Rapid Evolution of Ransomware Tactics Outpacing Enterprise Defenses

KEY ISSUE:

Ransomware Wreaking Havoc on Unprepared Enterprises

With the rise of WannaCry, a strain of ransomware that spreads via SMB worm capabilities, malware that encrypts files in exchange for payment has renewed its place on the forefront of the threat landscape.

Many strains of ransomware have been spread either by phishing campaigns or by exploit kits. WannaCry, however, represents a new frontier for ransomware delivery. In addition to having the ability to encrypt files and hold them for ransom, it has a built-in SMB worm capability. Instead of users opening an email or landing on a web page to become infected, a machine infected with WannaCry scans for other machines and automatically infects them with WannaCry ransomware as well. Even though the initial round of WannaCry infections has been slowed down by the registration of a hardcoded kill switch domain, other kinds of ransomware are adopting the SMB vulnerability as an infection vector. Its rise shows that ransomware writers are adapting their tactics in 2017, and quickly experimenting with and adopting newly released exploits as ways of ensnaring targets and making money.

CHALLENGES AND OPPORTUNITIES:

Optiv's threat intelligence has continued to see the update and pushing of new ransomware in underground and deep web market places, indicating that malicious actors continue to develop new strains to outpace signature detection.

Opportunistic ransomware campaigns will continue to target consumers and enterprises in 2017. The WannaCry issue in May 2017 shows a similar tactic as recent Samas ransomware campaigns, in the sense that infected machines scan for and attack other vulnerable machines, but against SMB instead of JBoss. WannaCry has functioned as an SMB worm, targeting the same vulnerability that the ETERNALBLUE exploit from the Shadow Brokers release targets. That vulnerability has been patched, but enough unpatched machines remain in the wild to make it a worthwhile endeavor for the attackers. WannaCry transmits itself like a traditional computer worm: infected machines scan for other machines vulnerable to an SMB issue, and then exploit the identified machines. WannaCry activity has been identified in multiple industrial verticals, most prominently including healthcare, oil and gas, and education.

Because ransomware remains a tactical weapon of choice, custodians of data face unique challenges as frequency of attacks increase and grow more complex. Organizations have an opportunity to assess current security postures to withstand this current wave of attacks and prepare for the next.

THE PATH FORWARD:

Enterprises can mitigate ransomware attacks and subsequent impact through people, process and technology and "cyber hygiene."

PEOPLE

Empower users with knowledge

Ransomware spreaders continue to target **end users** as entry points for their efforts of infection. In light of this data point, organizations should build robust security awareness programs, if not already in place, or enhance existing programs. These measures are crucial, states Social-Engineer.com CEO and author Chris Hadnagy, because "ransomware cannot be human hardened." Security leaders should focus on empowering users with relevant awareness to identify, recognize and report phishing attempts. Increased awareness can improve resistance against ransomware campaigns. Any enterprise's greatest assets is its users, so here the users become single points of resistance in the overall strategy against ransomware and similar malware. Employees should come away from awareness training with thoughts such as, "My company is at risk from ransomware, so how can I help protect my organization and its data?" Organizations are encouraged to run periodic simulated attacks to reinforce the effectiveness of the awareness training.

PROCESSES

Enterprises can achieve success against extortion-based threats by focusing on three stages of ransomware attacks.

1. Have a well-defined response plan in place in anticipation of ransomware campaigns. Preparation becomes more critical as attackers evolve and innovate.

   A typical response team should include staff from IT, legal communication and the executive level. Define their roles and responsibilities and verify vetting and testing of communication channels between members of the response team.

2. During an attack, resist paying hostage demands as this behavior encourages further attacks. Ensure that end users are aware of this policy of engagement with ransomware dealers. Disconnect infected systems to prevent the spread of the attack and remediate infections. If removal of ransomware is not achievable, reimage systems and restore data from backups. In cases where data is highly susceptible to risk, consider offline backups.

3. Perform a postmortem of the attack. Identify and remediate gaps in process. Refine the incident response process as needed.

In short, security practice managers should validate that security processes and guidelines are adhered to in the case of specialized attacks like ransomware.

