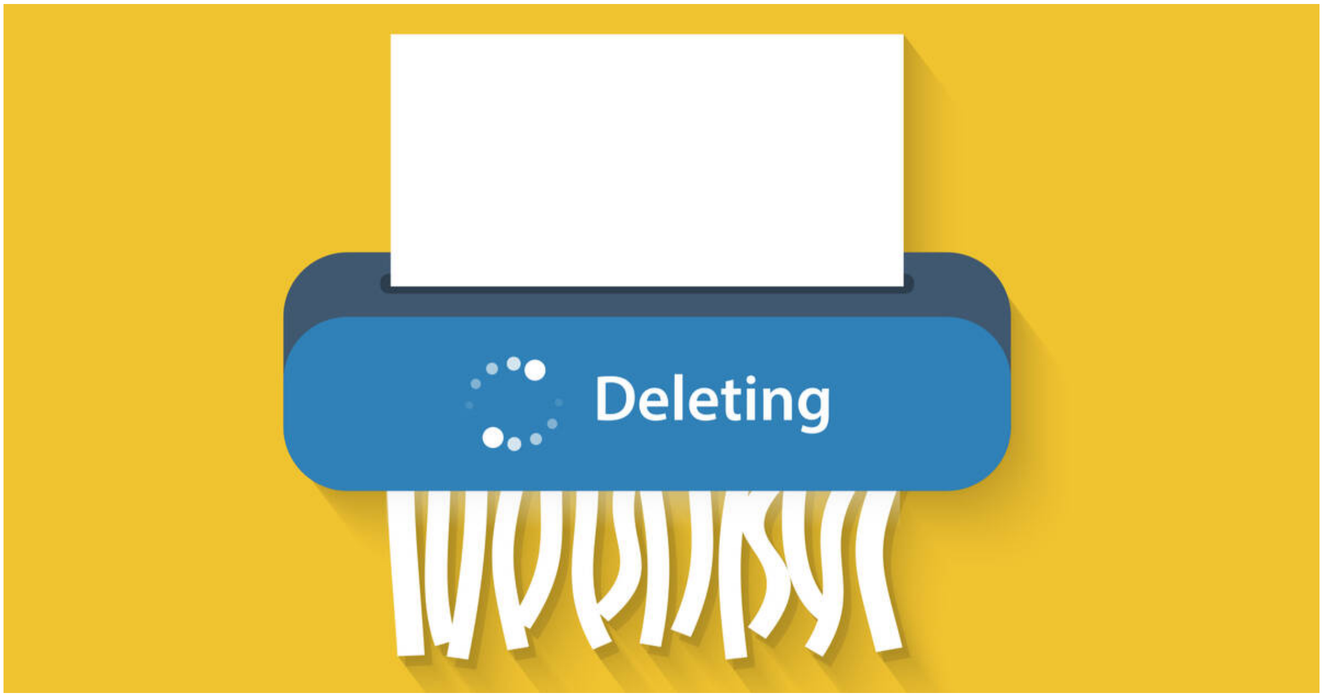
LokiLocker ransomware family spotted with built-in wiper

theregister.com/2022/03/16/blackberry_lokilocker_ransomware/

Jeff Burt



Security

BlackBerry says extortionists erase documents if ransom unpaid

Jeff Burt Wed 16 Mar 2022 // 21:00 UTC

1

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.

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. ®

Other stories you might like

- Big Tech loves talking up privacy – while trying to kill privacy legislation

  Study claims Amazon, Apple, Google, Meta, Microsoft work to derail data rules

  Thomas Claburn in San Francisco Fri 27 May 2022 // 21:48 UTC
  Amazon, Apple, Google, Meta, and Microsoft often support privacy in public statements, but behind the scenes they've been working through some common organizations to weaken or kill privacy legislation in US states.

  That's according to a report this week from news non-profit The Markup, which said the corporations hire lobbyists from the same few groups and law firms to defang or drown state privacy bills.

  The report examined 31 states when state legislatures were considering privacy legislation and identified 445 lobbyists and lobbying firms working on behalf of Amazon, Apple, Google, Meta, and Microsoft, along with industry groups like TechNet and the State Privacy and Security Coalition.

