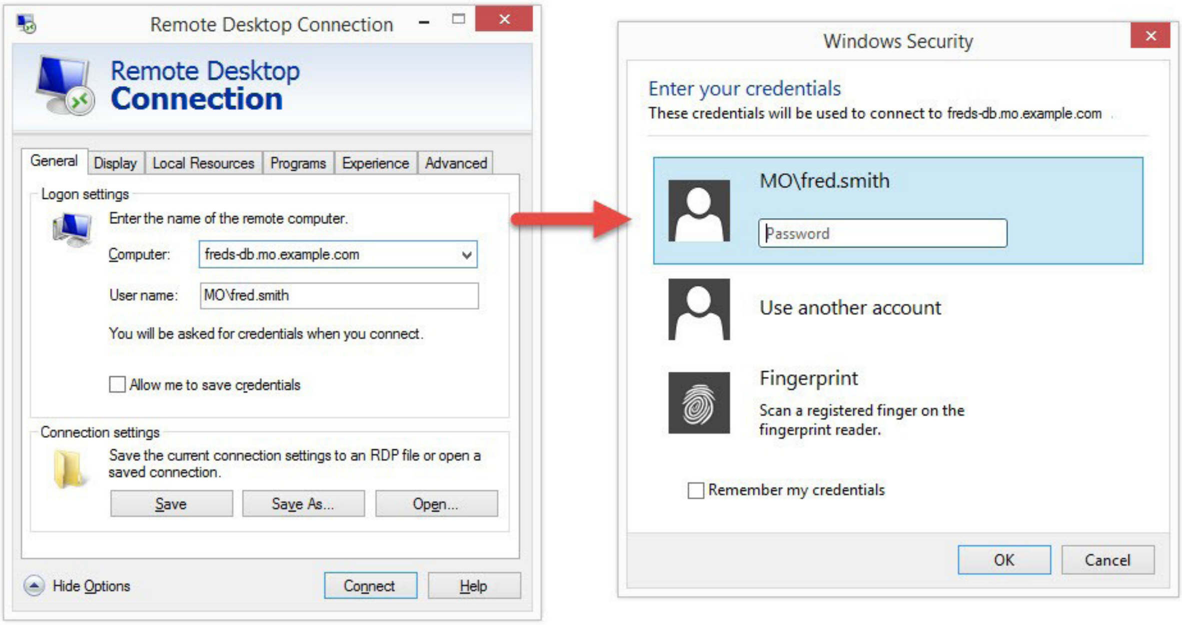
An RDP endpoint is a device, such as a database server, that is running Remote Desktop Protocol (RDP) software so that the device can be accessed over a network, such as the internet. If a user name and password are required to access the device then an attacker, having identified the server as a target, 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.



Enter the name of the remote computer.

Computer: freds-db.mo.example.com

User name: MO\fred.smith

You will be asked for credentials when you connect.

□ Allow me to save credentials

Save the current connection settings to an RDP file or open a saved connection.

Enter your credentials

These credentials will be used to connect to freds-db.mo.example.com

MO\fred.smith

Password

Use another account

Fingerprint

Scan a registered finger on the fingerprint reader.

