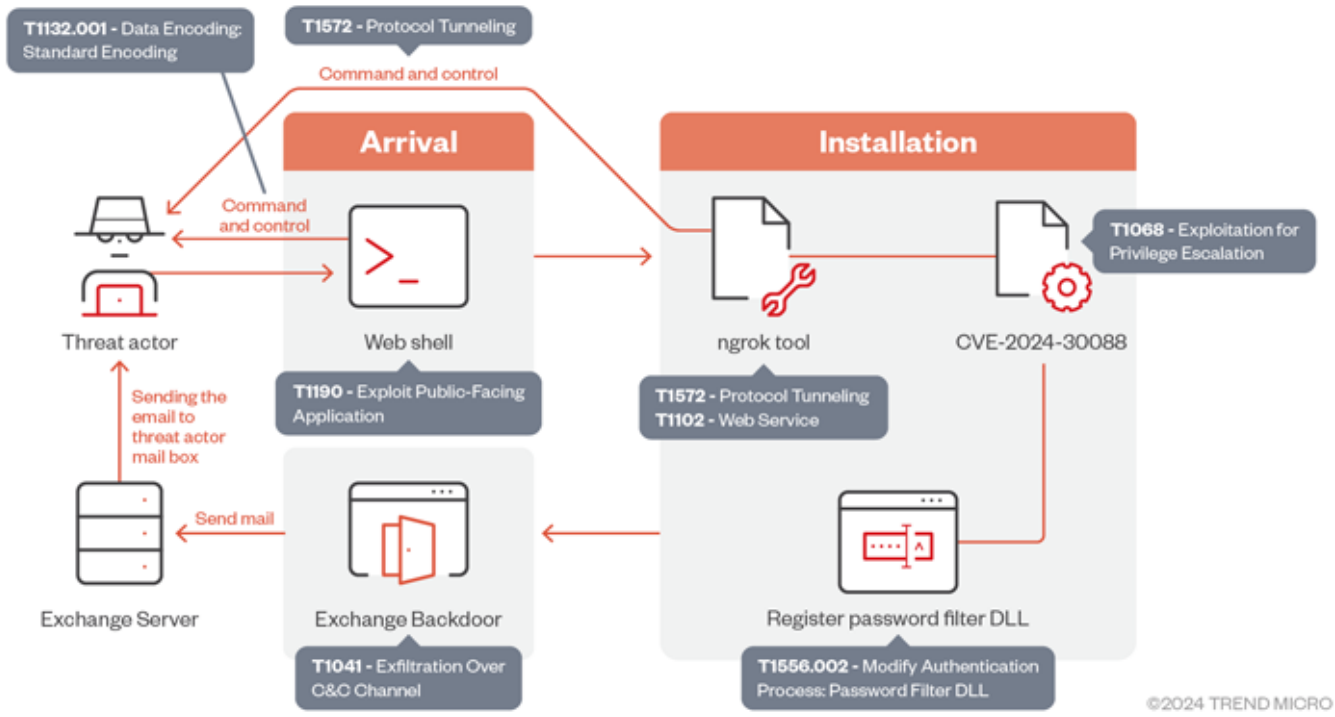
OilRig Exploits Windows Kernel Flaw in Espionage Campaign Targeting UAE and Gulf



The Iranian threat actor known as OilRig has been observed exploiting a now-patched privilege escalation flaw impacting the Windows Kernel as part of a cyber espionage campaign targeting the U.A.E. and the broader Gulf region.

"The group utilizes sophisticated tactics that include deploying a backdoor that leverages Microsoft Exchange servers for credentials theft, and exploiting vulnerabilities like CVE-2024-30088 for privilege escalation," Trend Micro researchers Mohamed Fahmy, Bahaa Yamany, Ahmed Kamal, and Nick Dai said in an analysis published on Friday.

The cybersecurity company is tracking the threat actor under the moniker Earth Simnavaz, which is also referred to as APT34, Crambus, Cobalt Gypsy, GreenBug, Hazel Sandstorm (formerly EUROPIUM), and Helix Kitten.

The attack chains entail the deployment of a previously undocumented implant that comes with capabilities to exfiltrate credentials through on-premises Microsoft Exchange servers, a tried-and-tested tactic adopted by the adversary in the past, while also incorporating recently disclosed vulnerabilities to its exploit arsenal.

CVE-2024-30088, patched by Microsoft in June 2024, concerns a case of privilege escalation in the Windows kernel that could be exploited to gain SYSTEM privileges, assuming the attackers can win a race condition.

Initial access to target networks is facilitated by means of infiltrating a vulnerable web server to drop a web shell, followed by dropping the ngrok remote management tool to maintain persistence and move to other endpoints in the network.

The privilege escalation vulnerability subsequently serves as a conduit to deliver the backdoor, codenamed STEALHOOK, responsible for transmitting harvested data via the Exchange server to an email address controlled by the attacker in the form of attachments.

A notable technique employed by OilRig in the latest set of attacks involves the abuse of the elevated privileges to drop the password filter policy DLL (psgfilter.dll) in order to extract sensitive credentials from domain users via domain controllers or local accounts on local machines.

"The malicious actor took great care in working with the plaintext passwords while implementing the password filter export functions," the researchers said. "The threat actor also utilized plaintext passwords to gain access and deploy tools remotely. The plaintext passwords were first encrypted before being exfiltrated when sent over networks."

It's worth noting that the use of psgfilter.dll was observed back in December 2022 in a connection with an OilRig campaign targeting organizations in the Middle East using another backdoor dubbed MrPerfectionManager.

"Their recent activity suggests that Earth Simnavaz is focused on abusing vulnerabilities in key infrastructure of geopolitically sensitive regions," the researchers noted. "They also seek to establish a persistent foothold in compromised entities, so these can be weaponized to launch attacks on additional targets."