



PROTECTING STATE AND LOCAL GOVERNMENTS AGAINST RANSOMWARE

With attacks on the rise and cybercriminals growing more resourceful, agencies must mount a strong, proactive defense.

You don't have to look long or hard for examples of ransomware attacks on state and local governments. Over the past several years, attackers have hobbled city computer networks, locked students out of Wi-Fi networks and online textbooks, shut down state legislative voicemail and bill-drafting applications, threatened municipal water and power systems, and more.

Events like these disrupt essential public services, put lives at risk and cost taxpayers huge sums of money. In 2020, ransomware accounted for one-third of cybersecurity attacks on government entities.¹ And the barrage of ransomware attacks is only growing more intense over time. The FBI's Internet Crime Complaint Center says it received 2,084 ransomware complaints in the first half of 2021, representing a 62 percent increase year-over-year.²

To make matters worse, ransomware continues to evolve. Cybercriminals are moving from broad-based phishing attacks to highly targeted attacks on specific organizations. To protect your agency from these threats, you need to understand the anatomy of ransomware.

How Ransomware Works


Here's a simple description of a ransomware attack:

- The attacker injects malicious code through broad-based phishing, targeted spear-phishing, or direct attacks on vulnerable VPN systems and web applications.

- Once inside a government computer network, the malware searches for and then exploits vulnerabilities and misconfigurations.
- The attacker then moves laterally through your organization, gathering credentials along the way.
- Finally, the attacker escalates privileges, gaining access to hundreds or even thousands of devices to acquire and encrypt their data.

Attackers today don't simply exploit an end user's computer to gain initial access into a network. They have expanded their attack methods to rapidly spread malware across networks to other devices and assets. Now, nearly any device, application, operating system or network could become an entry point. And the growing attack surface and vulnerability-riddled environments make it nearly impossible to prevent attackers from compromising at least one entry point.

Attackers also no longer take a linear path to their target; rather they take a dynamic approach based on the compromised device's environment. Their tactics often include evading defenses, executing malicious code, collecting credentials, enumerating the network and Active Directory (AD), and attacking passwords. The attacker gathers information, analyzes the environment, and exploits vulnerabilities and misconfigurations, all in an effort to obtain even more access privileges. AD is almost always the first



target for attackers, because it's the primary authentication and authorization tool used by most organizations.

Having gained privileges within AD, the attacker's work is nearly complete. The final steps include copying targeted data, deploying ransomware (usually via group policy), establishing persistence and backdoors, deleting backup files, and triggering network infrastructure encryption.

Where to Start

Ransomware is the monetization of poor cyber hygiene, so agencies must put in place key fundamentals to reduce risk. According to experts such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.K. National Cyber Security Centre (NCSC), organizations should take these basic measures:

- Conduct cybersecurity awareness training sessions to decrease phishing attacks.
- Segment your networks to separate various business units and resources, allowing you to contain an intrusion more easily when it occurs.
- Enable multi-factor authentication everywhere.
- Maintain frequent, encrypted backups of data and system images.
- Perform continuous risk-based vulnerability management and Active Directory assessments of your entire attack surface.

Six Steps to Defend Against Ransomware

Beyond these basic measures, here are six specific steps government agencies can take to protect their infrastructure against ransomware attacks.

Step 1

Scan often, scan everything

More and more ransomware strains use software vulnerabilities as an initial attack vector. These flaws can be older and well known or new vulnerabilities such as Log4j, so it's essential to continuously assess your entire attack surface as your environment changes and new threats emerge.

Since there is no one-size-fits-all solution, this requires an adaptive approach.

Network scanners are highly effective for identifying exposures in traditional on-premises IT infrastructure, and it's critical that you use credentialed scans wherever possible to gain deep insight into vulnerabilities and misconfigurations.

Agent-based scanning is another approach for organizations that prefer not to manage credentials or have remote endpoints frequently disconnected from the network during scheduled scans.

Modern web applications require a purpose-built scanner to gain visibility into dynamic, JavaScript-based and HTML5 elements and single-page applications that are invisible to many other scanners.

Protecting operating technology (OT) is another concern for governments. OT assets are generally purpose-built systems that run water plants, power grids and other industrial infrastructure. They operate very differently from IT assets. OT systems may be standalone, but in other cases, IT and OT are converged, creating attack vectors that span both environments. In these complex environments, you cannot actively scan for threats using IT-based network scanners because they may disrupt mission-critical services. Instead, assessing OT devices requires a mix of device and network-based detection methods that leverage native command language, protocols and passive monitoring of traffic across systems.





Vulnerabilities exploited by ransomware tend to cluster around specific types of weaknesses or asset categories. Knowing these patterns in advance lets savvy defenders predict which vulnerabilities attackers will target and proactively address them.

Step 2 **Harden Active Directory defenses**

Ransomware groups increasingly target Active Directory because it contains the keys to your kingdom — controlling login credentials; configuration settings; and access policies for all users, endpoints, services and servers.

