FEATURE

# Avoid Having to Run Somewhere From Ransomware, Part 2

## Top 10 Steps to Stay Protected

Ransomware can be defined as a malware deployed for the specific purpose of denying access to a victim's systems and/or files until something of value is exchanged. The primary motivating factor for most ransomware attacks is clearly in the name, a ransom. Part 1 of this article series reviewed several prominent examples of the damage caused by recent ransomwares attacks, the most common attack vectors used to infiltrate systems, and the money trail from pre-attack to payout. By knowing the common thread that runs through ransomware attacks, a general risk profile can be built.

The research and development arm of the cybersecurity industry is reacting to the problem of ransomware. Decryption tools are available for some ransomware families (e.g., FortuneCrypt, WannaCryFake, JSWORM, IAMSooRRY, ZERO&UCKS).[1] However, there are many others that do not have decryption tools, and new variants are always on the horizon. What can enterprises, which are in the crosshairs of this arms race between hackers and defenders, do? The following are the top 10 most impactful steps that enterprises can take to avoid becoming the next ransomware victim.

### 1. Restrict Macros

It was noted in part 1 that the most common software vulnerability is macros embedded in trusted applications such as the Microsoft Office Suite. The newest versions of Office programs have options to disallow embedded macros that are not digitally signed. This option should be enabled by default across the board, allowing only macros from trusted people or enterprises.

### 2. Provide Email Awareness Training

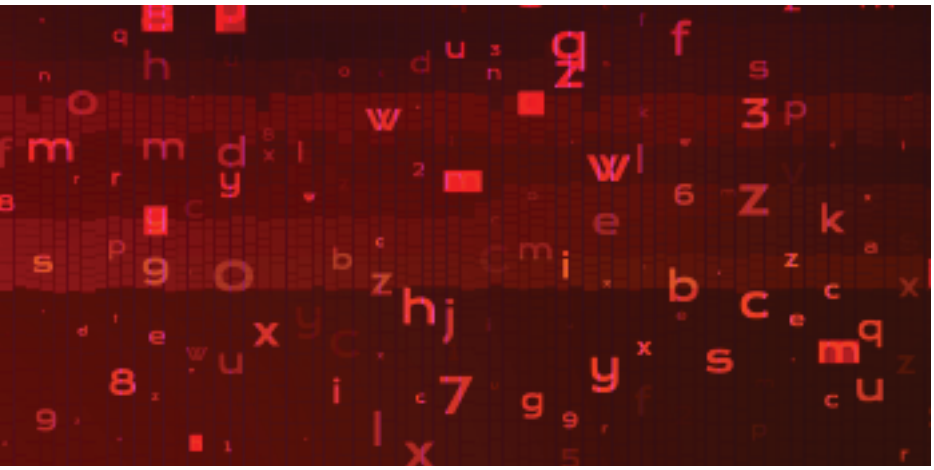
In large-scale environments, it is not feasible for members of the cybersecurity team to maintain a one-on-one relationship with every user. However, they can educate the user community about proper email behavior and why it should be a priority for everybody. Users are often considered the weakest link in an enterprise's security system, but with proper training, testing and follow-up, they can become the strongest. This positive transformation is possible with a good training program that empowers users with the knowledge they need to succeed, encourages users to implement what they have learned and regularly evaluates users' knowledge via live tests.

A good security awareness training program should start with email fundamentals and then expand on them to keep users engaged. Some of the basics of email that all staff should know are:

- Do not click on links or download attachments from parties that are not completely trusted.
- Look at the email headers. ("From" fields are usually giveaways.) Does something about the domain seem off? Is it .net when it should be .com? Is it misspelled? Is the "from" field completely absent? Quickly delete these emails without opening them.

**Syed Ishaq, CISA, CRISC, CCISO**
Has 15 years of information security experience serving Fortune 50 and government organizations. He advises chief information security officers (CISOs) on behalf of ControlPoints, a high-growth cyberrisk consulting firm. He can be reached at syed@controlpoints.com.

**Faizan Mahmood, CISSP, PMP**
Is a former CISO with more than 10 years of hands-on experience, much of that time spent as a data center and cloud architect. He is currently a senior member of the Security Test and Evaluation team at the US Federal Communications Commission (FCC). He can be reached at mahmoofx@gmail.com.



