Scottish Cyber Coordination Centre

# Daily threat bulletin

29 October 2024

## Vulnerabilities

### New Research Reveals Spectre Vulnerability Persists in Latest AMD and Intel Processors

The Hacker News - 29 October 2024 12:23

More than six years after the Spectre security flaw impacting modern CPU processors came to light, new research has found that the latest AMD and Intel processors are still susceptible to speculative execution attacks.

### More Details Shared on Windows Downgrade Attacks After Microsoft Rolls Out Mitigations

SecurityWeek - 28 October 2024 13:48

Microsoft has rolled out mitigations for recently disclosed downgrade attacks targeting the Windows Update process.

## Threat actors and malware

### BeaverTail Malware Resurfaces in Malicious npm Packages Targeting Developers

The Hacker News - 28 October 2024 20:21

Three malicious packages published to the npm registry in September 2024 have been found to contain a known malware called BeaverTail, a JavaScript downloader and information stealer linked to an ongoing North Korean campaign tracked as Contagious Interview.

### Redline, Meta infostealer malware operations seized by police

BleepingComputer - 28 October 2024 10:30

The Dutch National Police seized the network infrastructure for the Redline and Meta infostealer malware operations in “Operation Magnus,” warning cybercriminals that their data is now in the hands of law enforcement.

### Black Basta affiliates used Microsoft Teams in recent attacks

Security Affairs - 28 October 2024 09:07

ReliaQuest researchers observed Black Basta affiliates relying on Microsoft Teams to gain initial access to target networks. ReliaQuest researchers warn that Black Basta ransomware affiliates switched to Microsoft Teams, posing as IT support to deceive employees into granting access.

## Chinese Hackers Use CloudScout Toolset to Steal Session Cookies from Cloud Services

The Hacker News - 28 October 2024 23:56

A government entity and a religious organization in Taiwan were the target of a China-linked threat actor known as Evasive Panda that infected them with a previously undocumented post-compromise toolset codenamed CloudScout.”The CloudScout toolset is capable of retrieving data from various cloud services by leveraging stolen web session cookies,” ESET security researcher Anh Ho said.