□ Remember my credentials

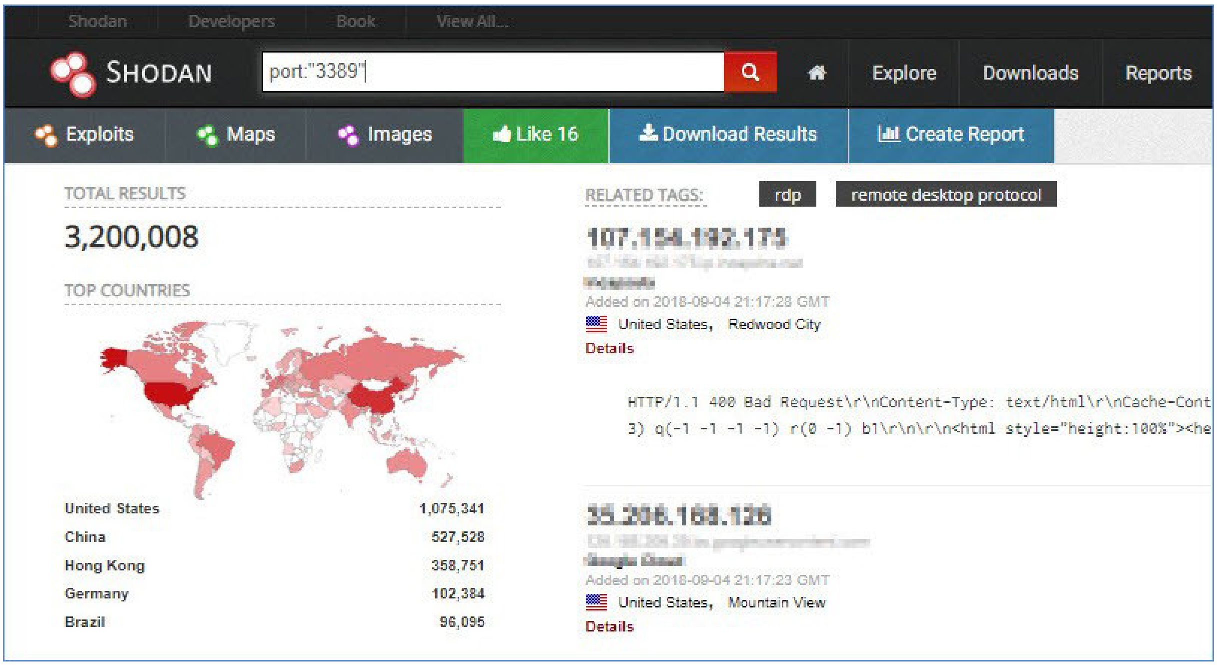
Figure 1.

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.



TOTAL RESULTS

3,200,008

TOP COUNTRIES

United States	1,075,341
China	527,528
Hong Kong	358,751
Germany	102,384
Brazil	96,095

RELATED TAGS: rdp remote desktop protocol

[redacted]

Added on 2018-09-04 21:17:28 GMT

United States, Redwood City

Details

```
HTTP/1.1 400 Bad Request\r\nContent-Type: text/html\r\nCache-Cont
3) q(-1 -1 -1 -1) r(0 -1) b1\r\n\r\n<html style="height:100%"><he
```

[redacted]

Added on 2018-09-04 21:17:23 GMT

United States, Mountain View

Details

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.

