RansomEXX - SentinelOne

sentinelone.com/anthology/ransomexx/

RansomEXX Ransomware: In-Depth Analysis, Detection, and Mitigation

What is RansomEXX Ransomware?

RansomEXX (*aka* Defray, Defray777), a multi-pronged extortion threat, has been observed in the wild since late 2020. RansomEXX is associated with attacks against the Texas Department of Transportation, Groupe Atlantic, and several other large enterprises. There are Windows and Linux variants of this malware family, and they are known for their limited and exclusive targeting.

What Does RansomEXX Ransomware Target?

RansomEXX ransomware is known to target large enterprises and high-value targets. They have also been known to focus on those in the government and healthcare sectors as well as high-value manufacturing entities.

How Does RansomEXX Ransomware Work?

RansomEXX ransomware targets its victims through phishing and spear phishing emails. They are also known to leverage exposed and vulnerable applications and services such as remote desktop protocol (RDP) and third-party frameworks (e.g., Vatet Loader, Metasploit, Cobalt Strike).

RansomEXX Ransomware Technical Details

Specific victim details are often hardcoded into the malware samples, adding a 'personal touch' to the ransom notes and peripheral artifacts. Victim files (local) are encrypted via AES (ECB Mode). The key itself is embedded into the payloads and is encrypted via RSA-4096. Operators have also been known to rely on additional, malicious, tools including PyXie RAT, Trickbot, and Vatet Loader.

How to Detect RansomEXX Ransomware

The SentinelOne Singularity XDR Platform detects and prevents malicious behaviors and artifacts associated with RansomEXX ransomware.

Watch Video At:

https://youtu.be/sdh_FHOGuBg

If you do not have SentinelOne deployed, here are a few ways you can identify RansomEXX ransomware in your network:

Security Tools

Use anti-malware software or other security tools capable of detecting and blocking known ransomware variants. These tools may use signatures, heuristics, or machine learning algorithms, to identify and block suspicious files or activities.

Network Traffic

Monitor network traffic and look for indicators of compromise, such as unusual network traffic patterns or communication with known command-and-control servers.

Security Audits

Conduct regular security audits and assessments to identify network and system vulnerabilities and ensure that all security controls are in place and functioning properly.

Education & Training

Educate and train employees on cybersecurity best practices, including identifying and reporting suspicious emails or other threats.

Backup & Recovery Plan

Implement a robust backup and recovery plan to ensure that the organization has a copy of its data and can restore it in case of an attack.

How to Mitigate RansomEXX Ransomware

SentinelOne Singularity XDR Platform prevents RansomEXX ransomware infections. In case of an infection, the SentinelOne Singularity XDR Platform detects and prevents malicious behaviors and artifacts associated with RansomEXX ransomware.

SentinelOne customers are protected from RansomEXX ransomware without any need to update or take action. In cases where the policy was set to Detect Only and a device became infected, remove the infection by using SentinelOne's unique rollback capability. As the accompanying video shows, the rollback will revert any malicious impact on the device and restore encrypted files to their original state.

In case you do not have SentinelOne deployed, there are several steps that organizations can take to mitigate the risk of RansomEXX ransomware attacks:

Educate employees

Employees should be educated on the risks of ransomware, and how to identify and avoid phishing emails, malicious attachments, and other threats. They should be encouraged to report suspicious emails or attachments, and to avoid opening them, or clicking on links or buttons in them.

Implement strong passwords

Organizations should implement strong, unique passwords for all user accounts, and should regularly update and rotate these passwords. Passwords should be at least 8 characters long and should include a combination of uppercase and lowercase letters, numbers, and special characters.

Enable multi-factor authentication

Organizations should enable multi-factor authentication (MFA) for all user accounts, to provide an additional layer of security. This can be done through the use of mobile apps, such as Google Authenticator or Microsoft Authenticator, or the use of physical tokens or smart cards.

Update and patch systems

Organizations should regularly update and patch their systems, to fix any known vulnerabilities, and to prevent attackers from exploiting them. This includes updating the operating system, applications, and firmware on all devices, as well as disabling any unnecessary or unused services or protocols.

Implement backup and disaster recovery

Organizations should implement regular backup and disaster recovery (BDR) processes, to ensure that they can recover from ransomware attacks or other disasters. This includes creating regular backups of all data and systems and storing these backups in a secure, offsite location. The backups should be tested regularly to ensure that they are working and that they can be restored quickly and easily.