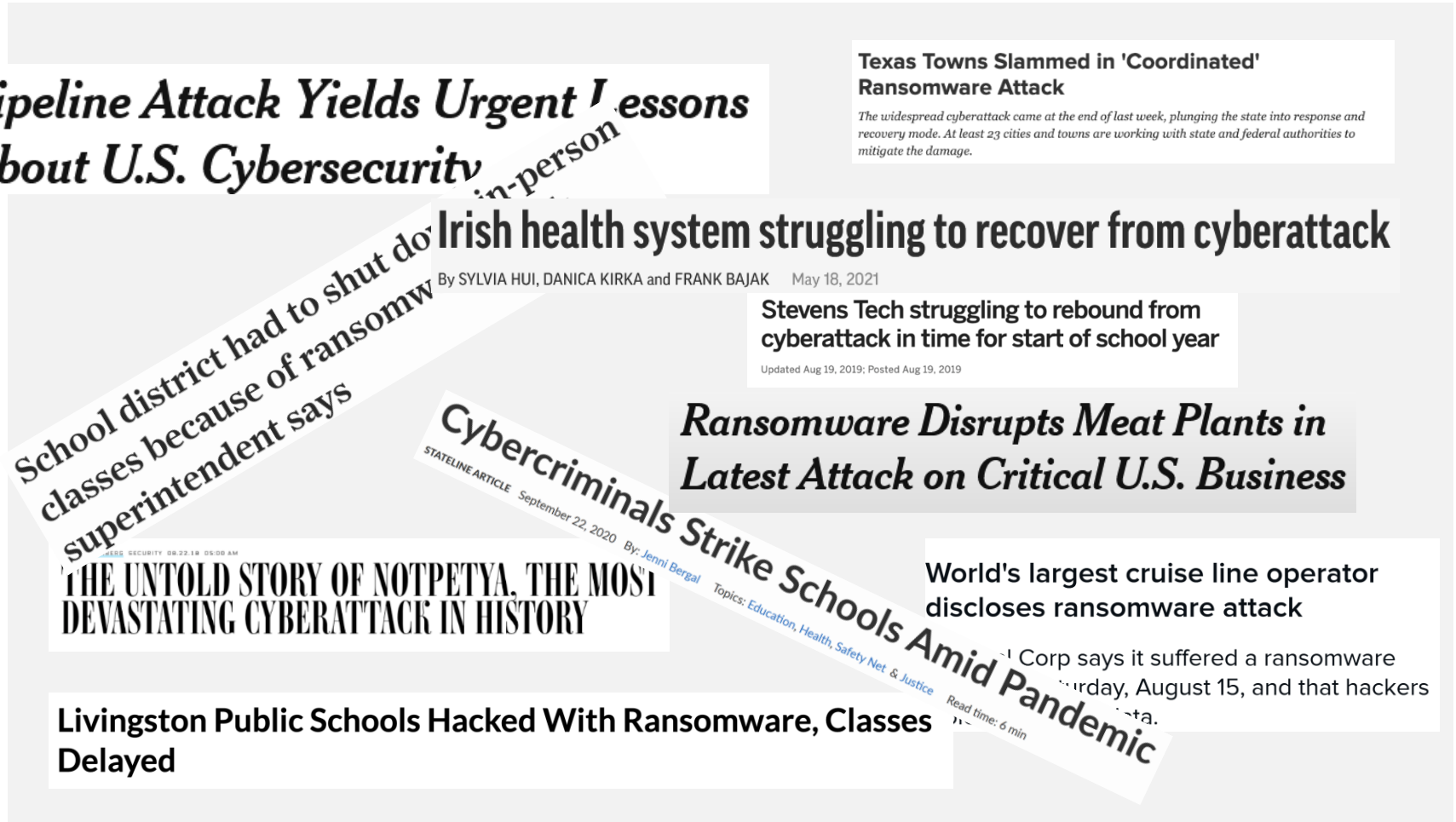
NJCCIC

PROTECT, DEFEND, RESPOND

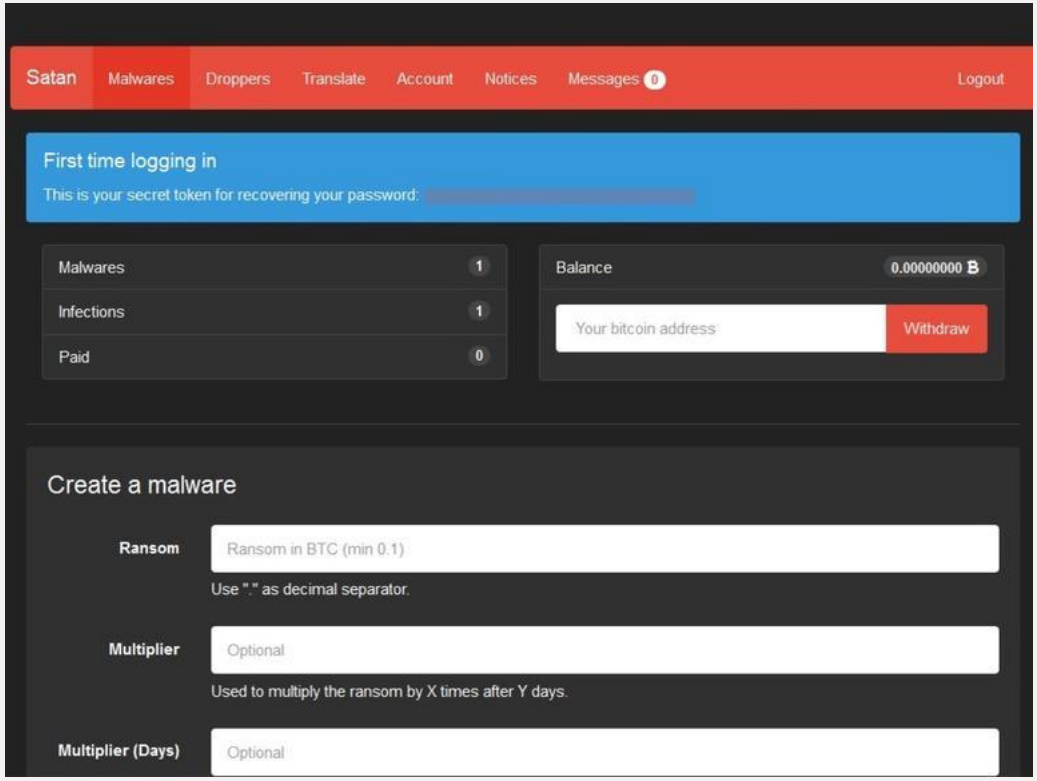
cyber.nj.gov

The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) is known as the Division of Cybersecurity of the New Jersey Office of Homeland Security and Preparedness (NJOHSP). NJOHSP helps to direct prevention, detection, protection, response, and recovery planning, not only at the State level, but also at the regional and national levels with our varied partners. NJOHSP is comprised of four Divisions: Intelligence, Policy and Planning, Cybersecurity, and Administration.

Ransomware



Ransomware-as-a-Service



Ransomware – Q1 2021

Average ransom amount paid in Q1 2021 was between $220,298 + from Q4

Average downtime is 23 days

Top attack vectors:

Phishing
RDP Compromise
Software vuln +

Ransomware costs in 2020 estimated at $20 billion

77% of cases include data exfiltration

Top Targets:

Healthcare and professional services

*According to Coveware and Purplesec

Ransomware – Q2 2021 - Evolution

Average ransom amount down 38% to $136,576

Average downtime is 23 days

Top attack vectors:

