



Scottish  
Cyber  
Coordination  
Centre

# Daily Threat Bulletin

9 June 2025

## Vulnerabilities

### [Cisco Patches Critical ISE Vulnerability With Public PoC](#)

SecurityWeek - 06 June 2025 10:47

Cisco has released patches for a critical vulnerability impacting cloud deployments of Identity Services Engine (ISE).

### [Critical Fortinet flaws now exploited in Qilin ransomware attacks](#)

BleepingComputer - 06 June 2025 10:53

The Qilin ransomware operation has recently joined attacks exploiting two Fortinet vulnerabilities that allow bypassing authentication on vulnerable devices and executing malicious code remotely.

### [HPE Patches Critical Vulnerability in StoreOnce](#)

SecurityWeek - 06 June 2025 09:52

An HPE StoreOnce vulnerability allows attackers to bypass authentication, potentially leading to remote code execution.

## Threat actors and malware

### [New Atomic macOS Stealer Campaign Exploits ClickFix to Target Apple Users](#)

The Hacker News - 06 June 2025 22:55

Cybersecurity researchers are alerting to a new malware campaign that employs the ClickFix social engineering tactic to trick users into downloading an information stealer malware known as Atomic macOS Stealer (AMOS) on Apple macOS systems.

### [New Supply Chain Malware Operation Hits npm and PyPI Ecosystems, Targeting Millions Globally](#)

The Hacker News - 08 June 2025 20:17

Cybersecurity researchers have flagged a supply chain attack targeting over a dozen packages associated with GlueStack to deliver malware. The malware, introduced via a change to "lib/commonjs/index.js," allows an attacker to run shell commands, take screenshots, and upload files to infected machines.



Scottish  
Cyber  
Coordination  
Centre

### **Cutting-Edge ClickFix Tactics Snowball, Pushing Phishing Forward**

darkreading - 06 June 2025 21:07

Several widespread ClickFix campaigns are underway, bent on delivering malware to business targets, and they represent a new level of phishing sophistication that defenders need to be prepared for.

### **New PathWiper Data Wiper Malware Disrupts Ukrainian Critical Infrastructure in 2025 Attack**

The Hacker News - 06 June 2025 15:05

A critical infrastructure entity within Ukraine was targeted by a previously unseen data wiper malware named PathWiper, according to new findings from Cisco Talos.

### **BADBOX 2.0 Targets Home Networks in Botnet Campaign, FBI Warns**

darkreading - 06 June 2025 18:18

Though the operation was partially disrupted earlier this year, the botnet remains active and continues to target connected Android devices.

### **Scattered Spider Uses Tech Vendor Impersonation and Phishing Kits to Target Helpdesks**

Infosecurity Magazine - 06 June 2025 15:00

Scattered Spider, the ransomware collective believed to be behind recent retail hacks in the UK, including those targeting Marks & Spencer (M&S) and Harrods, has evolved its arsenal to incorporate more sophisticated tactics like Evilginx to breach its targets.