Booz | Allen | Hamilton

RANSOMWARE REALITY CHECK

GETTING BEYOND THE HEADLINES

Are you prepared for a ransomware attack? Recent headlines have exposed the increased sophistication of this evolving threat. Once largely limited to major organizations such as hospitals, banks, and more, cybercriminals have expanded the attacks to include individuals. While ransomware's methods are constantly advancing, there are ways to protect and prepare for an attack—and the time to act is now.

FROM EASY ACCESS TO TOTAL LOCKDOWN

Picture this: You're routinely checking your email when a suspicious message pops up. An anonymous attacker has encrypted your organization's account—locking down access to key information—and is demanding a significant sum of money to decrypt. This is ransomware. A growing threat from cybercriminals, ransomware is an attack on your systems, both personal and organizational, that encrypts your files and demands a ransom payment to restore access. Cybercriminals are targeting organizations that are lacking security hygiene and are willing to pay the ransom in order to avoid any disruptions to their operations. Preventing and recovering from a ransomware attack is best done through strong security planning and incident response capabilities and resiliency options, as well as solid security hygiene practices.

CASTING A TIGHTER NET

Although the tools and techniques to conduct a ransomware cyber attack have been around for years, they've only recently evolved. Threat actors have proven ransomware to be both enormously profitable and extremely low risk, largely due to the decreased likelihood of being caught and prosecuted. This assumed anonymity has led to a substantial increase in attacks over the past year. Additionally, the movement from physical record-keeping to digital storage methods for critical, proprietary, and/or sensitive information has also spurred an increase in attacks. The recent influx of publicly disclosed attacks, including the widely reported incidents resulting from WannaCry, signals an evolution to a model where cybercriminals are increasingly focusing their attention on extortion schemes that are likely to result in a large cash payout. Given that ransomware was initially opportunistic in nature with small monetary gains, it should come as no surprise that organizations are now targeted for the increased payout potential. Booz Allen is monitoring related activity from several angles to include:

- Ransomware types
- Delivery mechanisms
- Targeted organizations
- Targeted systems.

ATTACK, ADAPT, REPEAT

As threat actors test the water, we're typically seeing two types of ransomware attacks:

1. Phishing. Threat actors have sought to spread ransomware via widespread spam that includes leveraging a well-known vulnerability in Windows and Windows Server operating systems that initiate the malware downloading process when clicked. New reports suggest attempts to increase the sophistication and realism of the spam emails. In recent cases, TeslaCrypt ransomware was distributed via emails disguised as United States Postal Service messages with malicious attachments appearing as receipts.[1] In a similar campaign, threat actors attempted to dupe Windows-based users into downloading attachments weaponized with Locky ransomware or the Dridex Trojan by disguising them as Bank of America invoices; in this particular case, there are reportedly up to 11 different customized versions of the email.[4]

2. Compromised Website. A common attack vector for multiple kinds of malware, Web compromises and the use of exploit kits (EK) are another popular method for distributing ransomware. For the latter, Booz Allen has noted the increased use of the Angler and Nuclear EK's in Locky ransomware distribution. What's interesting is that the previously referenced Locky spam campaign and the Angler EK distribution effort both use the same command and control infrastructure and Bitcoin wallet, suggesting that the group behind this ransomware campaign is seeking multiple attack vectors to maximize access to potential victims.[5]

SYSTEMATIC ENCRYPTION

Regardless of the specific ransomware variant, attack vector, or method used to deploy it, once the ransomware is successfully activated it follows a standard process on the victim's computer. First, it systematically encrypts each file it finds, excluding important operating system files, so the system can continue to function in order to facilitate victim notification and ransom payment. Next, files in mapped network folders, and even unmapped network folders that are available to the victim, will be encrypted. This includes files in cloud storage services that back up or synchronize files in real-time. The ransomware changes each file name and leaves "help" files throughout the victim's computer systems that provide instructions for paying the ransom with Bitcoins in exchange for the decryption key—all of which is done anonymously through TOR.