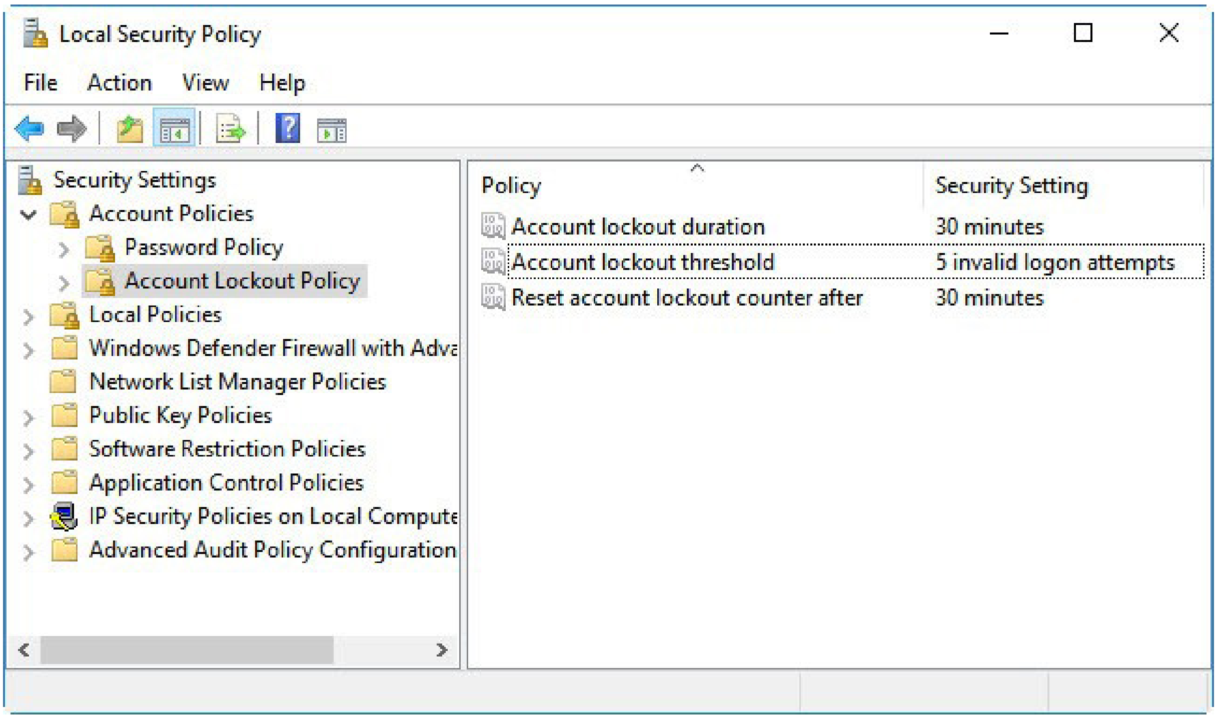
Case study: The CDOT Cyber Incident

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.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Account lockout duration	30 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

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.

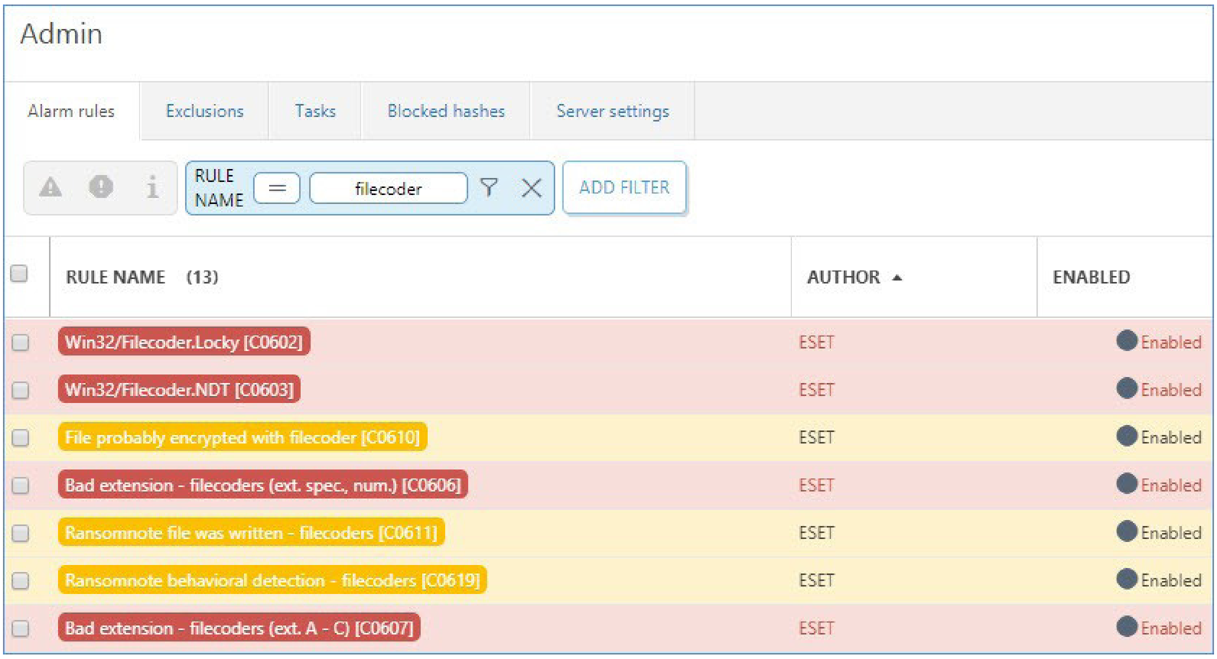
You will also want to make sure your Incident/Crisis Response Plan is ready in case of a ransomware attack. Here's an outline of the ground that your response plan needs to cover:

- 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*).



