CHAPTER 17

Ransomware and Privileges

Let me get this out right off the bat: **no one solution is 100% effective in mitigating the risk of ransomware**. Some technologies are claiming to have tested hundreds of samples, and that their tool is perfect in stopping all types of attacks. I'm sorry, but that is a falsehood. Why? If any single vendor had a solution that could solve the problem completely, ransomware would not be such a problem.

At its core, ransomware is a form of malware that cybercriminals use to infect computers or cloud resources and then to encrypt files and data, making them inaccessible until the owner has paid a ransom. Of course, even paying the ransom is no guarantee that access will be restored by the perpetrators.

From catastrophic, lengthy downtime to economic devastation and even loss of life, today's ransomware is clearly beyond the scope of just being a nuisance. It has already been well documented that ransomware has even caused loss of life and reduced health outcomes. So, where are organizations getting it wrong? And what changes can you make to get it right when it comes to ransomware defenses?

All security professionals should be able to tell you that there's no silver bullet to defend against all varieties of ransomware. But there are strategic IT security practices, like privileged access management, that can help eliminate many types of ransomware outright and dramatically

M. J. Haber, *Privileged Attack Vectors*, https://doi.org/10.1007/978-1-4842-5914-6_17

reduce the overall risk of suffering a devastating attack. For example, application control solutions, endpoint protection products, and least privilege solutions are effective in mitigating various types of ransomware, but none are 100% effective across all ransomware types. Modern ransomware can leverage privileges when available, does not always launch separate executables, does not always drop files on the file system, and sometimes targets obscure devices, like smart TVs. We have seen a spike in ransomware that uses Microsoft Office macros to propagate the threats, and even versions that use JScript embedded in a document to conduct malicious activity. We have also seen ransomware like WannaCry and NotPetya leverage exploits across modern and end-of-life operating systems to devastate organizations. The attack vectors are growing as ransomware continues to mature and escalate as this decade's (and last decade's) largest cybersecurity threat. Ransomware wasted no time in exploiting fears around Coronavirus (COVID-19) It's been quick to evolve and weaponized to hit us where it can do the most damage.

Unfortunately, the delivery of the ransomware payload is equally as horrific to identify as seeing a ransomware payment message. To understand how privileges affect ransomware, consider the sources in which ransomware may originate:

- An exploitable vulnerability in an application or website
- An errant, malicious executable executed by the asset
- A PowerShell script or batch file
- Embedded as an application macro or script in a file
- Compromised auto-update mechanisms per application or the entire operating system
- A phishing attack designed to socially engineer the user into high risk behaviors

What makes this a little more disturbing is that many attacks combine methods and use a command control server to hold encryption certificates, vs. locally based per infection that can be cured with a decryption solution. The privileges ransomware executes will help dictate how successful the malicious infiltration will be. And, modern ransomware may be just a Trojan Horse for other advanced threats designed to distract IT security teams. This is why ransomware is so difficult to stop, and no one technology is 100% effective.

As a defense, there are some actions you can perform with privileged access management to minimize the threats of ransomware. Unfortunately, nothing will ever replace training users not to select Run Macros when opening an unknown file. However, here are a few rules that are easy to implement that will block the vast majority of mistakes users can make, stop droppers from executing, and block vulnerable applications from being leveraged against your assets:

- **Implement Application Control**: Privileged access management solutions allow for application control and the ability to elevate applications based on rules. In addition, PAM solutions can operate in the opposite mode—they can block any unauthorized application from executing, regardless of the source, if it is not properly digitally signed, launched from an improper location, called inappropriately as a child process, or tries to execute a malicious child process of its own.

- **Secure Remote Access**: Remote access, particularly by third-party vendors, is often the weakest link in network security and can lead to a ransomware attack. Vendors authorized to access the network and applications might not adhere to the organization's same level of security protocols, or they may use virtual private networks (VPNs) to extend "secure" access to internal resources. If the vendor is infected, has malicious intent of their own, or is a carrier of ransomware, your organization could be the next victim. Therefore, the best way to mitigate the risk is to use remote access technology that does not use any protocol tunneling, VPN, nor rely on traditional remote access protocols that could be leveraged as an attack vector.

- **Secure Privileged Credentials**: Compromised credentials are a well-known ingredient of almost all IT security incidents and ransomware is no exception. To execute, ransomware wants privilege. Privilege is a critical path for ransomware's persistence. That's why it's critical to secure privileged credentials with an enterprise privileged password management solution that will consistently discover, onboard, manage, rotate, and audit these powerful credentials. Automated rotation of credentials and consistent enforcement of strong password policy protect your organization from password reuse attacks as well as infection by ransomware and lateral movement once ransomware has gained a foothold.
- **Enforce Least Privilege**: Ransomware can only run with the privileges of the user or the application that launches it. That is fundamentally its biggest weakness. The best defense starts by not granting it excessive privileges in the first place. Therefore, removing local admin privileges and applying least privilege access across all users, applications, resources, and systems

won't prevent every ransomware attack, but it will stop the vast majority of them. It will also mitigate the impact of those ransomware payloads that make their way into an environment by closing down lateral pathways and reducing the ability to elevate privilege. Least privilege can even mitigate the impact of stolen credentials. If the credentials are for a user, endpoint, or application with limited or no privileges, the credentials can essentially not be used by the malware to infect another host unless it can scrape additional credentials or exploit a vulnerability that allows privileged escalation.

- **Apply Security Updates**: Of course, one of the most fundamental ways to reduce ransomware and other vulnerability-based exploits is simply staying up-to-date with patching and remediating of known, published vulnerabilities. This condenses the attack surface, reducing the potential footholds in your environment available to threat actors. To that end, very few ransomware attacks leverage zero-day vulnerabilities (MS Office Macros being the most prevalent). And, if a ransomware attack does happen to leverage a zero-day exploit, following all of the other strategies listed here will help reduce your attack surface to ransomware and, hopefully, blunt the impact of any attack should it make it into your environment.
- **Stopping Droppers**: Unfortunately, trusted applications can launch other applications to perform their intended functions. This includes browsers, email programs, and even PDF readers. The consistent

part of this problem is that these executables almost always launch from temporary file directories. Using privileged access management to manage file integrity, administrators can track, alert, and block rogue dropper executables that appear in these directories or that do not meet minimum reputation requirements.

- **Leverage Application Reputation**: Privileged access management solutions typically have a reputation service engine or other technology to measure the risk of an application before its launch. This component allows for real-time assessment of an application's health with regards to malware, vulnerabilities, permissions, and privacy. To that end, policies can be established to deny (or notify of) the launch of risky applications that could be leveraged in a ransomware attack. This helps ensure service-level agreements are being met for cybersecurity hygiene and no system is left out that could pose an unacceptable risk.

Ransomware risk can be minimized using the same technology used for managing privileged accounts. While this approach is not 100% effective, it is a residual return on investment when organizations embrace this approach. Organizations can stop most ransomware from executing simply by not giving it the privileges it needs to execute in the first place.