


Austria subjected to pro-Russian DDoS intrusions

 scworld.com/brief/austria-subjected-to-pro-russian-ddos-intrusions

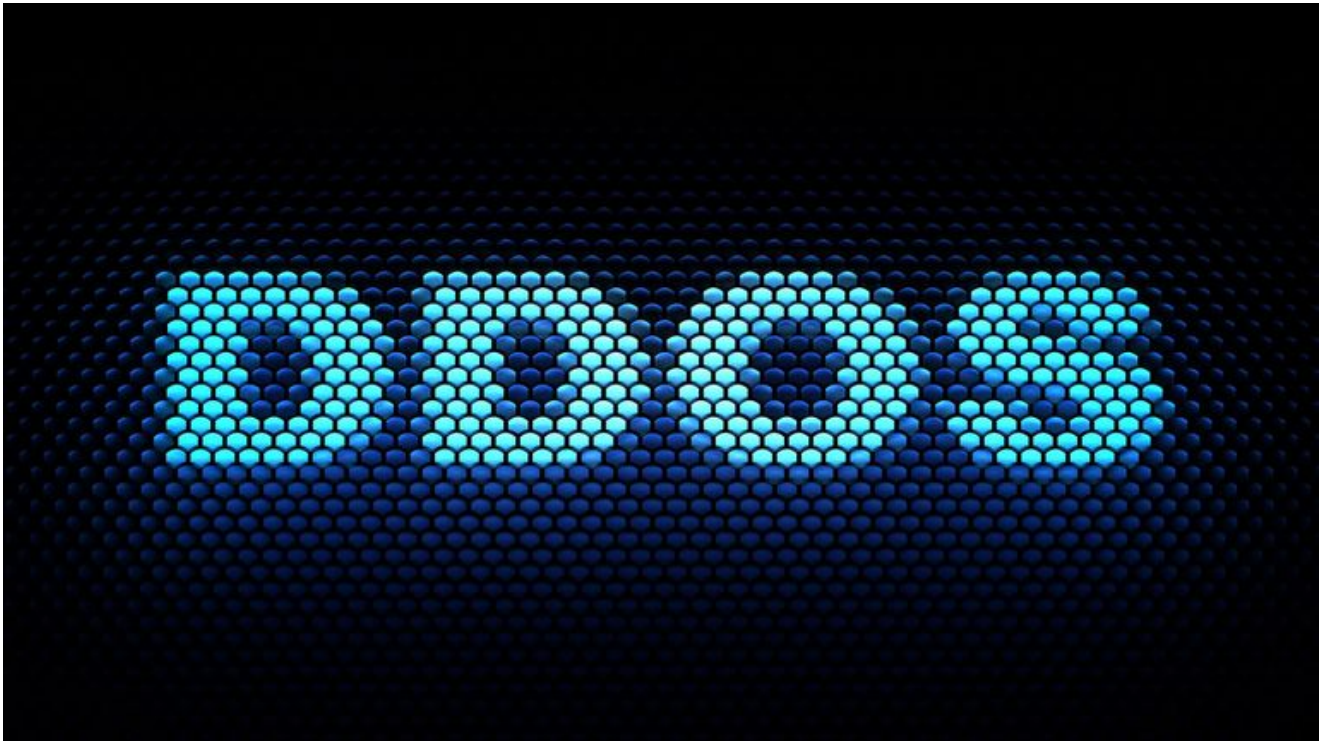
September 25, 2024

Threat Intelligence

September 25, 2024

 Share

By SC Staff



(Adobe Stock)

More than 40 Austrian organizations had their websites subjected to distributed denial-of-service attacks by pro-Russia hacktivist operations [NoName057\(16\)](#) and OverFlame that have been underway since last week ahead of the country's election on Sunday, according to [The Record](#), a news site by cybersecurity firm Recorded Future.

Aside from disrupting the websites of the country's financial service entities, airports, and stock exchange, both NoName057(16) and OverFlame hackers have also deployed DDoS intrusions against the websites of Austria's OVP and SPO political parties. However, Radware noted that long-term impact has not been observed from the hacktivist operations' attacks. Attacks by NoName057(16) have been primarily facilitated by the DDoSia botnet project, which is dependent on the usage of other hacktivist groups, according to Radware, which also noted the Cyber Army of Russia Reborn's participation in the latest intrusions. "It is common to see like-minded threat actors form ad-hoc alliances and collaborate on campaigns to increase their impact," added Radware.



SC Staff

Related



RANSOMWARE

Joint RustyStealer, Ymir ransomware attacks emerge

SC Staff November 12, 2024

Numerous systems have been initially targeted with the RustyStealer credential-harvesting tool to facilitate high-privilege account compromise and lateral movement prior to the execution of SystemBC malware-related scripts and exfiltration of data over two days, an analysis from Kaspersky researchers showed.



GOVERNMENT REGULATIONS

Legal protections for security researchers sought in new German draft law

Laura French November 7, 2024

A proposed amendment would exclude legitimate security research from the definition of data espionage.



MALWARE

Attacks with novel SteelFox trojan hit Windows machines

SC Staff November 7, 2024

Malicious posts detailing instructions for downloading cracked software on torrent trackers and forums enable deployment of SteelFox and acquisition of administrator access, which is then leveraged to establish a WinRing0.sys driver susceptible to privilege escalation via the CVE-2020-14979 and CVE-2021-41285 flaws, according to an analysis from Kaspersky.