- Think twice before clicking on hyperlinks in emails and instant messenger, even from trusted senders. Domain names and display names can easily be spoofed. Hover over links to ascertain their credibility before clicking on them.
- Immediately turn off the Internet connection if a suspicious process is detected. This is particularly effective in the early stages of a ransomware attack because the malware will be prevented from establishing a connection with its command and control server and, thus, will be unable to complete the encryption routine.

> "THERE IS NEVER A GOOD REASON FOR AN ENTERPRISE TO HAVE RDP OPEN TO THE INTERNET."

## 3. Enable Network Level Authentication

Network Level Authentication (NLA) is a technology used in RDP to protect a network from becoming accessible to unauthenticated users. It requires remote users to authenticate themselves (i.e., pass on their credentials via a client-side secured connection) before they can establish a session with a server to use its resources.

If NLA is not enabled, a user can directly authenticate against a server and possibly deplete its resources. Without NLA, the server also allows clients onto the network without first identifying or authenticating them.

With Windows, this is a simple toggle switch in remote settings. It should be turned on immediately if it is not already set.

## 4. Use Strong Passwords

The amount of time it takes for someone to crack a password can be the difference between immunity and infection. The difference between scenario A, a 10-character alphanumeric password that includes a special character and is truly novel (i.e., not subject to common dictionary attacks), and scenario B, a 6-character alphanumeric password that includes no special characters and is truly novel, is significant. For those with a curious mind, the time required to crack each type of password is:

- Scenario A: 4,687.6 hours (195.32 days)
- Scenario B: 0.2 hour (12 minutes)

Raising the minimum password length from 10 to 12 characters (scenario C) or longer is even better, as each additional character makes the password exponentially less susceptible to a brute-force attack. This assumes that common words and phrases are not employed; otherwise, the password would be susceptible to a dictionary attack.

- Scenario C (12 characters): 7,556,404.5 hours (314,850.19 days)

It goes without saying that all default passwords should be changed across all access points to prevent brute-force attacks.

## 5. Implement Multifactor Authentication

Despite the sense of security a long password may offer, if someone wants to get in, it is just a matter of having a computer and time. With artificial intelligence, 5G and quantum computing right around the corner, even computers and time will soon become irrelevant. Until then, multifactor authentication (MFA) offers a safety net. Think of it as a moat around a castle wall. It fortifies already fortified defenses. No matter what type of phone or device an enterprise utilizes, there is a very strong likelihood that there is a soft-token application in the marketplace that will allow easy multifactor integration. At a minimum, MFA should be required for externally initiated access or access to sensitive materials.

## 6. Secure RDP

Remote Desktop Protocol (RDP) should be cut off from the world. There is never a good reason for an enterprise to have RDP open to the Internet. Whether through social engineering or brute force, bad actors are actively looking for exposed and vulnerable RDPs. They do so by scanning large swaths of Internet Protocol (IP) ranges to see whether Port 3389 is open, and when it is, they can target malicious behavior.

The threat monitoring company AlertLogic reviewed 130,000 attacks against its 4,000 customers and discovered that 65 percent of incidents occurred on only three ports: 22 (SSH), 80 (HTTP) and 443 (HTTPS). (Although each is used for communication, SSH should not be open to the world, and 80 should redirect to 443 wherever possible.) Fourth on the list was Port 3389 (RDP).[2] Enterprises would be wise to keep their RDPs out of the path of the storm by cutting their ports off to the world.

Organizations should also limit RDP to users who truly need it. Although this may be easier said than done in certain environments, security professionals need to sell this idea to key business stakeholders. Giving everyone full access is always the path of least resistance, but just like an open Any/Any firewall that allows everything to work, it surrenders its security purpose as a consequence. Instead, allow personnel with legitimate claims to RDP to make those claims, create a process in which true needs are judged against wants, and continuously monitor to determine whether access needs have changed as the enterprise matures and shifts.

Not all administrators require RDP, even though it is granted as a default setting. The administrator account should be removed from the RDP access group and only specific authorized users should be allocated to a "remote desktop users" group. Accounts within the domain administrator group have full control of the domain by default, and any compromise here lets an attacker hold the "keys to the kingdom." It goes without saying that the number of domain administrators should be limited to the absolute minimum, and they should refrain from accessing the RDP server or other externally exposed systems via these accounts to avoid inadvertently making credentials accessible.