□	RULE NAME (13)	AUTHOR ▲	ENABLED
□	Win32/Filecoder.Locky [C0602]	ESET	● Enabled
□	Win32/Filecoder.NDT [C0603]	ESET	● Enabled
□	File probably encrypted with filecoder [C0610]	ESET	● Enabled
□	Bad extension - filecoders (ext. spec., num.) [C0606]	ESET	● Enabled
□	Ransomnote file was written - filecoders [C0611]	ESET	● Enabled
□	Ransomnote behavioral detection - filecoders [C0619]	ESET	● Enabled
□	Bad extension - filecoders (ext. A - C) [C0607]	ESET	● Enabled

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.

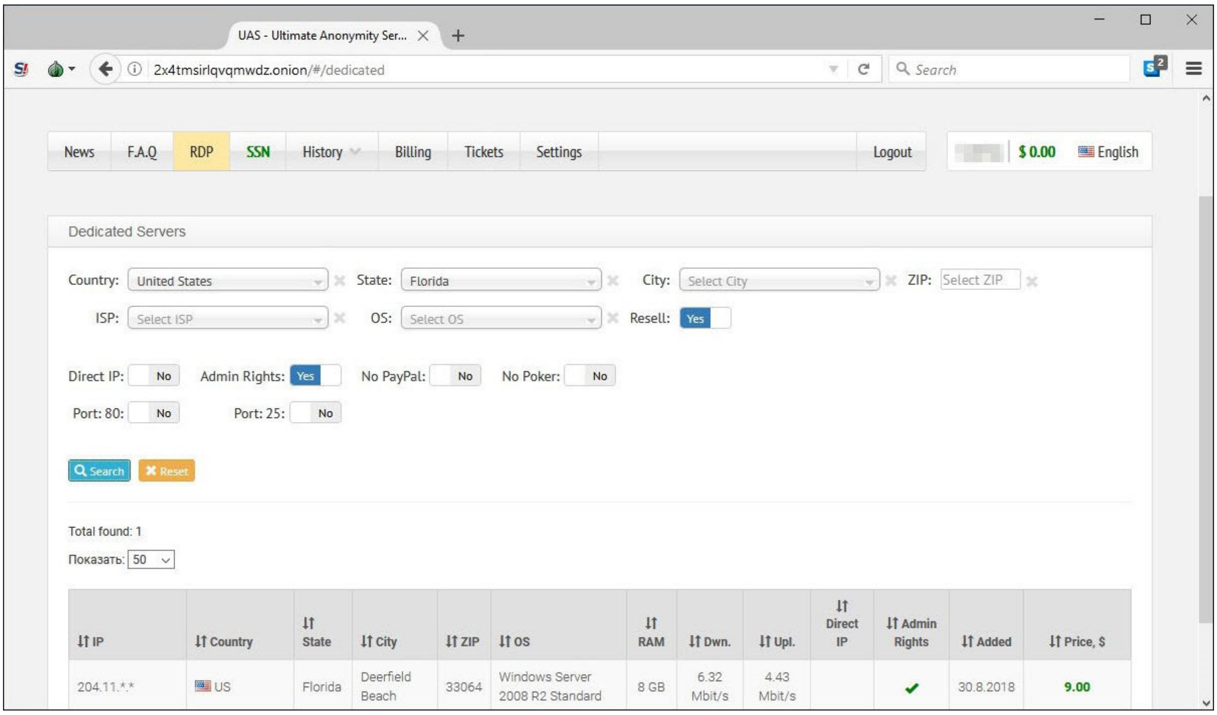
Gaining the upper hand in this struggle begins with understanding the attackers and attack vectors. Naturally, these evolve over time, but in a cumulative manner. The fact that criminal abuse of computing resources to mine cryptocurrency has surged recently does not mean that there is a shortage of criminals 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:



