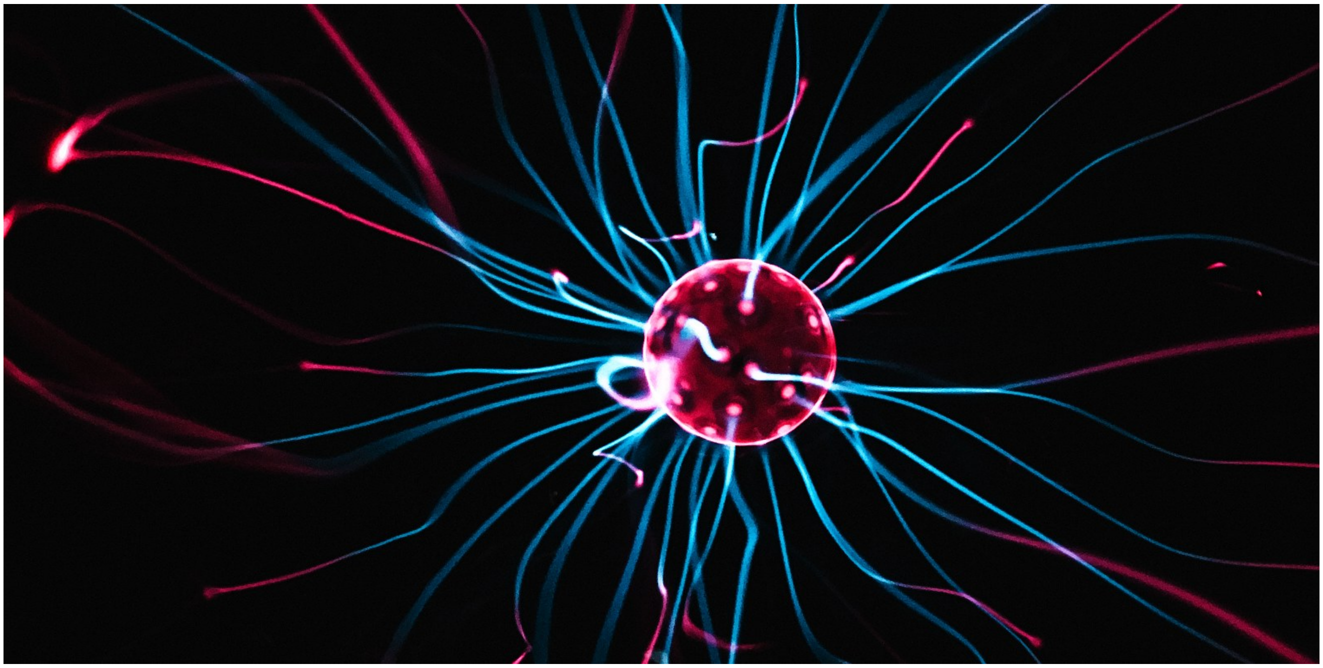
FreakOut malware worms its way into vulnerable VMware servers

bleepingcomputer.com/news/security/freakout-malware-worms-its-way-into-vulnerable-vmware-servers/

Sergiu Gatlan

By
Sergiu Gatlan

- June 4, 2021
- 09:03 AM
- 0



A multi-platform Python-based malware targeting Windows and Linux devices has now been upgraded to worm its way into Internet-exposed VMware vCenter servers unpatched against a remote code execution vulnerability.

The malware, dubbed **FreakOut** by CheckPoint researchers in January (aka Necro and N3Cr0m0rPh), is an obfuscated Python script designed to evade detection using a polymorphic engine and a user-mode rootkit that hides malicious files dropped on compromised systems.

FreakOut spreads itself by exploiting a wide range of OS and apps vulnerabilities and brute-forcing passwords over SSH, adding the infected devices to an IRC botnet controlled by its masters.

The malware's core functionality enables operators to launch DDoS attacks, backdoor infected systems, sniff and exfiltrate network traffic, and deploy XMRig miners to mine for Monero cryptocurrency.

Malware upgraded with new exploits

As Cisco Talos researchers shared in a report published today, FreakOut's developers have been hard at work improving the malware's spreading capabilities since early May, when the botnet's activity has suddenly increased.

"Although the bot was originally discovered earlier this year, the latest activity shows numerous changes to the bot, ranging from different command and control (C2) communications and the addition of new exploits for spreading, most notably vulnerabilities in VMWare vSphere, SCO OpenServer, Vesta Control Panel and SMB-based exploits that were not present in the earlier iterations of the code," Cisco Talos security researcher Vanja Svajcer said.

FreakOut bots scan for new systems to target either by randomly generating network ranges or on its masters' commands sent over IRC via the command-and-control server.

For each IP address in the scan list, the bot will try to use one of the built-in exploits or log in using a hardcoded list of SSH credentials.

