


Cybersecurity / Securing Your Work Environment

Tim Cunningham & Kyle Ackerman




1

WHAT IS RANSOMWARE?

- Ransomware is a type of malware that denies access to your system and personal information, and demands a payment (ransom) to get your access back.
- May 2019 the City of Baltimore fell victim to the first data extortion incentivized ransomware attack.
- Exfiltrating data from victim networks and leaking it if companies refuse to comply, criminal actors might be able revitalize their financial returns.

RANSOMWARE, BY THE NUMBERS



- 100% increase in ransomware attacks, fueled by the pandemic; 11.5% Anticipated global ransomware recovery costs by the end of 2021: \$20 billion
- 100% Average ransom demand in Q4 2020: \$154,100 (+34% from Q3 2020)
- 100% Average days of downtime in Q4 2020: 21 days (+11% from Q3 2020)
- 100% Percentage of ransomware in Q4 that included the threat to leak exfiltrated data: 79% (+43% from Q3 2020)
- 100% How quickly a new Remote Desktop Protocol (RDP) port – one of the top three ransomware attack vectors – is discovered after first connecting to the Internet: 50 seconds
- 100% How many misconfigured RDP ports are open to the Internet: 4.7 million
- 100% Average number of ransomware attacks that have occurred daily since January 1, 2016: 4,000
- 100% Email messages that contain malware (email phishing) is also included in the top three ransomware attack vectors: 1 in 2,000



2

Colonial Pipeline



- On May 7, 2021, Colonial Pipeline issued a statement that, due to a cyber-attack, they had partially shut down operations of their pipeline that supplies almost 50% of gasoline to the eastern United States.
- During the attack, over 100GB in corporate data was stolen in just two hours.
- The initial attack vector isn't known, but it may have been an old, unpatched vulnerability in a system.
- On May 13, Bloomberg reported that the company paid a ransom demand of close to \$5 million in return for a decryption key.

3

JBS MEAT SUPPLIER

- The JBS campaign began with a reconnaissance phase in February 2021, followed by data exfiltration from March 1, 2021, to May 29, 2021, and finally, the threat actors encrypted their environment on June 1st. This is the first time that data exfiltration, for this attack, has been identified.
- The U.S Government confirmed on June 3, 2021, that the Revil / Sodinokibigroup was responsible for the attack.
- Research discovered leaked credentials belonging to employees in JBSAustralia from early March 2021. Such credentials appeared right before data exfiltration began.
- JBS USA Holdings Inc. paid an \$11 million ransom to cybercriminals






4

CHANGES FOR CYBER INSURERS

- “Claims are growing exponentially, which will be an issue if prices cannot keep up with rising frequency”
- “greater clarity in their insurance contracts to set transparent expectations for themselves and their clients.”
- Before the pandemic, cyber insurance rates were increasing by 4% to 5%. Policyholders can expect 20% to 50% rate increases for cyber coverage throughout 2021.

U.S. Cyber Insurers Face Changing Landscape; Top 20 Cyber Insurers

5

INSURANCE RECOMMENDATIONS

TRAVELERS

Multifactor Authentication (MFA) Best Practices for Travelers CyberRisk Policyholders

Why is MFA critical?


99.9% of account compromise attacks can be blocked by MFA¹

94% of ransomware victims investigated did not use MFA²

What is MFA?
Multifactor Authentication (MFA) is the use of two or more authentication factors. MFA is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user's identity prior to granting access.

When should be protected with MFA?

- Remote Network Access
- Privileged/Administrative Access
- Remote Access to Email



6

CHANGES FOR GOVERNMENT CONTRACTS

- In one of the biggest compliance shake-ups in a decade, the Department of Defense (DoD) has replaced its self-assessment model with one of the most stringent cybersecurity frameworks ever devised: the Cybersecurity Maturity Model Certification (CMMC).
- Anyone who wants to do business with the DoD will need to be certified under CMMC. Subcontractors aren't exempt every organization throughout the supply chain will need some level of certification.
- Although currently unsubstantiated, there have already been rumors that — if successful — CMMC could be expanded to cover all government contracts in the future.

CMMC Timeline

- Late 2019:** DoD releases draft CMMC levels and associated NIST controls, gather industry feedback.
- Jan 2020:** Official CMMC levels and requirements released.
- June 2020:** CMMC requirements appear in DoD Requests for Information (RFI).
- September 2020:** DoD contractors will need to be certified by September 2020.

Additional milestones: DoD announces the non-profit in charge of certifying third-party auditors; Kick-off development of program to certify auditors; Third-party auditors are available to begin CMMC certification assessments.

stratix systems
strategic technology solutions

7

GOVERNMENT SUGGESTED ACTION

SMART CYBER HABITS
During this awareness campaign, CISA emphasizes nine key messages that promote smart cyber behaviors or actions that individuals and organizations should implement to help prevent and mitigate ransomware attacks.

① **KEEP CALM & PATCH ON**
Patching is essential for preventative maintenance that keeps machines up-to-date, stable, safe and secure against malware and other cyber threats.

② **BACKING UP IS YOUR BEST BET**
It is critical to set up offline, encrypted backups of data and to regularly test your backups. The more you automate your backup system, the more frequently you can back up your data.

③ **SUSPECT DECEIT? HIT DELETE.**
If an email looks suspicious, do not compromise your personal or professional information by responding or opening attachments. Delete junk email messages without opening them.

stratix systems
strategic technology solutions

8

GOVERNMENT SUGGESTED ACTION

① **ALWAYS AUTHENTICATE**
Implement multifactor authentication (MFA) to prevent data breaches and cyber-attacks. This includes a strong password and at least one other method of authentication.

③ **SECURE YOUR SERVER MESSAGE BLOCK (SMB)**
SMB vulnerabilities allow their protocols to spread laterally through connected systems like a worm. CISA recommends all IT professionals disable their SMB protocols to prevent ransomware and other malware attacks.

② **PREPARE & PRACTICE YOUR PLAN**
Create, maintain and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures for a ransomware incident.

④ **PAYING RANSOMS DOESN'T PAY OFF**
The US government recommends against paying any ransom to cyber-criminals or malicious cyber actors. Paying ransom only funds cybercriminals, and there is no guarantee that you will recover your data if you do pay.

⑤ **YOUR DATA WILL BE FINE IF IT'S STORED OFFLINE.**
Local backups, stored on hard drives or media, provide a sense of security in case any issues occur. Keep your backup media in a safe and physically remote environment.

⑥ **RANSOMWARE REBUILD & RECOVERY RECOMMENDATIONS**
Identify the systems and accounts involved in the initial data breach and conduct an examination of existing detection or prevention systems. Once the environment is fully cleaned and rebuilt, issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or viability.

stratix systems
strategic technology solutions

9

10 LAYERS OF SECURITY

Layers from top to bottom: 24/7 SECURITY MONITORING SERVICES, INCIDENT MANAGEMENT, HUMAN PROTECTION, AUTHENTICATION PROTECTION, FIREWALL PROTECTION, DATA PROTECTION, EMAIL PROTECTION, INTERNET PROTECTION, ANTIVIRUS PROTECTION, PATCH MANAGEMENT PROTECTION.

stratix systems
strategic technology solutions

10

QUESTIONS?

For More Information:

- www.StratixSystems.com
- E-mail: sgriffith@stratixsystems.com
Shelby Griffith

stratix systems
strategic technology solutions

11