Phishing
RDP Compromise
Software vuln

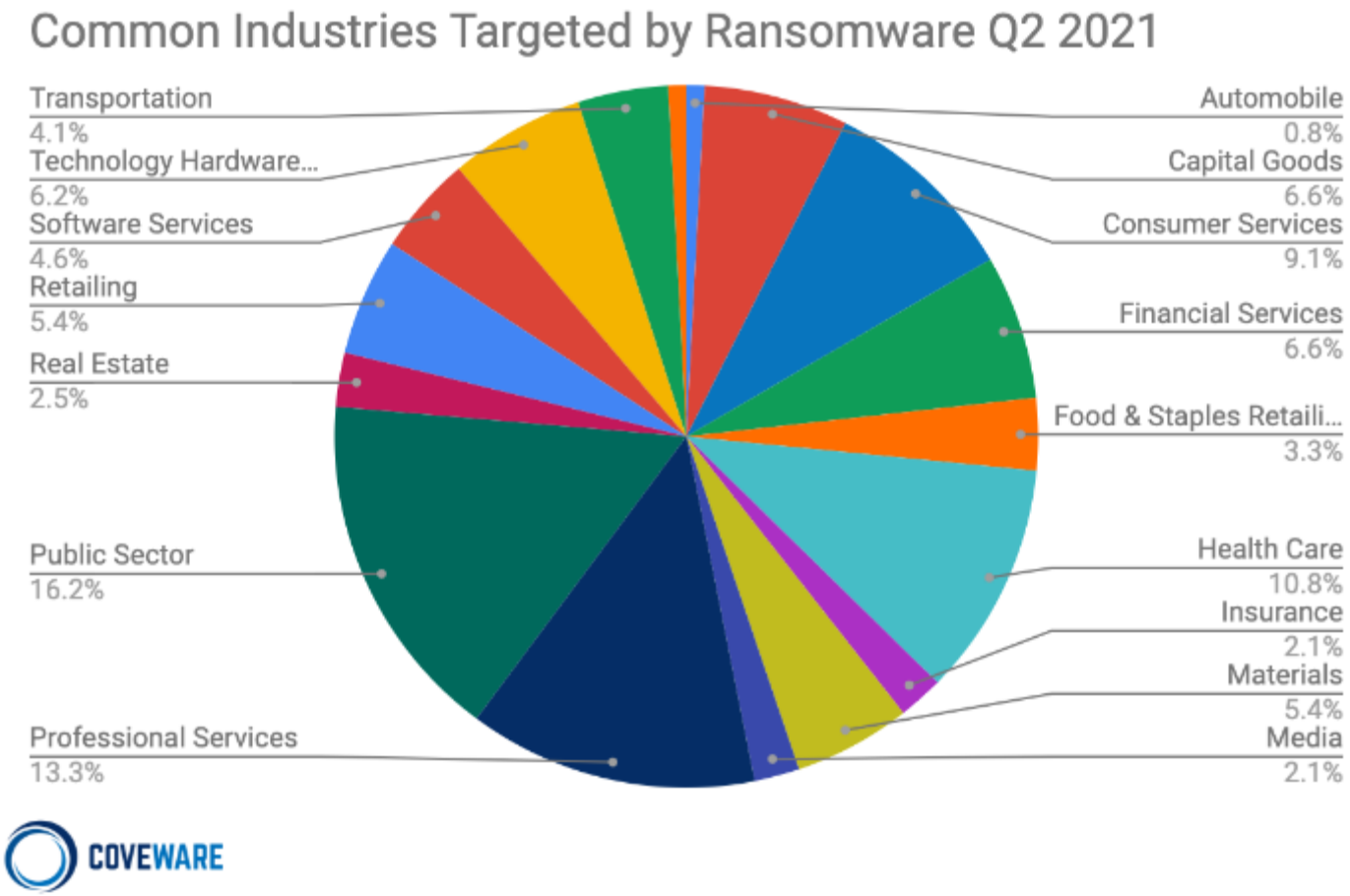
Ransomware focus by heads of state, LE, CEOs, & Insurance Co

81% of cases include data exfiltration

Top Targets:

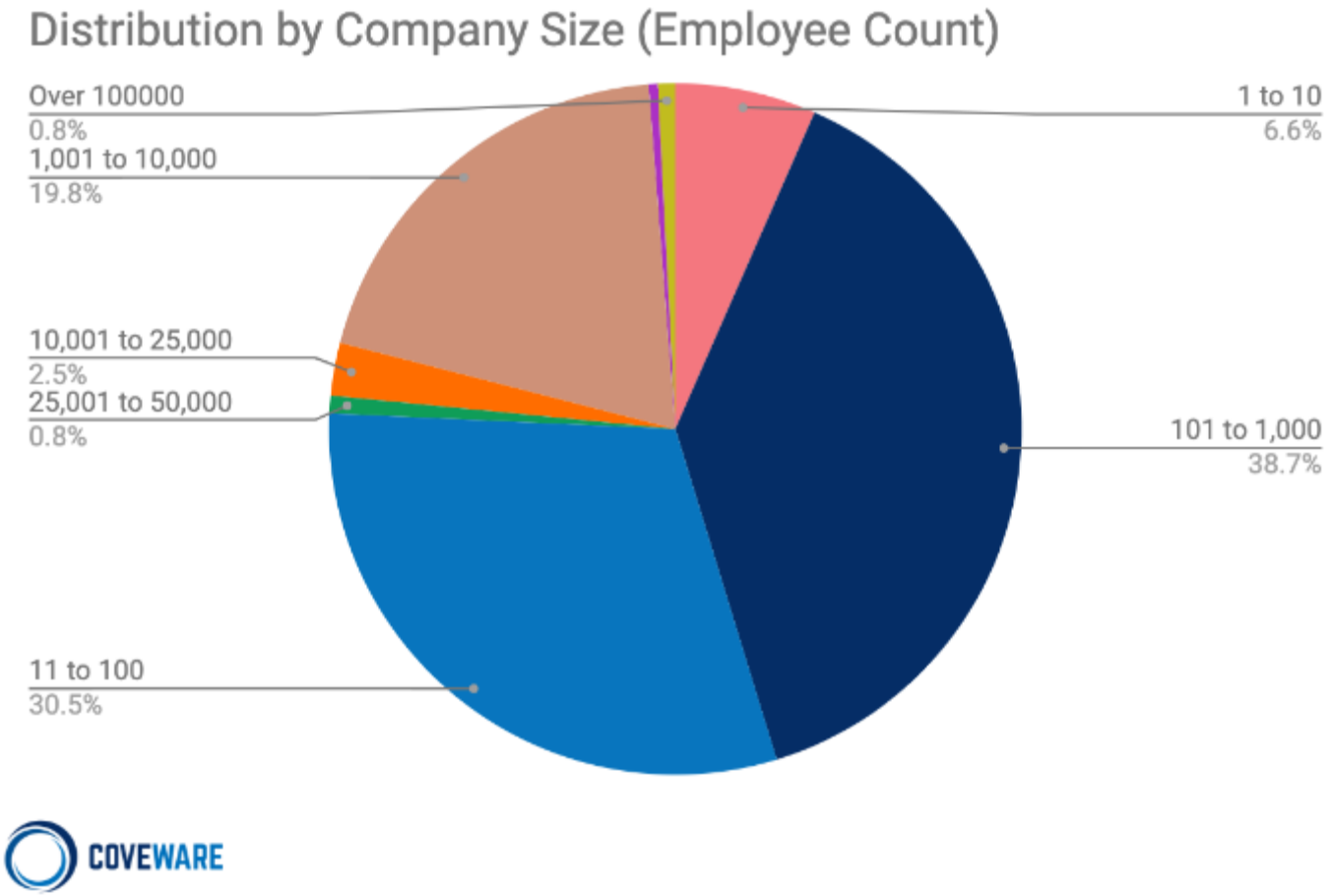
Public Sector and Professional Services

Ransomware targets



COVEWARE