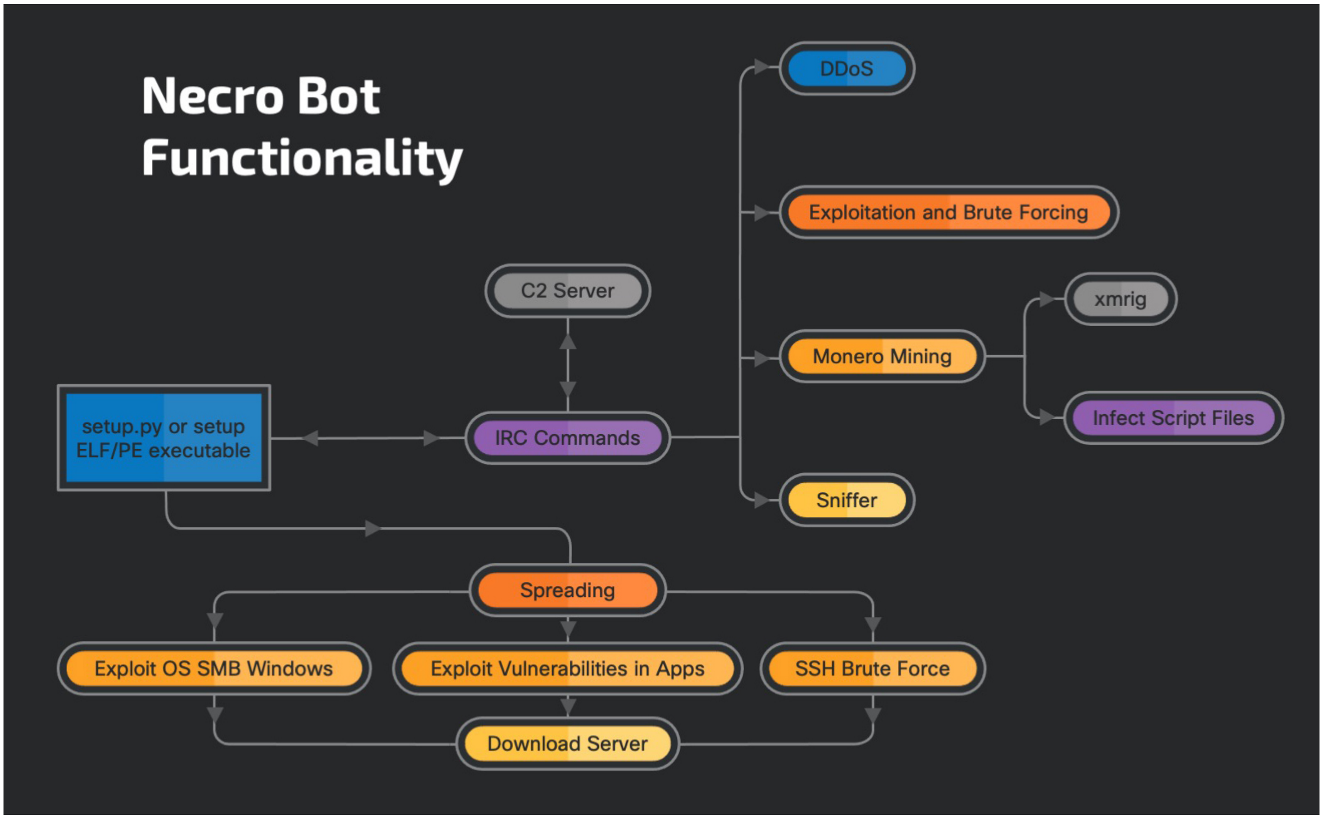


Image: Cisco Talos

While early FreakOut versions were able to exploit only vulnerable versions of Lifearay, Laravel, WebLogic, TerraMaster, and Zend Framework (Laminas Project) web apps, the latest ones have more than double the number of built-in exploits.

Newly added exploits to malware variants observed by Cisco Talos in May include:

- VestaCP — VestaCP 0.9.8 - 'v_sftp_licence' Command Injection
- ZeroShell 3.9.0 — 'cgi-bin/kerbynet' Remote Root Command Injection
- SCO Openserver 5.0.7 — 'outputform' Command Injection
- Genexis PLATINUM 4410 2.1 P4410-V2-1.28 — Remote Command Execution vulnerability
- OTRS 6.0.1 — Remote Command Execution vulnerability
- VMWare vCenter — Remote Command Execution vulnerability
- An Nrdh.php remote code execution exploit for an unknown app
- Python versions of EternalBlue (CVE-2017-0144) and EternalRomance (CVE-2017-0147) exploits

Thousands of VMware servers exposed to attacks

The VMware vCenter vulnerability (CVE-2021-21972) is present in the vCenter plugin for vRealize Operations (vROps) and is particularly interesting because it impacts all default vCenter Server installations.

Thousands of unpatched vCenter servers are currently reachable over the Internet, as shown by Shodan and BinaryEdge.

Attackers have previously mass scanned for vulnerable Internet-exposed vCenter servers after security researchers published a proof-of-concept (PoC) exploit code.

Russian Foreign Intelligence Service (SVR) state hackers have also added CVE-2021-21972 exploits to their arsenal in February, actively exploiting them in ongoing campaigns.

VMware vulnerabilities have also been exploited in the past in ransomware attacks targeting enterprise networks. As Cisco Talos revealed, FreakOut operators have also been seen deploying a custom ransomware strain showing that they are actively experimenting with new malicious payloads.

Multiple ransomware gangs, including RansomExx, Babuk Locker, and Darkside, previously used VMWare ESXi pre-auth RCE exploits to encrypt virtual hard disks used as centralized enterprise storage space.

"Necro Python bot shows an actor that follows the latest development in remote command execution exploits on various web applications and includes the new exploits into the bot. This increases its chances of spreading and infecting systems," Svajcer added.

"Users need to make sure to regularly apply the latest security updates to all of the applications, not just operating systems."

Related Articles:

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots

Microsoft detects massive surge in Linux XorDDoS malware activity

Qbot malware switches to new Windows Installer infection vector

Malicious PyPI package opens backdoors on Windows, Linux, and Macs