Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

FEBRUARY 2020

THE BEST LINE OF DEFENSE AGAINST RANSOMWARE: BACKUPS

Ransomware attacks are becoming more targeted, sophisticated, and costly. Since early 2018, the incidence of broad,indiscriminate ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information. In its October 2019 Public Service Announcement (PSA), the FBI also reports state and local governments along with healthcare, industrial, and transportation organizations have notably fallen victim to ransomware attacks.

Ransomware system infection techniques

Cybercriminals have upgraded techniques to make their attacks more effective and to prevent detection. Techniques include:

Email phishing

The cybercriminal sends an email containing a malicious file or link that deploys malware when clicked.

- More recent ransomware campaigns have been more targeted, but typically cyber criminals use generic, broad-based spamming strategies to deploy malware.
- Criminals may also compromise a victim's email account by using precursor malware that enables the cybercriminal to use a victim's email account to further spread the infection.

Exploiting Remote Desktop Protocol (RDP) vulnerabilities

RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer. After they have RDP access, criminals deploy a range of malware—including ransomware—to victim systems.

Criminals employ trial-and-error to obtain user credentials and credentials purchased on darknet marketplaces to gain unauthorized RDP access to victim systems.

Exploiting software vulnerabilities

Cybercriminals take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware. They exploit vulnerabilities in remote management tools used by managed service providers (MSPs) to deploy ransomware on the customers of those networks.

How to help protect against ransomware

A system of backups is the most important defense against ransomware. With a recent backup of critical data, you can prevent a ransomware attack from crippling your organization.

Because ransomware techniques and malware continue to evolve, prevention is not enough. Contingency and remediation planning and ongoing plan testing are critical for business continuity.

What is Ransomware?

Ransomware is a form of malware that encrypts files on a victim's computer or server, making them unusable. The cybercriminal then demands a ransom in exchange for providing a key to decrypt the victim's files.

Best practices for ransomware prevention

- Verify backup integrity. Ensure backups are not connected to the computers and networks they are backing up (e.g., physically store them offline).
- Increase awareness and training.
- Patch device operating systems, software, and firmware.
- Automatically update antivirus and antimalware solutions.
- Configure access controls with least privilege.
- Disable macro scripts from Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- Prevent the execution of programs in common ransomware locations (e.g., temporary folders).
- Employ best practices for use of RDP, including auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts.
- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units. For example, sensitive research or business data stored separately from the email environment.
- Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall. For example, require users to type information or enter a password when their system communicates with websites uncategorized by the proxy or firewall.

Source: Federal Bureau of Investigation (FBI) Public Service Announcement. *Alert Number I-1—219-PSA: High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, October 2, 2019. https://www.ic3.gov/media/2019/191002.aspx.

(continued)

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

MUFG

UNDERSTANDING INSIDER THREATS: INTENTIONAL VS. UNINTENTIONAL

While anyone with authorized access to company resources can be an insider threat—wittingly or unwittingly—only 14% of organizations indicate they are concerned about insider attacks from existing employees responding to a recent KnowBe4 poll. Yet 76% of the organizations polled say the biggest and most persistent security threat comes from careless end users who unintentionally put organizations at higher risk of falling victim to email phishing, ransomware, CEO fraud scams, and malware when they click on bad links.[1]

For unintentional threats, ongoing training that instills a secure culture, limiting data access, and using secure access (e.g., two-factor authentication, strong passwords, VPN access) can help innocent employees from inadvertently placing an organization at risk.

INSIDER THREAT
Intentional threat – A person or organization with an intention to inflict harm on an organization.
AND
Unintentional threat – Negligent insiders who harm the organization without malice or intent

For intentional threats, employees can be the best defense when they pay attention to the behaviors of employees and business partners. In the FBI brochure, *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*, the FBI profiles insider threat cases that include scientists, programmers, and others stealing trade secrets to sell them to foreign governments and other organizations. The FBI also shares motives, factors and behavioral indicators insider threats:

Motives

- Anger/Revenge: Disgruntlement to the point of wanting to retaliate against the organization. Dissatisfaction may be caused by a lack of recognition, co-worker and management disagreements, or pending layoffs.
- Ideology: A desire to help a particular cause or an allegiance to a person, company, or country.
- Adventure/Thrill: Intrigued by clandestine activity and living life as a spy.
- Vulnerability to blackmail: Drivers may be extra-marital affairs, gambling, or fraud.

Organizational factors

- The availability and ease of acquiring sensitive information, sometimes by those who do not need, but still have, access privileges. Physical access to and from a facility or network system with protected materials.
- Proprietary information that is not labeled as classified or incorrectly labeled.
- Undefined work-from-home policies on sensitive projects.
- A perception of lax security with minimal to no consequences for theft.
- Time-pressured employees who inadequately secure proprietary materials and/or disregard consequences of their actions.
- No training on how to protect sensitive information correctly.

Spying and stealing behaviors

- Taking or copying documents, data drives, or email without need or authorization.
- Interest outside the scope of duties or in classified information.
- Remote access while sick or on vacation or other abnormal times. Working odd hours without authorization or enthusiasm for overtime, weekend, or unusual schedule work.
- Disregard for policies on installation of personal software or hardware, access to restricted websites, unauthorized searches, or download of confidential information.
- Unreported foreign contacts (particularly with foreign government officials or intelligence officials) or other suspicious contacts and unreported overseas travel. Short trips to foreign countries for unexplained or questionable reasons.
- Affluence unsupported by household income.
- Seemingly overwhelmed by life crises or career disappointments.[2]

For additional information, visit the U.S. Office of the Director of National Intelligence National Insider Threat Task Force (NITTF), which includes access to the Insider Threat Program Maturity Framework and the U.S. Department of Homeland Security Insider Threat Mitigation site.

[1] Sjouwerman, Stu. 2019. *KnowBe4 2019 Security Threats and Trends Report – October 2019*. September 25, 2019. https://blog.knowbe4.com/knowbe4-2019-security-threats-and-trends-report-october-2019.

[2] Federal Bureau of Investigation (FBI). *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*. https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view.

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

8913482-M-Online (02/20)