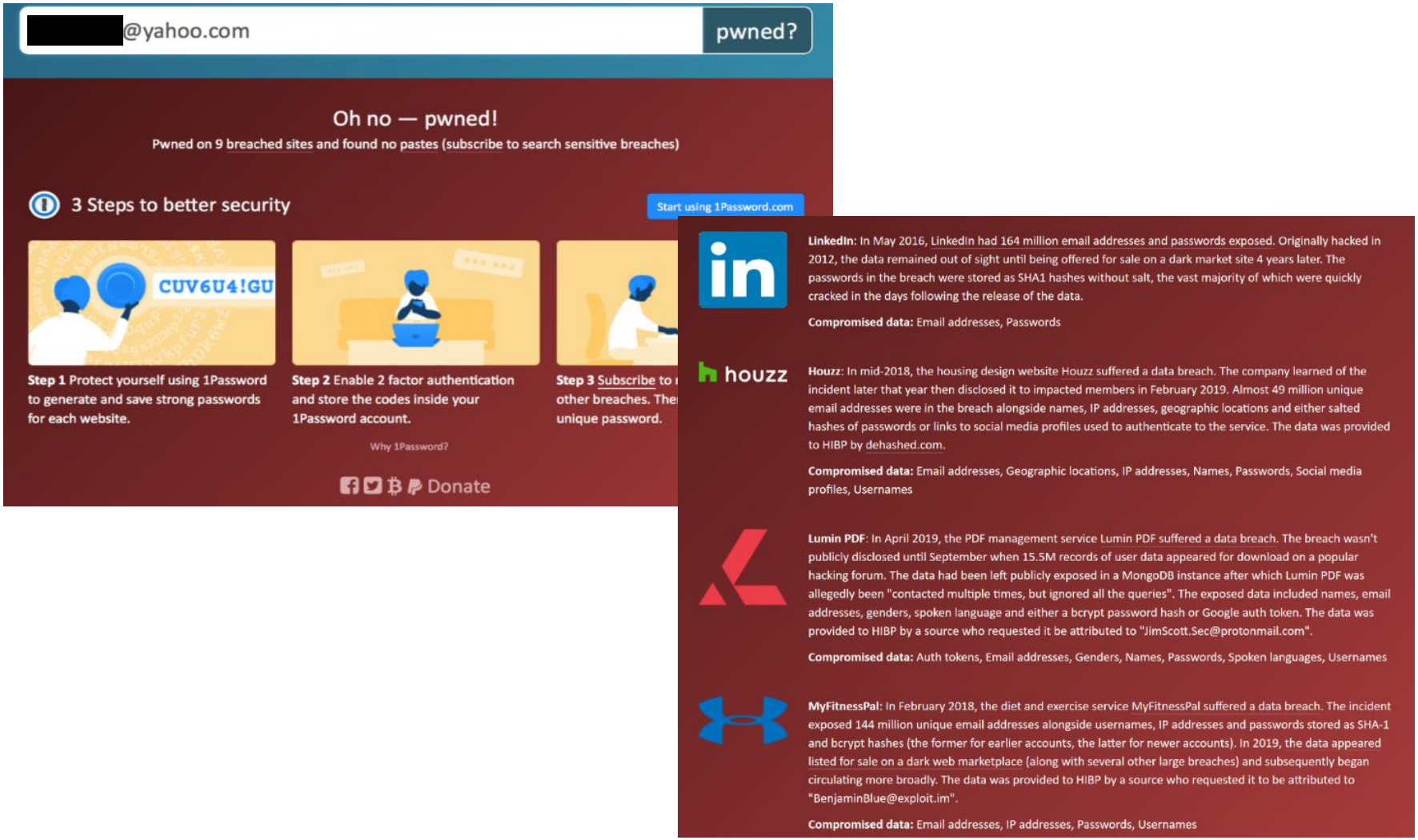
Ransomware Targets



Credential Compromise

Why are credentials the keys to the kingdom?

