BLUF

The current threat landscape is characterized by a high volume of critical threats, with 39 out of 42 analyzed incidents classified as critical. The most targeted sectors are Government, Technology, and Finance, with the United States, Ukraine, and Taiwan being the most affected countries. Attackers are primarily using techniques such as modifying registry settings and exploiting registry run keys to gain persistence and evade detection.

Threat landscape

The threat landscape is dominated by advanced threat actors, including The Gentlemen, DragonForce, and Gamaredon, who are targeting various sectors and regions. The top malware families used by these actors include Cobalt Strike, Vidar, and Sliver. The most exploited vulnerabilities are CVE-2025-8088, CVE-2025-5777, and CVE-2024-55591.

Where to focus

To mitigate these threats, organizations should prioritize hardening their systems against hidden persistence techniques, particularly those that involve modifying registry settings and exploiting registry run keys. This can be achieved by implementing robust security controls, such as regularly monitoring and restricting changes to registry settings, and ensuring that all software is up-to-date and patched. Additionally, organizations should focus on preventing phishing attacks and account manipulation, as these are common tactics used by attackers to gain initial access to systems.

Notable campaigns

- Critical: Interlock and Rhysida within the Ransomware Ecosystem (linked to Hive0163)
- Critical: Hacktivists are broadening their scope beyond political motivation (linked to 4BID)
- Critical: Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software Keeps the Door Open (linked to Earth Dahu)
- Critical: From emerging threat to top-tier ransomware-as-a-service: The evolution of INC ransomware (linked to INC)

Outlook

The threat landscape is expected to continue evolving, with attackers adapting and refining their techniques to evade detection and exploit new vulnerabilities. As such, organizations must remain vigilant

and proactive in their security efforts, staying informed about emerging threats and adjusting their defenses accordingly.

Notable campaigns: (the list of notable campaigns is appended below, as provided in the factsheet) ...

Appendix // The week by the numbers

Derived from 42 unique campaigns collected this period. Every figure below is a direct count, not an estimate.

Severity

Band	Campaigns
Critical	39
High	3

Sectors targeted

Sector	Campaigns
Government	16
Technology	10
Finance	10
Education	8
Healthcare	7
Defense	7

Geographies

Country	Campaigns
United States of America	8
Ukraine	5
Taiwan	4
Brazil	4
Russian Federation	4

Country	Campaigns
India	4

Most active actors

Actor	Campaigns
The Gentlemen	4
DragonForce	2
Gamaredon	2
Qilin	1
INC	1
Hive0163	1

Malware families

Family	Campaigns
Cobalt Strike	7
Vidar	5
Sliver	4
ValleyRAT	4
SystemBC	3
Havoc	3
XMRig	3
Mimikatz	3

CVEs in play

CVE	Campaigns
CVE-2025-8088	4
CVE-2025-5777	2
CVE-2024-55591	2

CVE	Campaigns
CVE-2026-50751	1
CVE-2026-50752	1
CVE-2023-52271	1

Defensive priority // recurring chokepoints

The techniques that were the decisive control point in the most campaigns. Hardening these is the highest-leverage move for the period.

Technique	Control point	Campaigns
T1112	Modify Registry	10
T1547.001	Registry Run Keys / Startup Folder	9
T1078	Valid Accounts	4
T1566	Phishing	4
T1098	Account Manipulation	3
T1505.003	Web Shell	3

Notable campaigns (expanded roster)

Severity	Campaign	Attributed to
Critical	Interlock and Rhysida within the Ransomware Ecosystem	Hive0163
Critical	Hacktivists are broadening their scope beyond political motivati	4BID
Critical	Old WinRAR Flaw Fuels Attacks on Ukraine: How Unmanaged Software	Earth Dahu
Critical	From emerging threat to top-tier ransomware-as-a-service: The ev	INC
Critical	Attackers Weaponize Microsoft Teams Relays to Stay Hidden	DragonForce
Critical	Ongoing exploitation of Cisco Catalyst SD-WAN vulnerabilities	UAT-8616
Critical	LBIOC-20260071 - The Gentlemens Leak	The Gentlemen
Critical	Vidar Stealer Unmasked: Code Signing Abuse, Go Loaders and File	X3D MINER
Critical	Targets Education Sector with Oracle PeopleSoft Exploit	UNC6240

Severity	Campaign	Attributed to
Critical	The Gentlemen are knocking: custom backdoors and evolving tactic	The Gentlemen