  Continue reading

- SEC probes Musk for not properly disclosing Twitter stake

  Meanwhile, social network's board rejects resignation of one its directors

  Katyanna Quach Fri 27 May 2022 // 21:26 UTC
  America's financial watchdog is investigating whether Elon Musk adequately disclosed his purchase of Twitter shares last month, just as his bid to take over the social media company hangs in the balance.

  A letter [PDF] from the SEC addressed to the tech billionaire said he "[did] not appear" to have filed the proper form detailing his 9.2 percent stake in Twitter "required 10 days from the date of acquisition," and asked him to provide more information. Musk's shares made him one of Twitter's largest shareholders.

  Musk quickly moved to try and buy the whole company outright in a deal initially worth over $44 billion. Musk sold a chunk of his shares in Tesla worth $8.4 billion and bagged another $7.14 billion from investors to help finance the $21 billion he promised to put forward for the deal. The remaining $25.5 billion bill was secured via debt financing by Morgan Stanley, Bank of America, Barclays, and others. But the takeover is not going smoothly.

  Continue reading
- Cloud security unicorn cuts 20% of staff after raising $1.3b

  Time to play blame bingo: Markets? Profits? Too much growth? Russia? Space aliens?

  Jessica Lyons Hardcastle Fri 27 May 2022 // 19:19 UTC **2**
  Cloud security company Lacework has laid off 20 percent of its employees, just months after two record-breaking funding rounds pushed its valuation to $8.3 billion.

  A spokesperson wouldn't confirm the total number of employees affected, though told *The Register* that the "widely speculated number on Twitter is a significant overestimate."

  The company, as of March, counted more than 1,000 employees, which would push the jobs lost above 200. And the widely reported number on Twitter is about 300 employees. The biz, based in Silicon Valley, was founded in 2015.

  Continue reading

- Talos names eight deadly sins in widely used industrial software

  Entire swaths of gear relies on vulnerability-laden Open Automation Software (OAS)

  Jeff Burt Fri 27 May 2022 // 18:30 UTC
  A researcher at Cisco's Talos threat intelligence team found eight vulnerabilities in the Open Automation Software (OAS) platform that, if exploited, could enable a bad actor to access a device and run code on a targeted system.

  The OAS platform is widely used by a range of industrial enterprises, essentially facilitating the transfer of data within an IT environment between hardware and software and playing a central role in organizations' industrial Internet of Things (IIoT) efforts. It touches a range of devices, including PLCs and OPCs and IoT devices, as well as custom applications and APIs, databases and edge systems.

  Companies like Volvo, General Dynamics, JBT Aerotech and wind-turbine maker AES are among the users of the OAS platform.

  Continue reading
- Despite global uncertainty, $500m hit doesn't rattle Nvidia execs

  CEO acknowledges impact of war, pandemic but says fundamentals ‘are really good’

  Dylan Martin Fri 27 May 2022 // 16:08 UTC **1**
  Nvidia is expecting a $500 million hit to its global datacenter and consumer business in the second quarter due to COVID lockdowns in China and Russia's invasion of Ukraine. Despite those and other macroeconomic concerns, executives are still optimistic about future prospects.

  "The full impact and duration of the war in Ukraine and COVID lockdowns in China is difficult to predict. However, the impact of our technology and our market opportunities remain unchanged," said Jensen Huang, Nvidia's CEO and co-founder, during the company's first-quarter earnings call.

  Those two statements might sound a little contradictory, including to some investors, particularly following the stock selloff yesterday after concerns over Russia and China prompted Nvidia to issue lower-than-expected guidance for second-quarter revenue.

  Continue reading

- Another AI supercomputer from HPE: Champollion lands in France

  That's the second in a week following similar system in Munich also aimed at researchers

  Dan Robinson Fri 27 May 2022 // 15:30 UTC
  HPE is lifting the lid on a new AI supercomputer – the second this week – aimed at building and training larger machine learning models to underpin research.

  Based at HPE's Center of Excellence in Grenoble, France, the new supercomputer is to be named Champollion after the French scholar who made advances in deciphering Egyptian hieroglyphs in the 19th century. It was built in partnership with Nvidia using AMD-based Apollo computer nodes fitted with Nvidia's A100 GPUs.

