LokiLocker ransomware family spotted with built-in wiper

By Jeff Burt

Published: 2022-03-16 · Archived: 2026-04-05 17:46:31 UTC

BlackBerry security researchers have identified a ransomware family targeting English-speaking victims that is capable of erasing all non-system files from infected Windows PCs.

LokiLocker, a ransomware-as-a-service (RaaS) family with possible origins in Iran, was first seen in the wild in mid-August 2021, BlackBerry Threat Intelligence researchers write in a blog post today.

"It shouldn't be confused with an older ransomware family called Locky, which was notorious in 2016, or LokiBot, which is an infostealer," they say. "It shares some similarities with the LockBit ransomware (registry values, ransom note filename), but it doesn't seem to be its direct descendant."

They describe LokiLocker – named after Loki, the trickster god in Norse lore – as a "limited-access ransomware-as-a-service scheme that appears to be sold to a relatively small number of carefully vetted affiliates behind closed doors." Affiliates are identified by a chosen username and assigned a unique chat-ID number. The researchers estimate there are about 30 different such affiliates across the LokiLocker samples that they have found in the wild.

Like other cyber threats, such as distributed denial-of-services (DDoS), ransomware has evolved in recent years to include bad actors offering to lease their malware as a service to other criminals, enabling those less skilled to fire off relatively sophisticated campaigns via someone else's malicious code and backend infrastructure.

McAfee last year issued a threat report that showed a significant drop in the incidence of ransomware in the first quarter of 2021. However, the decline had less to do with cybercriminals embracing other attack methods and more with many of them using RaaS campaigns that target fewer but larger organizations that bring in more money than mass multi-target ransomware attacks.

BlackBerry researchers say there are victims around the world, which isn't surprising given that different affiliates may have different targeting patterns. Most so far are in Eastern Europe and Asia.

The researchers are still trying to determine the origins of the RaaS family but wrote that all the embedded debugging strings are in English and mostly free of the kinds of mistakes and misspellings typically seen in malware coming from Russia or China. Some of the earliest known LokiLocker affiliates have usernames that are found exclusively on Iranian hacking channels.

"Also, perhaps more interestingly, some of the cracking tools used to distribute the very first samples of LokiLocker seem to be developed by an Iranian cracking team called AccountCrack," says Blackberry. "Moreover, at least three of the known LokiLocker affiliates use unique usernames that can be found on Iranian hacking channels. It's not entirely clear whether this means they truly originate from Iran or that the real threat actors are trying to cast the blame on Iranian attackers."

In addition, the malware appears to contain a list of countries to exclude from encryption and in the samples the BlackBerry researchers have seen, the only country on the list is Iran.

"It seems that this functionality is not yet implemented, as there are no references to this array in the code," the researchers write. "However, like the references to Iranian attackers and hacking tools, it could just as well be a false flag meant to misdirect our attention" and put blame on Iran.

The malware is written in .NET and protected with NETGuard – a commercial product that the researchers call a "modified ConfuserEX," an open-source tool for protecting .NET applications – while also using KoiVM, a virtualization plugin. It used to be a licensed commercial protection for .NET applications, but after its code was open-sourced in 2018, it became publicly available on GitHub.

- Russia-linked attackers breach NGO by exploiting MFA, PrintNightmare vuln
- UK regulator puts NortonLifeLock merger with Avast on ice
- The Windows malware on Ukraine CERT's radar
- OpenSSL patches crash-me bug triggered by rogue certs

The use of KoiVM as a protector is an unusual method for complicating analysis of the malware that hasn't been seen with many other threat actors and may mark the start of a new trend, according to BlackBerry.

The ransomware uses a combination of AES for file encryption and RSA for key protection to encrypt documents on victims' local hard drives and network shares. It then tells the victims to email the attackers to receive instructions for paying the ransom.

An early sample of the ransomware was distributed inside trojanized brute-checker hacking tools, including PayPal BruteCheck, Spotify BruteChecker, PiaVNP Brute Checker by ACTEAM, and FPSN Checker by Angeal. Such tools are used to automate validation of stolen accounts and get access to other accounts through credential stuffing, in which hackers use usernames and passwords stolen from one website to log into other websites, sometimes using a botnet to accelerate the process.

"It's possible that the LokiLocker version distributed with these hacking tools constituted some kind of beta testing phase before the malware was offered to a wider range of affiliates," the researchers say.

Like other ransomware, LokiLocker puts a time limit for paying the ransom and will make the system unusable if the payment isn't made. However, if configured to do so, the malware also includes a wiper function that will erase the data if the payment deadline passes.

"It will delete files on all of the victim's drives, except for the system files, and it will also try to overwrite the Master Boot Record (MBR) of the system drive to render the system unusable," the researchers write, adding that the victims are greeted with this message: "You did not pay us. So we deleted all your files :)"

Presumably this is so that there's no chance at all to recover the scrambled documents, save from backups. In addition, after overwriting the MBR, the ransomware will try to crash the system by forcing a Blue Screen of Death.

The wiper function is part of an escalation by ransomware gangs in recent years to encourage victims to pay the ransom by including additional threats beyond just refusing to decrypt the files, such as erasing data or leaking stolen files on the dark web.

There are no free tools to decrypt files captured by LokiLocker and BlackBerry – like the FBI and other security authorities – urge victims not to pay the ransom, arguing that it adds fuel to the global growth in ransomware and there is no guarantee they will get their data returned. Also, even if it is returned, the hackers could have put a backdoor into the system, making the organization more vulnerable to future attacks.

"After all, people who pay one ransom can often be persuaded to pay another," the team at BlackBerry concludes. ®
