MAG212 CYBER

DAILY DAILY CYBER INTELLIGENCE

Friday 13 November 2026

Research cutoff: 07:00 PT (15:00 UTC) · Stories from the 24 h before cutoff, extended to 72 h where labelled

From the edge to the hypervisor

A Check Point gateway flaw led to root, hidden implants and a wiper on VMware ESXi. An MSP platform was exploited on its newest build within five hours. And Microsoft 365 entered a second day of disruption.

- **Check Point**: PHP2Shell to root to ESXi wiper · patch and hunt
- **N-central** "4EverAble2Shell": 21 servers mining, no fix yet
- **NetScaler**: 28 CVEs, one hits every appliance · Console 9.4
- **Microsoft 365** outage, day two · no root cause
- **Operation Endgame** hits Gootloader, CastleRAT, StealC
- **SignDrop** Windows LPE PoC · **Daybreak** AI pentest agents



By **El Mostafa Ouchen** · cyber.mag212.com

Free subscription: cyber.mag212.com/subscribe-free

Cover art: conceptual illustration, MAG212 CYBER original. Not a real system.

Executive briefing

MAG212 ANALYSIS Today's theme is **what sits behind the edge**. Check Point showed how one unpatched VPN portal became root on a firewall, a hidden implant, and finally a wiper on the hypervisor behind it. N-central, the platform many MSPs use to run their customers, was exploited on its newest build within hours of a public exploit. Citrix shipped 28 NetScaler fixes, and Microsoft 365 is still not fully back. The common lesson: **management planes are the target**, so isolate them, log them off-box and patch them first.

The three actions that matter most today

1

Check Point: apply the November Jumbo Hotfix and hunt

Prioritise internet-facing Mobile Access gateways. Look for `upload_progress_pwn` session files, `zz*.tpl` templates and a `CPconfigdaemon` process, and check ESXi for SSH logins from gateways. If you find one, treat it as a rebuild. ↗ Check Point ↗ CPR

2

N-central: keep Legacy API off and check for miners

There's no fix yet for 4EverAble2Shell, and Hotfix 2 doesn't stop it. Keep on-prem servers offline until N-able says otherwise; if one is online, confirm Legacy API is disabled, look for `xvd.service` and `/tmp/.xvd` , and treat a hit as full server compromise. ↗ BleepingComputer

3

NetScaler: upgrade every ADC and Gateway, then Console

14.1-73.57 or 13.1-64.39 (FIPS: 14.1-73.58 / 13.1-37.293), with internet-facing Gateway and AAA first. Console needs 14.1-74.34 and should be reachable only from management networks. ↗ Citrix ↗ Console

Story board

#	Story	Date label	Exploited?	Who should care
1	Check Point gateways to ESXi wiper	12 Nov	YES	Firewall, VPN and virtualisation teams
2	N-central 4EverAble2Shell zero-day	12–13 Nov	YES	MSPs and their customers
3	NetScaler ADC, Gateway and Console	12–13 Nov	NOT REPORTED	Remote access and app delivery owners
4	Microsoft 365 outage, day two	12–13 Nov	NO ATTACK SEEN	Every Microsoft 365 tenant
5	Operation Endgame	12 Nov	VICTIMS	Identity teams, WordPress owners
6	SignDrop Windows privilege escalation	13 Nov	POC ONLY	Windows and endpoint teams
7	AI pentest agents on both sides	12–13 Nov	N/A	AppSec leaders, CISOs

Labels: CONFIRMED primary source · REPORTED secondary outlet · CLAIMED attacker or unverified · MAG212 ANALYSIS our judgement · UNKNOWN not established.

In this issue

01 **From a VPN portal to an ESXi wiper** 4
Check Point PHP2Shell, CVE-2026-123039, TSGA implant

02 **N-central's newest build exploited within hours** 6
4EverAble2Shell · 21 servers mining · no fix

03 **28 NetScaler flaws, one in every appliance** 7
ADC/Gateway 14.1-73.57 · Console 14.1-74.34

04 **Microsoft 365 outage enters day two** 9
EX1550543 · network rollback · no root cause

05 **Operation Endgame hits three malware networks** 10
Gootloader · CastleRAT · StealC · 6M+ credentials

06 **SignDrop: a Windows path to SYSTEM via Defender** 11
Public PoC · no CVE or fix yet