Dedicated Servers

Country: United States State: Florida City: Select City ZIP: Select ZIP

ISP: Select ISP OS: Select OS Resell: Yes

Direct IP: No Admin Rights: Yes No PayPal: No No Poker: No

Port: 80: No Port: 25: No

Total found: 1

Показать: 50

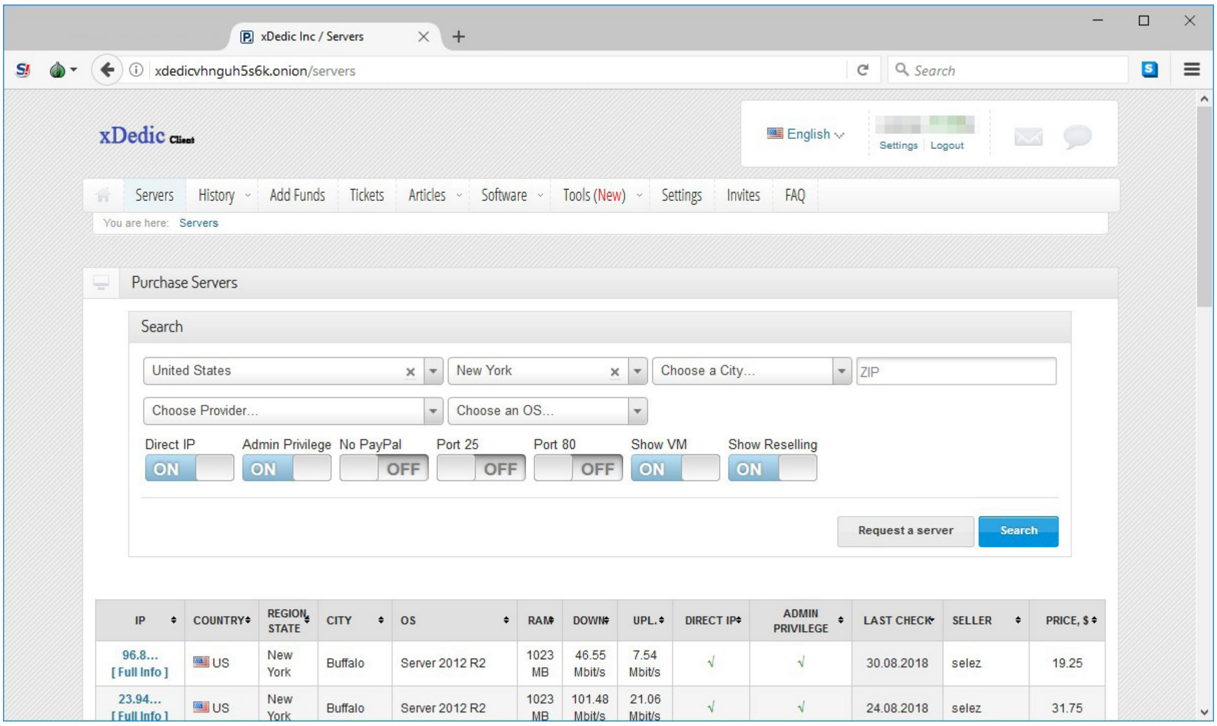
IP	Country	State	City	ZIP	OS	RAM	Dwn.	Upl.	Direct IP	Admin Rights	Added	Price, $
204.11.*.*	US	Florida	Deerfield Beach	33064	Windows Server 2008 R2 Standard	8 GB	6.32 Mbit/s	4.43 Mbit/s		✓	30.8.2018	9.00

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:



[redacted]