TECHNOLOGY

A core set of controls and processes that can slow or disrupt ransomware dealers includes, but is not limited to effective endpoint detection, containment, segmentation, access controls and backups.

Effective layered defense is the foundation for an effective security posture, especially against ransomware operations.

Endpoint protection starts with the basics – anti-virus, anti-exploit and host intrusion detection or prevention – to mitigate ransomware and other malware. Moreover, endpoints should have comprehensive restricted desktop policies (RDP). Leverage RDPs along with whitelisting solutions to minimize ransomware's ability to function. In addition, identity and access management (IAM) and privilege identity, user and access management (PIM, PUM, PAM) solutions are important controls to address shifts in perpetually shifting threat landscapes of ransomware. To extend endpoint protection beyond the corporate network, consider implementing hybrid endpoint strategies using

endpoint agents in conjunction with cloud infrastructure to provide off network protection. In this manner, organizations can thwart opportunistic attacks everywhere and at anytime. More mature organizations, with proficient staff, may wish to add an endpoint detection and response (EDR) capability to its arsenal.

Most solutions will detect commodity ransomware, but EDR solutions equip staff with additional capabilities to hunt for and potentially stop specialized and targeted attacks in progress.

The right mix of endpoint solutions can reduce ransomware dwell time, often before it becomes an incident. In instances where a ransomware event does become an incident, improved detection can enhance the response capability of security operations, affording proactive advantage for organizations attempting to disrupt attackers in the earliest stages of ransomware attacks.

Should endpoint protection fail to prevent an attack on a system, **containment** becomes the next layer of security to mitigate ransomware threats. Security operations should have the ability to spoil attacks midstream, leveraging next generation firewalls (NGFW), intrusion detection and prevention systems, and cloud access security brokers (CASB) that possess strong mitigation "beyond the firewall" for content filtering and security blocking. **Like other malware and botnet operators, ransomware dealers use domain name servers to front their ransomware operations. In order to take data hostage, systems infected by ransomware must "phone home" to attacker infrastructure for instructions to encrypt data and initiate the ransom process. The ability of organizations to contain these communications is crucial in the fight to frustrate attacker intentions to seize data from companies.**

Data loss prevention (DLP) strategies also play a vital role in blocking the exfiltration of data by unauthorized users or services, stopping attacks in play. Data in motion (DIM), data in use (DIU) and data at rest (DAR) are essential for the prevention of data leakage and a potential ransom situation.

Most importantly, organizations should emphasize the security fundamentals to improve situational preparedness for combatting ransomware operators. The WannaCry worm, and the rise of other strains such as UIWIX that are using SMB vulnerabilities to gain a foothold on machines, means that software patching and endpoint hardening also have a place in ransomware prevention. Unlike so many strains of ransomware that are transmitted by phishing attacks, this strain exploits open SMB ports and operating systems with vulnerable SMB installations. Start with SMB, since that is a technology actively targeted by ransomware. But, continue to ensure that all machines on the network are patched and running software that is getting security patches, and frequently assess the network for unnecessary open ports and running services. If there is no business need for that increased internet-facing attack surface, remove the services or firewall the ports. **Asset configuration and patch management, logging and network segmentation remain fundamental to mitigating these threats and should not be undervalued.** Ensure that backups are not stored on open network share, since many strains of ransomware also search for and encrypt open shares Backup often and test to ensure the ability to restore certified data.

Finally, organizations are encouraged to **automate security capabilities.** Data show that threat actors leverage automation in their campaign efforts to victimize organizations. Organizations must be equally quick and adaptable.

- Data scientist Michael Roytman argues that on the basis of CVE data, time–to-remediation (TTR) and threat intelligence, threat actors are using automation to their advantage to compromise organizations with exploits like ransomware. In contrast, companies contend with attacker persistence by means of manual processes. In short, Roytman concludes, "We are too slow. We need more automation."

We encourage the use of application programming interfaces (APIs) where possible to facilitate communication between security solutions and enhance overall time-to-detection (TTD) and time-to-response (TTR). Security tools should integrate and work together to scale human effort. It is increasingly important for organizations to use automation to keep pace with threat actor innovation.

