Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

AUGUST 2021

AS CYBERATTACKS EVOLVE, BUSINESSES MUST ADAPT

Criminals have become more patient and sophisticated, making them more difficult to detect. Devon Bryan, our Chief Information Security Officer, explains how the human firewall and additional tactics deter Business Email Compromise (BEC) and other scams in an article developed by Wall Street Journal Custom Content available at: https://partners.wsj.com/mufg/overcoming-challenges/as-cyberattacks-evolve-businesses-must-adapt/.

RANSOMWARE: UNDERSTANDING AND MANAGING THE IMMINENT THREAT

A primary threat to any and all businesses and agencies is ransomware.

How it works

Typically, ransomware infects a system through phishing emails, attachments, and/or links.

Prior to each attack, the cybercriminal analyzes the network and assets to identify weaknesses, assess traps, and determine whether the organization is worth attacking.

The ransomware malware attack encrypts data in the system or blocks access to it. Then, the criminal demands a ransom to decrypt the files.

Ransomware Categories

There are two types of ransomware and two tactics related to ransomware.

Crypto ransomware: Encrypts the most valuable files and prevents access until demands are met and the cybercriminals provide the data key. Without the key, the data cannot be recovered.

Locker ransomware: Locks an organization out of all systems until demands are met.

Scareware: Manipulates users into unfavorable actions like downloading and buying malicious software. It can be used to distribute ransomware and also fake law enforcement agency notifications.

Leakware (a.k.a., Doxware): Steals data and threatens to make it public until demands are met.

An ever-changing threat

Ransomware attacks are evolving continuously, which is part of what makes ransomware a powerful threat. For example, now that organizations often choose to recover data from backups rather than pay ransoms, many attackers employ a double-extortion strategy. They both encrypt files and prevent access, and also steal and threaten to make information public.

New variants surface routinely, but they typically rely on similar tactics.

(continued)

RANSOMWARE ALERTS, RESOURCES, AND RESPONSE GUIDANCE

The U.S. Government launched StopRansomware.gov to help public and private organizations defend against the rise in ransomware cases. The site provides threat information and guidance in order to mitigate the risks. It also provides a Ransomware Response checklist.

Source: Cybersecurity and Infrastructure Security Agency (CISA). *New StopRansomware.gov website—The U.S. Government's One-Stop Location to Stop Ransomware.* CISA. July 15, 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location.

MUFG Union Bank, N.A.
A member of MUFG, a global financial group

MUFG

Ransomware-as-a-Service (RaaS)
Developers employ the RaaS subscription business model that enables affiliates to deploy already developed ransomware attacks.

This drops the barrier to entry because the extensive coding knowledge previously required is no longer needed—anyone who meets the affiliate membership requirements can pursue victims. Affiliates receive high dividends for successful ransom payments with an elevated chance of success, and a low chance of discovery. RaaS adoption is on the rise, resulting in more targets.

DARKSIDE RANSOMWARE

DarkSide is ransomware-as-a-service (RaaS) that enables the ransomware developers to receive a share of the proceeds from the cybercriminal actors who deploy it (i.e., affiliates). Since August 2020, DarkSide actors have targeted large, high-revenue organizations, resulting in the encryption and theft of sensitive data.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Federal Bureau of Investigation (FBI) provide DarkSide technical details and risk mitigations in their joint *Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*.

Source: Cybersecurity and Infrastructure Security Agency (CISA). *Alert (AA21-131A) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*. CISA. May 11, 2021. https://csrc.nist.gov/publications/detail/nistir/8276/final.

Defending against attacks
Develop a layered security posture to defend against ransomware.

- **Maintain security awareness.** Develop campaigns to remind employees of best practices (e.g., avoid clicking on unknown sender links and attachments).
- **Set Group Policy Objects (GPOs) rules.** GPOs control the execution of files on endpoints. Examples: block file execution from specific directories, disable attachment-based file executions, restrict control panel access.
- **Provide multi-layered protection on endpoints.** Layer protection that can include antivirus software, firewalls, endpoint detection and response (EDR), and an endpoint protection platform (EPP).
- **Back up data.** Separate backups from the system so that they are not affected as part of a ransomware attack. Consider all options because each comes with a degree of risk.
- **Restrict administration rights on endpoints**. Reduce user privileges to decrease the attack surface.

As ransomware and security technologies advance, revisit the strong defense with maintenance and improvements.

Source: Levine, Josh. 7 things every CISO must know about ransomware. Security Magazine. May 6, 2021. https://www.securitymagazine.com/articles/95140-things-every-ciso-must-know-about-ransomware.

CUSTOMIZED, MEASURABLE SECURITY AWARENESS PROGRAMS SUPPORT A CYBERSECURE CULTURE

Enterprise security awareness programs typically train all employees the same way using phishing simulation exercises and online learning modules. They are not provided frequently enough to remain top of mind for employees and do not target the needs of at-risk users.

Take steps to implement a behavior-based, individual approach to effectively teach the correct conducts and establish a trackable, cyber-risk savvy culture:

- Take advantage of data, including each employee's role, risk profile, and awareness level to personalize content.
- Include guidance on phishing, peer-to-peer software, personal cloud storage, public Wi-Fi, risky apps, and visiting compromised websites.
- Track and measure metrics (e.g., phishing and malware rates, two-factor authentication and password manager usage) to monitor employee behavior changes.

Source: Venkataraman, Sai. *Security awareness programs: The difference between window dressing and behavior change*. Help Net Security. March 8, 2021. https://www.helpnetsecurity.com/2021/03/08/security-awareness-programs/.

EMBEDDING SECURITY IN OPERATIONS

As operations move from analog to digital, organizations need to productize security. This means that security is not driven by just the CISO and CIO, but engrained in the operational roadmap and planning and lifecycle management. Security convergence needs to occur for IT, operational technology, and physical security.

For suppliers, risk management goes beyond securing data and IT infrastructure to also include product security. Vendor risk policies need to be updated as supplier products and services become digital.

Instead of taking a static security approach, prioritize incorporating new security solutions to meet the demands of evolving threats.

Source: Uskert, Michael. *Ransomware is an operational problem*. Gartner, Inc. May 14, 2021. https://blogs.gartner.com/beyond-supply-chain-blog/ransomware-is-an-operational-problem/.

This *Cybersecurity News* contains news and information designed to help protect your company and employees.

8913482-M-Online (08/21)