07 **AI pentest agents, owned by defenders and attackers** 12
OpenAI Daybreak vs AntiFox

◆ **Defender's Action Desk** 13
Checklist · KEV deadlines · pending items

◆ **Awareness lesson and briefly noted** 14
"Need a contract template? Go to the source"

◆ **Source register** 15
38 sources, with whether we opened them

↻ Updates to earlier coverage

- **Barracuda: KEV deadline is today.** CONFIRMED CVE-2026-116606 and CVE-2026-111560 are due 13 November. CISA's catalog is still at version 2026.11.10, with no additions on 11–13 November. ↗ CISA KEV
- **Gaps in KEV.** CONFIRMED The PHP2Shell CVEs have been listed since 26 October. Check Point's exploited CVE-2026-123039 and the Apache Axis CVE-2026-90436 used against N-central are not listed yet, so don't wait for KEV to act on them. ↗ CISA KEV
- **ScreenConnect / SCKit** (covered 12 Nov): UNKNOWN We found no new verified details since yesterday. ConnectWise's advisory index still had no November entry. Yesterday's sweep and response steps stand. ↗ MAG212, 12 Nov
- **eMudhra:** Microsoft starts removing eMudhra roots **Monday 16 November**. Replace emSign/eMudhra certificates now.

ACTIVELY EXPLOITED · CHECK POINT SECURITY GATEWAYS

01

From a VPN portal to an ESXi wiper: inside the Check Point gateway intrusions

Exploited | Destructive in some cases | Patch + hunt | 12 Nov | Evidence: strong (vendor)

ENTRY	TO ROOT	SCALE	FIX
PHP2Shell (CVE-2026-109618/-109619, 9.2), Mobile Access portal	CVE-2026-123039 (7.8), Gaia DynamicCLI	"A couple of dozen" unpatched systems, one region	November Jumbo Hotfix on gateways and management

What happened

CONFIRMED Check Point says attackers exploited **PHP2Shell**, a PHP flaw that also affects its Security Gateways, through the **Mobile Access portal**. They then used a Gaia privilege-escalation flaw, **CVE-2026-123039**, to get root and persistence. Activity ran from **30 October to 4 November**, a week after fixes shipped on 23 October. Only "a couple of dozen unpatched systems, in a single region" were compromised. In many cases the attacker got a foothold in the network; in a limited number the activity was destructive and ideologically motivated. Check Point notified affected customers and helped remediate.
↗ Check Point advisory

CONFIRMED Check Point Research describes two waves. The first, on 30 October, targeted Israeli organisations and included destructive activity against some. The second, on 2 November, hit organisations in several countries and sectors with no sign of destruction. ↗ Check Point Research

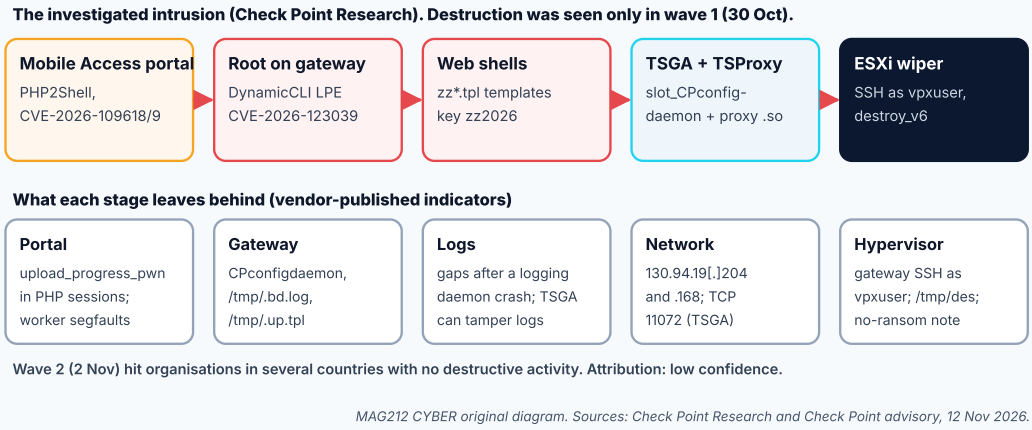


Figure 1 · From VPN portal to ESXi wiper. The five stages Check Point Research describes, with the artifacts each one leaves. How the ESXi credential was obtained is unknown.
MAG212 CYBER original diagram, based on Check Point's advisory and Check Point Research (12 Nov 2026).