  Champollion brings together HPC and purpose-built AI technologies to train machine learning models at scale and unlock results faster, HPE said. HPE already provides HPC and AI resources from its Grenoble facilities for customers, and the broader research community to access, and said it plans to provide access to Champollion for scientists and engineers globally to accelerate testing of their AI models and research.

  Continue reading

- Workday nearly doubles losses as waves of deals pushed back

  Figures disappoint analysts as SaaSy HR and finance application vendor navigates economic uncertainty

  Lindsay Clark Fri 27 May 2022 // 14:30 UTC **7**
  HR and finance application vendor Workday's CEO, Aneel Bhusri, confirmed deal wins expected for the three-month period ending April 30 were being pushed back until later in 2022.

  The SaaS company boss was speaking as Workday recorded an operating loss of $72.8 million in its first quarter [PDF] of fiscal '23, nearly double the $38.3 million loss recorded for the same period a year earlier. Workday also saw revenue increase to $1.43 billion in the period, up 22 percent year-on-year.

  However, the company increased its revenue guidance for the full financial year. It said revenues would be between $5.537 billion and $5.557 billion, an increase of 22 percent on earlier estimates.

  Continue reading

- UK monopoly watchdog investigates Google's online advertising business

  Another probe? Mountain View is starting to look like a pincushion at this rate

  Richard Currie Fri 27 May 2022 // 14:00 UTC **3** 🗨
  The UK's Competition and Markets Authority is lining up yet another investigation into Google over its dominance of the digital advertising market.

  This latest inquiry, announced Thursday, is the second major UK antitrust investigation into Google this year alone. In March this year the UK, together with the European Union, said it wished to examine Google's "Jedi Blue" agreement with Meta to allegedly favor the former's Open Bidding ads platform.

  The news also follows proposals last week by a bipartisan group of US lawmakers to create legislation that could force Alphabet's Google, Meta's Facebook, and Amazon to divest portions of their ad businesses.

  Continue reading
- Microsoft slows some hiring for Windows, Teams, and Office

  'Making sure the right resources are aligned to the right opportunity' ahead of next fiscal year

  Richard Speed Fri 27 May 2022 // 13:31 UTC **4** 🗨
  Microsoft has hit the brakes on hiring in some key product areas as the company prepares for the next fiscal year and all that might bring.

  According to reports in the Bloomberg, the unit that develops Windows, Office, and Teams is affected and while headcount remains expected to grow, new hires in that division must first be approved by bosses.

  During a talk this week at JP Morgan's Technology, Media and Communications Conference, Rajesh Jha, executive VP for the Office Product Group, noted that within three years he expected approximately two-thirds of CIOs to standardize on Microsoft Teams. 1.4 billion PCs were running Windows. He also remarked: "We have lots of room here to grow the seats with Office 365."

  Continue reading

- Recession fears only stoking enterprise tech spending for Dell, others

  Staving off entropy with digital transformation, hybrid office, and automation projects

  Paul Kunert Fri 27 May 2022 // 13:00 UTC
  Enterprises are still kitting out their workforce with the latest computers and refreshing their datacenter hardware despite a growing number of "uncertainties" in the world.

  This is according to hardware tech bellwethers including Dell, which turned over $26.1 billion in sales for its Q1 of fiscal 2023 ended 29 April, a year-on-year increase of 16 percent.

  "We are seeing a shift in spend from consumer and PCs to datacenter infrastructure," said Jeff Clarke, vice-chairman and co-chief operating officer. "IT demand is currently healthy," he added.

  Continue reading
- GitHub saved plaintext passwords of npm users in log files, post mortem reveals

  Unrelated to the OAuth token attack, but still troubling as org reveals details of around 100,000 users were grabbed by the baddies

  Richard Speed Fri 27 May 2022 // 12:15 UTC **7**
  GitHub has revealed it stored a "number of plaintext user credentials for the npm registry" in internal logs following the integration of the JavaScript package registry into GitHub's logging systems.

  The information came to light when the company today published the results of its investigation into April's unrelated OAuth token theft attack, where it described how an attacker grabbed data including the details of approximately 100,000 npm users.

  The code shack went on to assure users that the relevant log files had not been leaked in any data breach; that it had improved the log cleanup; and that it removed the logs in question "prior to the attack on npm."

  Continue reading