Search

United States × | New York × | Choose a City... | ZIP

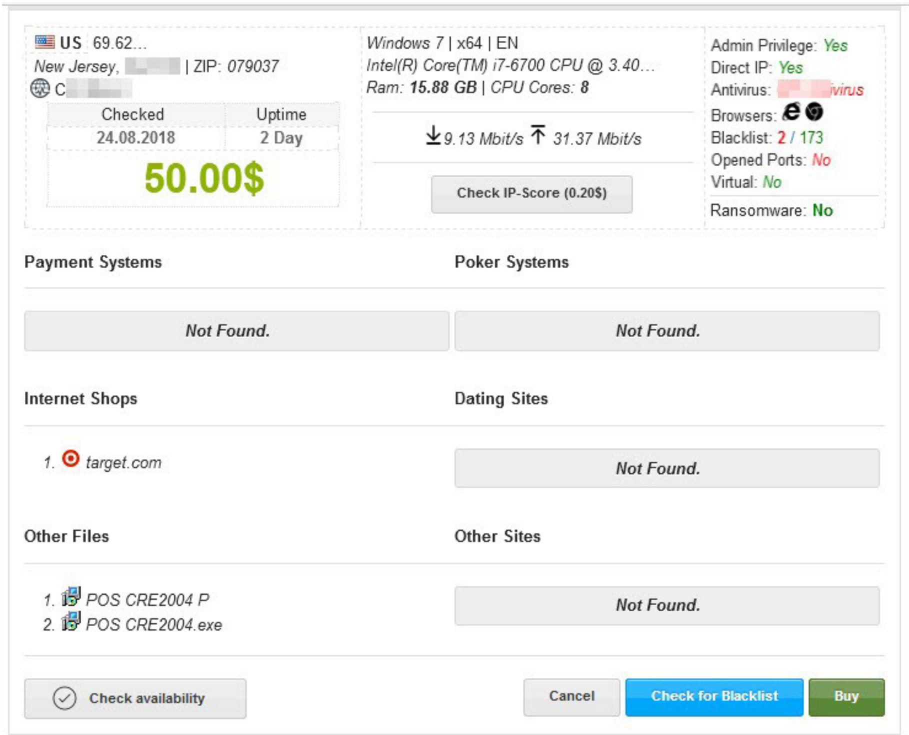
Choose Provider... | Choose an OS...

Direct IP: ON
Admin Privilege: ON
No PayPal: OFF
Port 25: OFF
Port 80: OFF
Show VM: ON
Show Reselling: ON

IP	COUNTRY	REGION, STATE	CITY	OS	RAM	DOWN	UPL.	DIRECT IP	ADMIN PRIVILEGE	LAST CHECK	SELLER	PRICE, $
96.8... [Full Info]	US	New York	Buffalo	Server 2012 R2	1023 MB	46.55 Mbit/s	7.54 Mbit/s	√	√	30.08.2018	selez	19.25
23.94... [Full Info]	US	New York	Buffalo	Server 2012 R2	1023 MB	101.48 Mbit/s	21.06 Mbit/s	√	√	24.08.2018	selez	31.75

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.



US 69.62...
New Jersey, [redacted] | ZIP: 079037
C[redacted]

Checked	Uptime
24.08.2018	2 Day

50.00$

Windows 7 | x64 | EN
Intel(R) Core(TM) i7-6700 CPU @ 3.40...
Ram: **15.88 GB** | CPU Cores: **8**

↓9.13 Mbit/s ↑ 31.37 Mbit/s

Admin Privilege: Yes
Direct IP: Yes
Antivirus: [redacted]virus
Browsers:
Blacklist: 2 / 173
Opened Ports: No
Virtual: No
Ransomware: **No**

Payment Systems

Not Found.

Poker Systems

Not Found.

Internet Shops

1. target.com

Dating Sites

Not Found.

Other Files

1. POS CRE2004 P
2. POS CRE2004.exe

Other Sites

Not Found.

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 more than 30 years, ESETR 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.