Who is affected

CVE	What	Affected	Exploited
CVE-2026-109618 / -109619	PHP2Shell: unauthenticated RCE via firewall web interfaces (9.2)	Security Gateways with Mobile Access Portal, R80 to R82.20; Spark R81.10.x, R82.00.x, R77.20.x, R80.20.x	YES
CVE-2026-123039	Local privilege escalation in the Gaia DynamicCLI service (7.8)	Gaia R81.20, R82, R82.10, R82.20	YES
CVE-2026-107484	Gaia Portal privilege escalation by an authenticated user (7.3)	Gaia WebUI R80 to R82.20	No
CVE-2026-120490	Management-to-gateway access via NAT rule (3.8)	R81.20, R82	No

Source: Check Point advisory (SK references sk1000302, sk1000362, sk1000291, sk1000364). The November Jumbo Hotfix also includes the Node2Shell/Brotli fix CVE-2026-111497.

How the attack works

CONFIRMED In the intrusion Check Point investigated, the attacker:

1. Exploited the portal, leaving PHP session files with `upload_progress_pwn` under `/opt/CPcvpn-R81.20/tmp/` and causing hundreds of Apache/PHP worker crashes.
2. Escalated from the portal's service account to root through DynamicCLI.
3. Wrote PHP web shells as `zz*.tpl` login-page templates, using the key `zz2026`, with uploads saved to `/tmp/.up.tpl`.
4. Launched the **TSGA** implant from `/tmp/CPconfigdaemon`, which relaunches as `slot_CPconfigdaemon`. TSGA drops **TSProxy** to `/lib/libcpfwcommon.so` and injects it into appliance processes to hide attacker connections. It can also steal configuration, persist in backups and snapshots, and tamper with firewall logs.
5. Scanned the internal network with the *gogo* scanner, then used SSH as `vpxuser` to reach a **VMware ESXi** host and run the `destroy_v6` wiper, which left `DREAM_ANNEXATION.txt` notes rejecting ransom.

↗ Check Point Research UNKNOWN How the attacker obtained a working ESXi credential. REPORTED TSGA and TSProxy are modified variants of **PhiliKit**, a backdoor seen in Ivanti VPN attacks that ESET associated with China-nexus UNC5221. Check Point says the evidence doesn't support a confident attribution: the actor may have run the whole campaign, acted as an access broker, or staged a false flag.

Gateway and ESXi hunt OS: Gaia (expert mode) · ESXi shell Shell: bash / sh Privileges: expert (root) · ESXi admin READ-ONLY

```
# Gaia: installed Jumbo Hotfix take
cpinfo -y all 2>/dev/null | grep -i -A2 'HOTFIX'
# Portal exploitation marker and template web shells
grep -l 'upload_progress_pwn' /opt/CPcvpn-*/tmp/sess_* 2>/dev/null
find / -xdev \( -name 'zz*.tpl' -o -name 'challenge_render.tpl' -o -name '*CPconfigdaemon' \
  -o -name 'libcpfwcommon.so' \) 2>/dev/null
ls -la /tmp/.bd.log /tmp/.up.tpl /tmp/.p_sock 2>/dev/null
netstat -tlnp 2>/dev/null | grep ':11072'
# ESXi: SSH logins as vpxuser (run on each host)
grep -i 'vpxuser' /var/log/auth.log | grep -i 'sshd'
```

Expected clean result: a current November take, and no output from the other commands. Any hit means a full compromise: isolate the device and call incident response before changing it. **Commands not tested by MAG212 CYBER.** Indicators from Check Point Research; check exact paths against your Gaia version.

Investigate, contain and remediate (in order)

1. **Preserve evidence off the box first:** remote syslog, SmartConsole logs, upstream NetFlow and vCenter/ESXi auth logs. TSGA can tamper with local firewall logs, so gaps after a logging-daemon crash are themselves a signal.
2. **Block** `130.94.19[.]204` and `.168`, and restrict traffic from gateways to hypervisor management networks.
3. **Install the November Jumbo Hotfix** on all management servers and gateways, internet-facing Mobile Access first (for example R81.20 Take 174, R82.10 Take 52). ↗ R81.20 ↗ R82.10
4. MAG212 ANALYSIS **If any indicator matches, rebuild rather than clean.** TSGA persists in backups and snapshots, so check backups before restoring. Then rotate VPN, admin and `vpxuser`/vCenter credentials.

