Scottish Cyber Coordination Centre

Daily threat bulletin

19 June 2024

Vulnerabilities

Report Reveals Record Exploitation Rate For Load Balancers

Infosecurity Magazine - 18 June 2024 11:00

Action1 reveals cybercriminals are increasingly targeting NGINX and Citrix load balancers

Threat actors and malware

New Malware Targets Exposed Docker APIs for Cryptocurrency Mining

The Hacker News - 18 June 2024 16:11

Cybersecurity researchers have uncovered a new malware campaign that targets publicly exposed Docket API endpoints with the aim of delivering cryptocurrency miners and other payloads.Included among the tools deployed is a remote access tool that's capable of downloading and executing more malicious programs as well as a utility to propagate the malware via SSH, cloud analytics platform Datadog

Cut & Paste Tactics Import Malware to Unwitting Victims

darkreading - 18 June 2024 19:35

"ClearFake" and "ClickFix" attackers are tricking people into cutting and pasting malicious PowerShell scripts to infect their own machines with RATs and infostealers.

Scattered Spider Pivots to SaaS Application Attacks

darkreading - 18 June 2024 13:56

Microsoft last year described the threat actor — known as UNC3944, Scattered Spider, Scatter Swine, Octo Tempest, and 0ktapus — as one of the most dangerous current adversaries.

New BadSpace Backdoor Deployed in Drive-By Attacks

SecurityWeek - 18 June 2024 14:11

The BadSpace backdoor is being distributed via drive-by attacks involving infected websites and JavaScript downloaders.The post New BadSpace Backdoor Deployed in Drive-By Attacks appeared first on SecurityWeek.

New TikTag Attack Targets Arm CPU Security Feature

SecurityWeek - 18 June 2024 13:16

Researchers have targeted the MTE security feature in Arm CPUs and showed how attackers could bypass protections.The post New TikTag Attack Targets Arm CPU Security Feature appeared first on SecurityWeek.

UK incidents

NHS boss says Scottish trust wouldn't give cyberattackers what they wanted

The Register - 18 June 2024 12:29

CEO of Dumfries and Galloway admits circa 150K people should assume their details leaked The chief exec at NHS Dumfries and Galloway will write to thousands of folks in the Scottish region whose data was stolen by criminals, admitting the lot of it was published after the trust did not give in to the miscreants' demands....