If, for some reason, an enterprise must enable RDP to the whole Internet, perhaps for a temporary scenario, change the listening port from the standard 3389 to something within the dynamic range. It must be pointed out that this acts only as a camouflage, helping to hide the open RDP server from common Internet Protocol (IP) scanners. The residual risk will not be static, though, because as the incentives for exploitation mature, so do the scanners. Opening RDP on a different listening port offers only temporary protection.

"GIVING EVERYONE FULL ACCESS IS ALWAYS THE PATH OF LEAST RESISTANCE, BUT JUST LIKE AN OPEN ANY/ANY FIREWALL THAT ALLOWS EVERYTHING TO WORK, IT SURRENDERS ITS SECURITY PURPOSE AS A CONSEQUENCE."

RDP servers should be placed behind a firewall within a demilitarized zone (DMZ) or other restricted area of the network. That way, in the event of a successful attack, its scope will be reduced and confined to the RDP server alone. If this is not feasible (e.g., because RDP needs to be exposed to allow external users onto the network), the quantity and types of services reachable within the internal network should be minimized. Computers running RDP services on the network should be placed behind virtual private networks (VPNs) to allow access to only trusted users.

Finally, a block or timeout should be imposed on IP addresses with too many failed logon attempts. A high number is a strong indication of a brute-force attack, and limiting the number of attempts per user can prevent such attacks. It is best to log both failed and successful logons.

## 7. Patch in a Timely Manner

Many IT professionals fondly remember Patch Tuesday, when major IT vendors pushed patches every second and fourth Tuesday of the month. But the time delay between a vulnerability being identified and a potential fix being released on Patch Tuesday left everyone at risk during that interval. Microsoft's new policy of continually releasing patches has made everyone a lot safer and helped close the dreaded vulnerability window.

## Enjoying this article?

- Read *Phishing Defense and Governance. www.isaca.org/phishing*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

But unfortunately, enterprises are not taking advantage of these continually releasing patches. For example, Microsoft emphasized the importance of installing the critical security update for EternalBlue (the vulnerability that powered WannaCry), but the scale of the global attack made it clear that a significant proportion of victims had not applied the patch. WannaCry took only a day to spread around the earth, infecting more than 230,000 computer systems in 150 countries and costing approximately US$4 billion in financial losses.[3] WannaCry exploited a known weakness in Windows computers for which Microsoft had released a fix months prior to the attack. Enterprises should keep up-to-date on all patches, especially security patches, and make sure to test all patches quickly and thoroughly before applying them.

Enterprises should develop a reliable patching strategy that, in addition to patching Windows operating systems, prioritizes the timely patching of Java, Flash and Adobe Reader. These are commonly exploited by ransomware. Automatic updating should be enabled whenever possible for devices and applications connected to the network.

**Control Legacy and Shadow IT**

The majority of malware and most active ransomware families rely on vulnerabilities in obsolete desktop operating systems because they make lateral movement frictionless. When hardware and software are no longer supported by the vendor, enterprises should upgrade it, replace it or air-gap it. This requires an enterprise to maintain a complete inventory of all IT assets, because if it cannot be seen, it cannot be protected.

## 8. Use Endpoint Protection

Employing endpoint protection and keeping software up-to-date are critical. Many antivirus packages now offer ransomware-spotting features or add-ons that can identify suspicious behavior common to all ransomware: file encryption. Some security packages even make copies of the files that are threatened by ransomware. In addition, content scanning and email filtering can be used to prevent attack emails from arriving in the inbox.

## 9. Implement Fail-Safe Backups

Sometimes bad things happen. If there is something worth protecting, someone somewhere is likely to come after it. One of the best protections against a ransomware attack is regular, viable backups. It is not possible to perform full backups of everything every second, but it is possible to identify the most critical data and ensure that backups are scheduled accordingly. Store at least one copy of backups offline to air-gap it from a network storage attack. Critical backups should be tested periodically to validate recoverability.

## 10. Have a Modern Incident Response Plan

At a US conference of mayors in July 2019, more than 14,000 mayors signed a resolution agreeing not to pay ransoms.[4] But if a violation occurs and critical life-saving services are not available, emotions must be taken out of the equation, and hard decisions must be made.

