# Dangerous 'Helldown' Ransomware Warning Expands to Linux and VMware

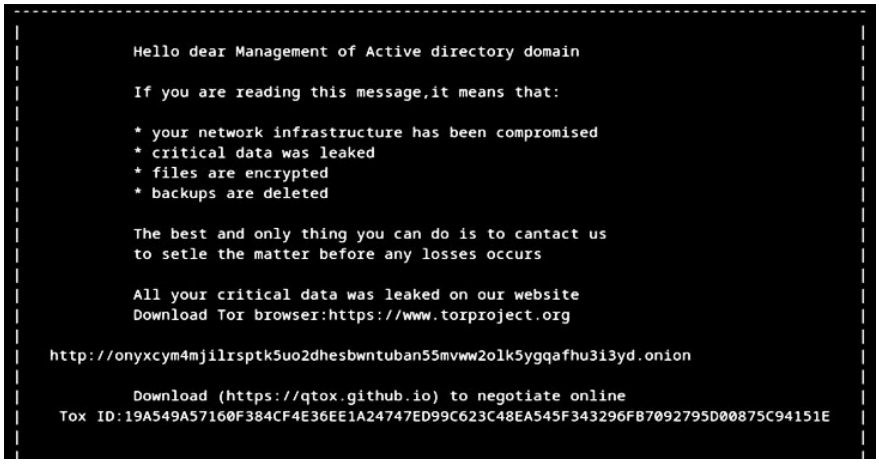
Dubbed Magniber, this dangerous ransomware strain has been around for a while now, and is ranked among the most dangerous with its diverse infection capabilities.

A dangerous ransomware strain called 'Helldown,' first discovered in the middle of this year on Windows, is now targeting VMware systems and Linux environments. This has caused serious concern among the global cybersecurity community, suggesting that the attackers behind the malware have found new ways to exploit vulnerabilities on various operating system platforms.

Helldown first gained attention in mid-2024, when it began targeting Windows systems across the globe en masse. The ransomware borrows its foundation from LockBit 3.0, another notorious ransomware family, and shares behavioral similarities with other malware strains like Darkrace and Donex. The latest Linux variant of Helldown is more dangerous in that it can also target VMware virtual machines (VMs), aiming to kill active VMs before encrypting them. Interestingly, however, researchers found that this feature is not yet fully functional, suggesting that it is still in development.

On the Windows side, Helldown's tactics are less refined than other advanced ransomware strains.

On the Windows side, Helldown's infection tactics are less refined than those of other advanced ransomware strains. For example, it uses batch files to terminate processes rather than more sophisticated embedding methods. Still, the focus on crippling virtual machines and encrypting data suggests the attackers are planning something more scalable and dangerous.



A key aspect of the Helldown Ransomware attack chain is the use of vulnerabilities in Zyxel VPN devices. Specifically, it exploits CVE-2024-42057, a command injection vulnerability in IPSEC VPNs, allowing attackers to execute OS commands using crafted usernames. Attackers exploit inappropriate vulnerabilities to breach networks. Once inside, they use simple but effective tools to escalate privileges, disable security, and exfiltrate data.

The Linux variant of Helldown is much less sophisticated than its Windows counterpart, lacking common evasion techniques like obfuscation. This simplicity suggests the malware is still in development, but it is still dangerous. Targeting VMs, on the other hand, allows ransomware operators to maximize their damage. By taking over VMS, they can disrupt critical operations in IT and other industries.

All activities of the malware are closely observed. TipsMake.com will continue to update information about this Ransomware strain, please pay attention to follow.