LokiLocker Ransomware May Use False Flag to Avoid Identification

msspalert.com/cybersecurity-research/lokilocker-ransomware-may-use-false-flag-to-avoid-identification/

March 23, 2022

A relatively new ransomware-as-a-service (RaaS) family known as LokiLocker is targeting Microsoft Windows users globally, BlackBerry threat researchers said.

by D. Howard Kass • Mar 23, 2022

A relatively new ransomware-as-a-service (RaaS) family known as LokiLocker is targeting Microsoft Windows users globally through a small, distributed network of affiliates, BlackBerry threat researchers said.

The malware, most likely in a beta stage release, encrypts files similar to other notables but also may have the ability to display a false flag tactic that blames Iranian actors, BlackBerry said in a recent blog post. The security provider compared LokiLocker to its namesake in Norse mythology, which often was an enemy to other gods and also acted as a hijacker of sorts.

LokiLocker was first seen in the wild in mid-August 2021. This LokiLocker is not a reconstituted version of the older ransomware family called Locky, which was notorious in 2016, or LokiBot, which is an infostealer. Most of the attacks thus far have occurred in Eastern Europe and Asia but there are other geographic instances as well. At this point, BlackBerry has not been able to determine the hackers' country of origin.

LokiLocker Ransomware Tactics

This is how LokiLocker works:

- The bug enters the victim's network, encrypts files, and demands a monetary ransom to restore access.

- The malware is written in .NET and protected with NETGuard (modified ConfuserEX) using an additional virtualization plugin called KoiVM that is publicly available on GitHub but not widely used in malware.
- Encrypts victim's files on local drives and network shares with a standard combination of AES for file encryption and RSA for key protection.
- The crew then asks the victim to email them to obtain instructions on how to pay the ransom.

Should the victim refuse to pay, LokiLocker also has wiper functionality to delete non-system files to make the system unusable. "With a single stroke, everyone loses," BlackBerry's researchers said. At this point, there is no free tool to decrypt files encrypted by LokiLocker.

LokiLocker is spread by about 30 vetted affiliates, based on samples that BlackBerry has found in the wild. Each affiliate is identified by a chosen username and is assigned a unique chat-ID number, BlackBerry said. It's possible that the LokiLocker version via brute-checker hacking tools used to automate validation of stolen accounts and gain access to other accounts with credential stuffing. This may be part of a beta testing stage, which would explain the current ties with so few affiliates, the analysts said.

Of particular interest, some of the cracking tools used to distribute the first samples of LokiLocker seem to be developed by an Iranian cracking team called AccountCrack. Still, it's not clear if the bug actually originates from Iran or the authors are trying to feint tracking.

"LokiLocker ransomware is adept at causing mayhem on the user's endpoints, and, like its namesake Norse god, can prove to be vengeful and destructive if not appeased with a (financial) offering," BlackBerry wrote. "LokiLocker's use of KoiVM as a virtualizing protector for .NET applications is an unusual method of complicating analysis. We haven't seen a lot of other threat actors using it yet, so this may be the start of a new trend."

BlackBerry is cautioning victims not to pay a ransom should an infection strike them. "Quite apart from the fact that every victim who pays the ransom perpetuates the global growth of ransomware, remember that you're dealing with criminals here, and there is no guarantee that you'll regain access to your data, even if you pay up," BlackBerry wrote. "Even if your data is restored, there is no way to know whether the threat actor planted a backdoor somewhere on your machine, for easy future access. After all, people who pay one ransom can often be persuaded to pay another."

How to Protect Against Ransomware Attacks

The FBI's general guidance vs. ransomware attacks includes these 10 recommendations:

1. Back-up critical data offline.
2. Ensure copies of critical data are in the cloud or on an external hard drive or storage device. This information should not be accessible from the compromised network.

3. Secure back-ups and ensure data is not accessible for modification or deletion from the system where the data resides.
4. Use multi-factor authentication with strong passwords, including for remote access services.
5. Keep computers, devices and applications patched and up-to-date.
6. Monitor cyber threat reporting regarding the publication of compromised VPN login credentials and change passwords and settings.
7. Consider adding an email banner to emails received from outside your organization.
8. Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
9. Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
10. Implement network segmentation.

How MSPs and MSSPs Can Respond to and Recover From Ransomware Attacks

If a ransomware incident occurs, then the CISA, FBI and NSA recommend the following four actions:

1. **Follow the Ransomware Response Checklist** on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
2. **Scan your backups.** If possible, scan your backup data with an antivirus program to check that it is free of malware.
3. **Report incidents immediately** to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.
4. **Apply incident response best practices** found in the joint Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

Return Home

No Comments

Leave a Reply

Your email address will not be published. Required fields are marked *