HaveIBeenPwned.com

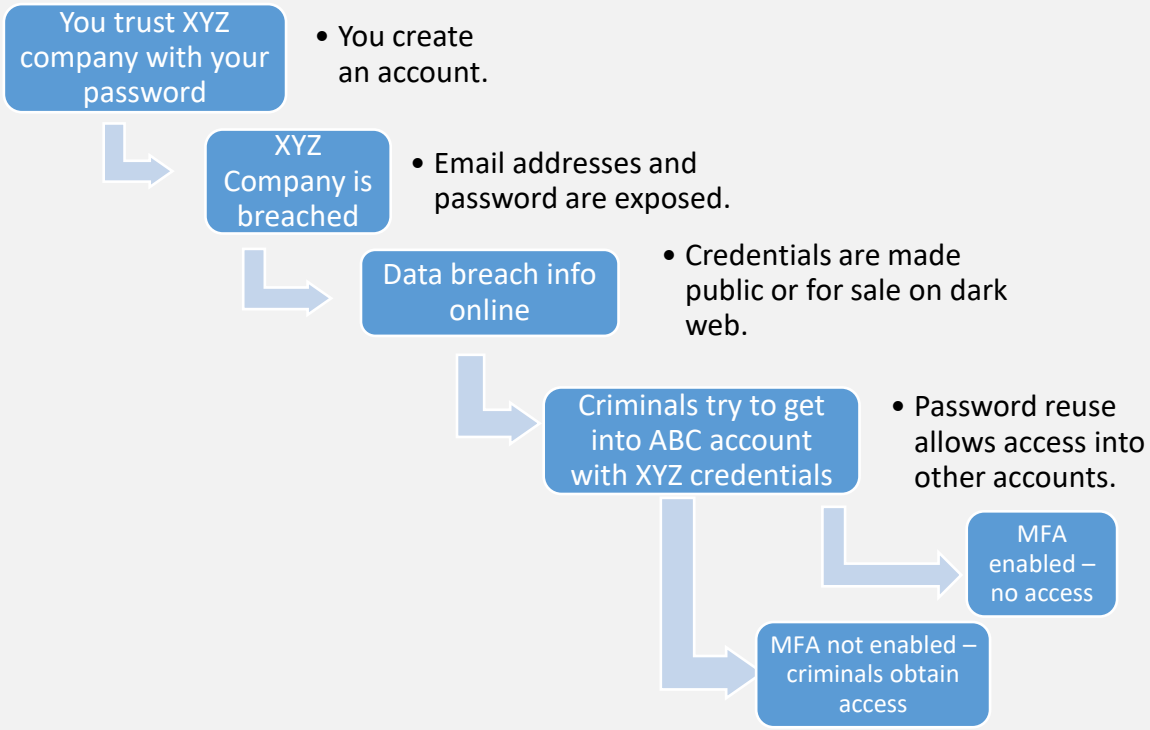


Credential Compromise

Best method to protect against account compromise as a result of credential theft

Choose authentication apps or hardware tokens over SMS or email codes

Why Multi-Factor Authentication Matters



Increase resiliency

Data Backups

- Keep backups OFF the network
- Store in separate and secure location
- Test backups regularly
- Keep multiple copies

Encrypt Data

- Encrypt sensitive data at rest and in transit
- Exfiltration of data prior to ransomware is increasingly common

Business Continuity

- Establish COOPs and Incident Response
- Test these plans
- Modify plans

What Can We Do?

- Separate IT and OT networks
- Enable MFA for ALL users
- Keep hardware/software updated
- Employ security technologies and manage them
- Close unnecessary connections (ports)
- Educate!

Ransomware

Ransomware

To view a complete list of all known ransomware variants, click here.

Learn More About How Ransomware Works +

What is Ransomware?

Ransomware is a type of malicious software (malware) that attempts to extort money from victims by restricting access to a computer system or files. The most prevalent form of this profit-motivated malware is crypto-ransomware, which encrypts files into encoded messages that can only be decrypted (decoded) with a key held by the malicious actor.

How Does Ransomware Work?

- Ransomware infections occur when a user opens a malicious email attachment, clicks on a malicious link, or visits a website infected with malicious code, known as a drive-by download.
- Once a system is infected, the ransomware contacts a command and control (C2) server to generate an encryption key and begins encrypting files on the victim's machine.
- The ransomware runs quietly in the background performing in-depth searches of all disk folders, including removable drives and network shares, and encrypts as many files as it can.
  - Ransomware may also delete Shadow Volume Copies, destroy restore points, and overwrite free disk space to prevent victims from recovering their files and systems without paying the ransom.
  - If a system is powered off as files are being encrypted, some ransomware variants resume where they left off when the system or device is powered on again.
- After files are encrypted, a ransom note is displayed on the screen with instructions on how and where to pay the ransom and the length of time before the hacker or software destroys the decryption key.
  - Some recent variants offer victims a 'second chance' to pay after the initial timer expires; however, the 'second chance' is often at least double the original ransom amount.
- If the victim pays the ransom, the malware is supposed to contact the C2 server for the decryption key and begin decrypting the victim's files; however, in many cases, the files are never decrypted.
  - Some ransomware files can delete themselves in order to avoid detection and analysis by security researchers or law enforcement.

READ FULL THREAT ANALYSIS REPORT HERE >

Ransomware Mitigation Strategies

For many organizations, preventing ransomware entirely is nearly impossible, however, the impact of a successful infection can be greatly reduced if a robust data backup process is in place. Comprehensive data backups should be scheduled as often as possible and must be kept offline in a separate and secure location. The most effective method to prevent ransomware infections is to conduct regular training and awareness exercises with all employees to ensure users are proficient in safe Internet-browsing techniques and the ability to identify phishing emails. For specific recommendations for data protection, systems management, network management, mobile device management, and post-infection remediation click below:

RECOMMENDATIONS >

Connect With Us

NJCCIC@CYBER.NJ.GOV

1-833-4-NJCCIC
(1-833-465-2242)

@NJCYBERSECURITY

CYBER.NJ.GOV