Unfortunately, agencies often don't pay enough attention to protecting AD because it's a legacy environment. Organizations must ensure AD is void of critical misconfigurations that would let attackers move laterally and escalate privileges. Finding and fixing these existing AD misconfigurations can be a laborious task, but it is essential.

Once AD is secured, agencies must continually analyze all modifications to ensure they do not create new misconfigurations and attack paths. This level of security hardening is the only way to keep attackers from using AD to deploy their malicious software across your computing environment.

Step 3 **De-escalate privilege escalation**

Just as it is important to use anti-malware software to scan Windows for unusual files and processes, it is crucial to monitor AD for unusual and malicious activity. Attackers will often create avenues they can leverage to attack AD. This eventually leads to privilege escalation, so the attacker can deploy encryption software, download data for exploitation, delete backups and create backdoors for future access.

With the right intelligence, you can correlate AD changes, Syslog changes and Windows event logs to reveal misuses of privileged accounts and active misconfiguration exploits. This information can help incident response teams proactively stop ransomware attacks from spreading via AD. Integrate this data with your security information and event management (SIEM) software to collect information forwarded from the Windows Server event logs and other systems.

Step 4 **Take a risk-based approach and prioritize using prediction**

You cannot patch everything, and the good news is you don't have to. Of the more than 18,000 new vulnerabilities

published in 2020, only 5 percent had a publicly available exploit. That 5 percent is where you need to focus.

Take advantage of real-time threat intelligence to understand the latest attack paths ransomware groups use and guide your remediation strategy. But don't stop there. Vulnerabilities exploited by ransomware tend to cluster around specific types of weaknesses and asset categories. Knowing these trends in advance lets savvy defenders predict which vulnerabilities attackers will target and proactively address them.

Risk-based vulnerability management (RBVM) reduces risk across your attack surface by prioritizing vulnerabilities for remediation based on the risks they pose to your organization. It uses machine learning to correlate asset criticality, vulnerability severity and threat actor activity. This reduces vulnerability overload and helps you focus on the relatively few vulnerabilities that pose the most risk to your enterprise, particularly those likely to be used in ransomware attacks.

Step 5 **Remediate as though your organization depends on it**

Too often, vulnerabilities and misconfigurations targeted for remediation are never fully fixed. Although security teams are responsible for detecting and prioritizing vulnerabilities, patching them is the responsibility of IT operations and developers — and these groups often speak a different language and have different goals.

It's more important than ever to integrate RBVM solutions with IT service management and ticketing systems to automate workflows, correlate vulnerabilities with patches, and verify that all instances of a vulnerability are patched or remediated by a compensating control. You can automatically send vulnerability and misconfiguration data to your SIEM to provide event context and identify potential areas for response automation.

Remediation is a team effort. Send customized reports to communicate vulnerability priority to DevOps and other groups across your organization, so they know what to fix first.

The same applies to addressing AD misconfigurations. Manual monitoring of most AD implementations is impractical because



of the size and complexity of these systems. Take advantage of technologies that provide step-by-step remediation guidance to fully eliminate AD weaknesses and block attack pathways.

Step 6 Measure to improve your game

Successful teams take time to reflect on their performance. Security teams are no different. Develop key metrics to gauge and communicate how your operational controls are working (or not working). Also gather benchmarking data to compare performance across internal groups or externally against your peers.

Measurements should include:

- How often you scan the majority of your assets
- The number of open vulnerabilities you are capturing
- Your effectiveness in remediating your highest risk vulnerabilities
- What your key functions are, and how well you're reducing their cyber risk

Conclusion

Defending against ransomware requires organizations to address flaws before attackers can exploit them. It's critical to see all vulnerabilities and misconfigurations across your attack

surface, predict what issues matter the most based on threat intelligence and act quickly to address cyber risk.

The Ransomware Guide from CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC) offers additional insight into ransomware preparedness.³ Among its recommendations:

- Conduct regular vulnerability scanning to identify and address vulnerabilities — especially those on internet-facing devices — to limit the attack surface.
- Regularly patch and update software and operating systems to the latest available versions. Prioritize timely patching of internet-facing servers — as well as software processing internet data, such as web browsers, browser plugins and document readers — for known vulnerabilities.
- Secure domain controllers (DCs). Threat actors often target and use DCs as a staging point to spread ransomware networkwide.

The measures outlined in this brief should become everyday aspects of your security operations. This extra level of vigilance will go a long way toward mitigating threats posed by ransomware — turning disruptive attacks into unsuccessful attempts.

¹ <https://www.afcea.org/content/sponsored-81-ransomware-statistics-data-trends-and-facts-2021>

² <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>

³ https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf



Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. The creator of Nessus®, Tenable extends its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and federal, state and local government agencies. Learn more at www.tenable.com.