HOW TO GET AHEAD

While the threat of ransomware is very real, there are numerous actions you and your organization can, and should, take in order to ensure your cyber security program is poised and prepared to meet this challenge:

Protect and Prepare

- Conduct continuous data protection in the form of incremental block-level replication, which combined with a journal, gives the ability to recover in minutes and be able to test recovery data in an isolated network.
- Ensure robust patch management of operating systems and updates to third-party software.
- Restrict privileged access to endpoints and servers to reduce the risk of administrative rights being leveraged during an attack.
- Implement advanced endpoint protection solutions that focus on Indicators of Compromise and Application Whitelisting.
- Create a playbook that addresses specific ransomware attack issues such as payment, backup restoration, and communication.
- Test backups on a regular basis to validate restoration capabilities and timelines.
- Identify malicious activity as quickly as possible by forwarding all applicable logs to an aggregation solution such as Splunk and tailor the detection logic for indicators of malware.

Recovery

- Conduct exercises to ensure impacted systems can be recovered quickly and completely.
- Attempt to recover the impacted system(s) with decryption tools that are available for numerous ransomware variants.
- If ransom payment is an option, implement the plan to transfer bitcoins to the attackers quickly. Consider the use of a third-party proxy to manage the transaction.

THE TIME IS NOW

Ransomware is a highly effective tool in the threat actor repository—and it's growing more sophisticated and lethal by the day. Indications show that healthcare, retail, and manufacturing sectors will be the primary target of ransomware attacks going forward. This is largely the result of threat actors seeking to increase profit margins by switching focus from widespread, but less effective, attacks on individual users to target corporations specifically. Cyber security leaders need to be prepared to address the risk ransomware poses to their networks, and their organization's business. With recent headlines of ransomware attacks, your customers, employees, and stakeholders will demand security against ransomware threats. The companies that earn trust will win out in the long term, by demonstrating the commitment and ability to reduce the risk—as well as communicate, manage, and fix a problem when a ransomware incident does occur.

$5B

Predicted victim ransomware payments in 2017.[5]

$6T

Predicted annual cost of cybercrime to the World by 2021.[5]

65%

Of respondents paid the ransomware demands and it took an average of 33 person hours to contain and re-mediate the original infection.[4]

About Booz Allen

Booz Allen Hamilton has been at the forefront of strategy, technology, and engineering for more than 100 years. Booz Allen partners with private and public sector clients to solve their most diffi cult challenges. To learn more, visit BoozAllen.com. (NYSE: BAH)

Contact

BILL PHELPS
Executive Vice President
Phelps_Bill@bah.com
+1-202-346-9816

BRAD MAIORINO
Executive Vice President
Maiorino_Bradley@bah.com
+1-202-346-9822

1 "TeslaCrypt Continues Its Tirade," AppRiver, February 23, 2016, accessed February 24, 2016, http://blog.appriver.com/2016/02/teslacrypt-continues-its-tirade/
2 Derek, "Bank of America Invoice Attached – word doc malware," My Online Security, February 22, 2016, accessed February 22, 2016, http://myonlinesecurity.co.uk/bank-of-america- invoice-attached-word-doc-malware/.
3 Proofpoint, "Dridex Actors Get In the Ransomware Game With "Locky," 16 February 2016, accessed 17 February 2016, https://www.proofpoint.com/us/threat-insight/post/Dridex- Actors-Get-In-the-Ransomware-Game-With-Locky.
4 Trend Micro Simply Security, "New Trend Micro Ransomware Research Shows Firms Should Wise Up, Not Pay Up,", September 8, 2016, http://blog.trendmicro.com/new-trend-mi cro-ransomware-research-shows-firms-wise-not-pay/
5 Cybersecurity Ventures, "Ransomware Damage Report, " May 18, 2017, http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/