CALL TO ACTION

The ransomware threat landscape remains active and evolves rapidly. Beyond attacks on organizations, ransomware purveyors continue to release new strains of ransomware and appear poised to launch mass-scale spear phishing campaigns that target executives. Dark web operators have launched Ransomware-as-a-service (RaaS) commerce sites with moderate success. Further, we predict that ransomware attackers will refine their tactics, techniques and procedures to re-focus their sights on critical infrastructure networks. We recommend that organizations take the appropriate actions now to prepare for the next waves of attack. Sources of ransomware will continue their onslaught so complacency is not an option. Ransomware attacks are beatable if not survivable. Do not panic or engage malicious actors if possible. An array of controls and countermeasures exist to mitigate all stages of a ransomware attack. Building a robust and resilient security system, along with an emphasis on security fundamentals, will allow organizations to block a large percentage of ransomware and related attacks.

Further, organizations are encouraged to reinforce security awareness training of its workforce with content that reflects the current threat landscape.

Enabling end users to spot suspicious activity early increases an organization's chances to withstand attacks. Security awareness coupled with technology helps ensure business resiliency and continuity regardless of threat.

The role of privacy officers and managers becomes more crucial as private data is seized. Understanding the implications of extorted data ahead of attacks is essential for the protection of customer data. CISOs and risk officers should anticipate the unique privacy issues that arise in light of these specialized attacks. Know where the sensitive data is and classify it based on risk. Plan to isolate and segment data most important to the company where possible.

For a more in-depth technical analysis of ransomware, contact Optiv's Global Threat Intelligence Center (gTIC) or go to www.optiv.com.

References

Retrieved from: https://www.carbonblack.com/2016/03/25/threat-alert-powerware-new-ransomware-written-in-powershell-targets-organizations-via-microsoft-word

Retrieved from: blog.trendmicro.com/trendlabs-security-intelligence/without-a-trace-fileless-malware-spotted-in-the-wild/

Retrieved from: http://www.healthcareitnews.com/news/healthcares-newest-security-threat-powerware-ransomware

Retrieved from: http://blog.courion.com/topic/multifactor-authentication

Retrieved from: http://www.latimes.com/business/hiltzik/la-fi-mh-2016-is-the-year-of-ransomware-20160308-column.html

Chris Hadnagy, personal communication, April 2, 2016

Verizon Data Breach Investigations Report (DBIR)

Retrieved from: https://www.resilientsystems.com/cyber-resilience-knowledge-center/incident-response-blog/predictions-for-2016/

Retrieved from: http://www.mcafee.com/us/resources/solution-briefs/sb-quarterly-threats-nov-2015-1.pdf.

Verizon 2015 Data Breach Investigation Report. Retrieved from: http://www.verizonenterprise.com/DBIR/2015/. Pp. 19-21. Retrieved from: http://www.slideshare.net/MichaelRoytman/data-metrics-and-automation-a-strange-loop-siracon-2015

Retrieved from: https://blog.knowbe4.com/hello-mass-spear-phishing-meet-ransomware

Retrieved from: http://blog.fortinet.com/post/encryptor-raas-yet-another-new-ransomware-as-a-service-on-the-block

Retrieved from: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

Retrieved from: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

Retrieved from: https://www.grahamcluley.com/2015/11/website-files-encrypted-linux-encoder-1-ransomware-free-fix/

Retrieved from: http://vms.drweb.com/virus/?i=7704004&lng=en

Retrieved from: https://medium.com/@networksecurity/locky-ransomware-virus-spreading-via-word-documents-51fcb75618d2#.irp2i62rv

Retrieved from: http://blog.dynamoo.com/2016/02/malware-spam-scanned-image-image-data_29.html

Mark Arnold
Senior Research Analyst
Solutions Research and Development, Optiv

Danny Pickens
Director, Threat Intelligence, Optiv

Nicolle Neulist
Intelligence Analyst, Optiv

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

6.17 | F2