MORETON & COMPANY

MUNICIPAL INSIGHTS

A Moreton & Company Public Entities Newsletter

Ransomware - Types, Techniques and Protocols

> "According to the latest research from technology corporation IBM, ransomware is one of the most damaging cyberattack methods..."

Ransomware is any type of malicious software–also called malware–that infects a victim's device or server and prevents the technology from working as it should or blocks access to certain data (e.g., confidential files or sensitive information) stored on such technology until the victim pays a ransom. Typically, the cybercriminals behind ransomware attacks demand bitcoin, a type of digital currency that can be difficult for authorities to trace. Businesses of all sizes and sectors can be targeted by ransomware, as it is not only capable of infecting personal devices but also entire organizational networks. According to the latest research from technology corporation IBM, ransomware is one of the most damaging cyberattack methods, incurring an average of more than $4.6 million in total losses per incident (not including the actual ransom payment).

Types of Ransomware Incidents

1. **Locker ransomware**–Deploying a malware program that physically locks the victim out of their device, requiring payment to access their technology. Not typically used to damage or destroy assets.
2. **Encrypting ransomware**–Malware used to gain unauthorized access to victim's device and encrypt sensitive information, making it unreadable. You may still have access to the device, but unable to view data. Payment is made in exchange for a key to decrypt the data.
3. **Leakware**–(AKA doxware or data exfiltration) Similar to encrypting ransomware; however, rather than a threat to delete data if ransom is not paid, the cybercriminal warns they will release sensitive information to the public.
4. **Destructive ransomware**–This mirrors encrypting ransomware, but data is deleted despite the payment of ransom. This is typically carried out by nation-state threat actors or large-scale hacktivist groups rather than common cybercriminals.
5. **Mobile ransomware**–This method only pertains to mobile devices. It leverages a malware-ridden application or device download. This form typically doesn't rely on data encryption procedures.
6. **Scareware**–This attack entails various scare tactics to frighten and manipulate the victim into paying a ransom, through seemingly legitimate prompts (e.g., a fraudulent virus infection alert prompting the victim to purchase security software or a message claiming to be from law enforcement that accuses the victim of a crime and demands payment for an associated fine. Scareware may either contain malware or coerce the victim into downloading malware.

Attack Vectors and Techniques

The most frequently used strategies for deploying malware and subsequent ransomware attacks are:

Phishing scams–This utilizes fraudulent messages–namely, emails–to manipulate victims into sharing sensitive information, clicking deceptive links, or opening harmful attachments. The scams rely on social engineering to trick victims (e.g., impersonating recognized senders, using threatening language or claiming urgent action is needed). This method represents nearly half (45%) of all ransomware attacks.

Software vulnerabilities–finding software vulnerabilities to provide entryways to inject malware. These may include outdated security programs, poorly written applications and unsecure third-party platforms. "Zero-day" exposures is an example, where software is new and vulnerabilities are not yet known to cybersecurity, and therefore unaddressed.

Remote desk protocol (RDP) **pitfalls**–RDP consists of digital interface allowing remote connection to other servers. Employees can retrieve files and applications stored on the network while working remotely. Organizations often leave their RDP ports exposed to the internet. Approximately 1.3 million RDP-based cyberattacks occur daily.

Credential theft–stealing a victim's credentials (leveraging password-cracking software, purchasing cracked credentials on the dark web, or brute-force techniques) they then infect the system.

Drive-by downloads–Leveraging deceptive applications, websites, or digital advertisements to pass malware onto victims' devices for future attack. These can scan a visitors' browsers for potential vulnerabilities.

Public Entities are a popular target for ransomware–Cybercriminals looking to cause widespread infrastructure damage are likely to target government organizations. These hold highly confidential data on their community members–such as property deeds and Social Security numbers. Compounding concerns, many local governments utilize outdated technology, allowing cybercriminals easier access to their systems.

Response Protocols

Although the steps an entity can take to prevent cyberattacks are numerous, we will address a few that help curtail the most prominent incidents of ransomware:

For all vectors and techniques–have penetration testing campaigns run by an IT professional, mimicking the actions of a cybercriminal to determine vulnerabilities in the system.

Phishing–Cyber Training: Have email campaigns sending out communications typically used by cybercriminals, to test employees on their tendency to click on questionable and potentially harmful emails.

Phishing–Implement email authentication technology. It monitors incoming emails and determines the validity of these messages based on specific sender verification standards. The most common is Sender Policy Framework (SPF) which focuses on verifying senders' IP addresses and domains.

RDP safeguards–have IT check for ports that are open unnecessarily.

When considering possible cyberattacks, it is said that it is more a discussion of "when" rather than "if" it will happen. Through additional employee training and IT protocols, we can delay, mitigate, and hopefully prevent a significant ransomware event.

For more risk management guidance, contact a member of Moreton & Company's Public Entity Team.

Please visit www.moreton.com/news-events/ for more information and to view other newsletters. For additional questions, please contact your Moreton & Company representative.

This newsletter is intended to inform recipients about industry developments and best practices. It does not constitute the rendering of legal advice or recommendations and is provided for your general information only. If you need legal advice upon which you can rely, you must seek an opinion from your attorney.