> "IT IS NOT A SIMPLE TASK TO RECOVER FILES ENCRYPTED BY RANSOMWARE, AND IN MANY CASES, IT IS IMPOSSIBLE."

## To Pay or Not to Pay?

What should an enterprise do if it is attacked? It is not a simple task to recover files encrypted by ransomware, and in many cases, it is impossible. Therefore, a modern and rehearsed incident response plan (IRP) is critical to preventing a ransomware attack and responding effectively to one. A 2019 report by the Ponemon Institute concluded that the formation of an incident response team and the existence of a tested IRP could save enterprises an average of US$680,000 in the event of an incident and contain the attack in less than 30 days, which could save more than US$1 million.[5] The city of Baltimore, Maryland, USA, may have avoided losing US$18 million had it simply formalized an IRP and tested it routinely.[6]

One component of a modern IRP is a cost-benefit calculus of time, effort and cost in determining whether to pay a ransom. Modern IRPs should consider the following:

- **Data criticality**—How important are the data in question, and are they worth recovering?
- **Business impact**—How long can the business operate without the data before profits or reputation are adversely impacted? Some attackers resort to publicly naming victims who refuse to pay the ransom and/or publish their stolen data little by little until payment is made or until all of the data have been released. What business impact will this have in the form of regulatory fines, data breach notification costs, tarnished brand image, loss of business and trade secrets, and potential lawsuits for the disclosure of personally identifiable information (PII)?
- **Feasibility of recovery**—Are there any viable backups of the data, and if so, are they also encrypted? It is safe to assume that the attackers have been inside the network for weeks and will have estimated how much time, effort and money it will take the victim to restore data from backups when deriving their ransom amount.
- **Recovery effort**—Large volumes of data take longer and require more effort to recover. Disparate locations can complicate recovery efforts, especially if the attacker is still lurking somewhere on the network. If a fresh image of the infected operating system must be loaded onto computers before data can be restored, this will add to the recovery time. If the enterprise must resort to pen-and-paper processes to log transactions during a lockdown, the time to tediously input these data once systems are restored must be considered.
- **Impact of recovery**—Estimate the effect of lost services on customers and employees. This may include lost revenue and damage to reputation. If recovery efforts are prolonged, these costs can skyrocket.
- **Paying the attacker**—Can the ransom amount be negotiated down? Will the insurer pay part or all of the ransom? Can the insurer's payment be quickly converted into cryptocurrency? Is it known where Bitcoins can be bought and a wallet acquired? Is the attacker likely to provide the decryption key upon receiving payment? Are there any indications that the decryption key will not work? Will the criminals launch future attacks against the enterprise? Which federal, state and local law enforcement agencies must be contacted before proceeding? Can the enterprise's reputation be defended against the ensuing political and public pressure?

Although ransomware is drawing headlines and driving fear, focused security measures can substantially enhance an enterprise's ransomware readiness and ensure that customers continue to be served uninterrupted.

> "FOCUSED SECURITY MEASURES CAN SUBSTANTIALLY ENHANCE AN ENTERPRISE'S RANSOMWARE READINESS."

## Endnotes


1 Emsisoft, "Free Ransomware Decryption Tools," Emsisoft, 18 October 2019, *https://www.emsisoft.com/ransomware-decryption-tools/free-download*

2 Ilascu, I.; "Most Cyber Attacks Focus on Just Three Ports," Bleeping Computer, 17 September 2019, *https://www.bleepingcomputer.com/news/security/most-cyber-attacks-focus-on-just-three-tcp-ports/*

3 Cooper, C.; "WannaCry: Lessons Learned 1 Year Later," Symantec, 15 May 2018, *https://www.symantec.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later*

4 SecureWorld, "Mayors: 'We're Done Paying Ransoms' to Hackers," 12 July 2019, *https://www.secureworldexpo.com/industry-news/mayors-refuse-to-pay-ransom*

5 Ponemon Institute; *2019 Cost of a Data Breach* Report, 2019, *https://databreachcalculator.mybluemix.net/?_ga=2.175324322.1495375045.1572557631-835423134.1572557631&cm_mc_uid=38498281627215725576306&cm_mc_sid_50200000=83112451572557630645&cm_mc_sid_52640000=73429421572557630657*

6 Duncan, I.; "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts," *The Baltimore Sun*, 29 May 2019, *https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html*