New ransomware strain discovered using leaked Windows and Linux encryption

A new ransomware operation called 'Buhti' uses leaked code of the LockBit and Babuk ransomware families to target Windows and Linux systems

A new ransomware operation called 'Buhti', which uses leaked code of the LockBit and Babuk ransomware families to target Windows and Linux systems respectively, has just been discovered by international security researchers. . Although the threat actors behind Buhti (nicknamed 'Blacktail', have not yet developed their own strain of ransomware, they have created a malicious utility that can extract custom data used to blackmail victims. This tactic is also known as "double blackmail".

Buhti was first discovered in February 2023 by the Unit 42 security team of Palo Alto Networks. The group later identified it as a Go-based Linux-targeting ransomware.

Another report published recently by Symantec's Threat Hunter team shows that Buhti also targets Windows, using a slightly modified LockBit 3.0 variant codenamed "LockBit Black".

'Ransomware recycling'

Blacktail uses the Windows LockBit 3.0 generator that a disgruntled developer revealed on Twitter in September 2022.

Successful attacks will change the compromised computer's wallpaper to ask the victim to open a ransom note, while all encrypted files will receive the ".buthi" extension on them. file extension.

Picture 1 of New ransomware strain discovered using leaked Windows and Linux encryption

For Linux attacks, Blacktail uses a payload based on the Babuk source code that a threater posted on a Russian-speaking hacking forum in September 2021.

Earlier this month, SentinelLabs and Cisco Talos highlighted new ransomware activity cases using Babuk to attack Linux systems.

While malware reuse is often seen as a sign of less sophisticated hacker groups, in this case many ransomware groups have turned to Babuk due to its proven ability to invade breach VMware ESXi and Linux systems, which bring a lot of profit to cybercriminals.

Blacktail malicious group

Blacktail does more than simply mimic reuse of other hackers' tools with minimal modifications. Instead, they use their own custom filtering engine and separate network penetration strategy.

Symantec reports that the Buhti attacks took advantage of the recently disclosed PaperCut NG and MF RCE vulnerability that the LockBit and Clop teams also exploited.

Attackers rely on CVE-2023-27350 to install Cobalt Strike, Meterpreter, Sliver, AnyDesk, and ConnectWise on target computers, use them to steal credentials and move sideways into compromised networks import, steal files, launch additional payloads, etc.

In February, this group exploited CVE-2022-47986, a critical remote code execution vulnerability affecting the IBM Aspera Faspex file exchange product.

Buhti's filtering engine is capable of stealing data based on Go. It can take command line arguments specifying the targeted directories in the file system. This tool mainly steals the following file types: pdf, php, png, ppt, psd, rar, raw, rtf, sql, svg, swf, tar, txt, wav, wma, wmv, xls, xml, yml, zip, aiff, aspx, docx, epub, json, mpeg, pptx, xlsx and yaml. The stolen files are then copied to a ZIP archive and filtered out to Blacktail's servers.

Blacktail and their Buhti ransomware operation are a modern example of how effectively threat actors can abuse malware and cause significant damage to organizations.

Furthermore, the leaked LockBit and Babuk source code can still be used by ransomware groups but under a different name, leaving no connection to previous encoders.

Attacks have been recorded in the Czech Republic, China, the United Kingdom, Ethiopia, the United States, France, Belgium, India, Estonia, Germany, Spain, and Switzerland. This means Buthi is still a very active ransomware, and Blacktail remains a significant threat to organizations around the world.

Blacktail's tactic of rapidly applying exploits to newly disclosed vulnerabilities makes them a potential threat that requires increased vigilance and proactive defensive strategies such as timely patching.