Verify recovery: the take is confirmed on both cluster members; there's no listener on 11072; ESXi shows no SSH from gateways; and policy install, VPN login and failover work. **Prevention** MAG212 ANALYSIS : a firewall should never be able to SSH to your hypervisors. Put ESXi management behind its own boundary, disable ESXi SSH when it's not in use, and keep firewall logs somewhere the firewall can't edit.

ZERO-DAY · N-ABLE N-CENTRAL

02

N-central's newest build exploited within hours of a public exploit

Exploited | No patch | Legacy API off | 12–13 Nov | Evidence: medium (press, multiple firms)

EXPLOIT	ALSO RELEASED	SEEN	VENDOR
4EverAble2Shell: unauthenticated root, needs Legacy API	Agent2Shell: claimed SYSTEM on managed Windows	21 servers mining Monero, 19 on 2026.4 HF2	Features restricted, Intune integration off; no fix yet

What happened

REPORTED Researcher Sean Bales published **more than 30 N-central zero-days** with exploits on 8 November. N-able took hosted N-central offline on 9 November and shipped **2026.4 Hotfix 2** (build 2026.4.1.26) on 10 November, fixing seven CVEs. On 12 November Bales released two more exploits, **4EverAble2Shell** and **Agent2Shell**, tested against that same Hotfix 2 build. ↗ SecurityWeek ↗ BleepingComputer

REPORTED Previdian saw probing at about 08:30 UTC on 12 November. Huntback saw the full chain from 09:16 UTC, and by 12:50 UTC counted **21 compromised N-central servers** running an XMRig miner. Huntback describes all 21 as hosted N-central servers; nineteen were on Hotfix 2, spread across the US, Canada, South Africa, the UK, Germany, France and Sweden. SecurityWeek, citing Lupovis and Huntback, puts the first successful compromises about five hours after the exploit was published. ↗ BleepingComputer ↗ SecurityWeek

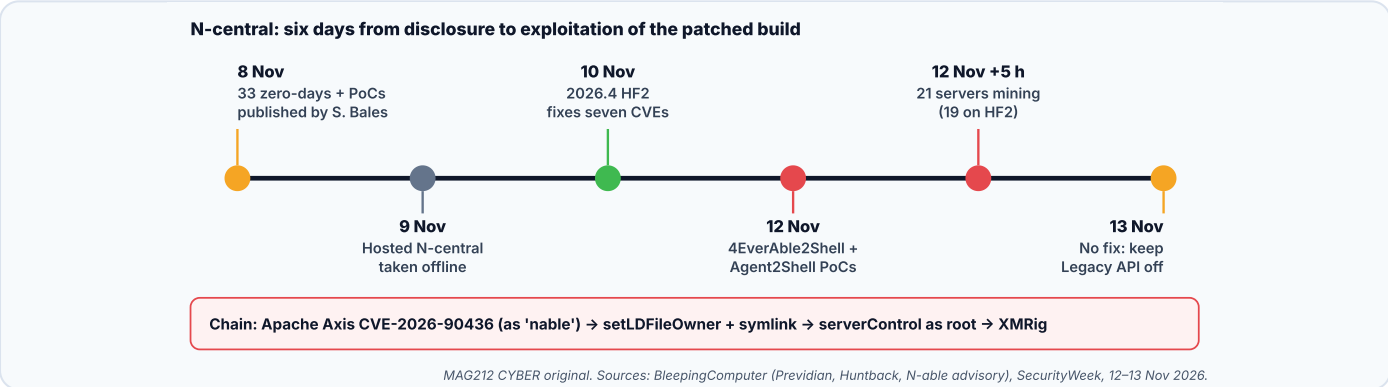


Figure 2 · N-central: 8 to 13 November. From the first zero-day dump to miners on the newest build. Times are UTC on 12 November. *MAG212 CYBER original chart, based on BleepingComputer and SecurityWeek (8–13 Nov 2026).*

Who is affected and how it works

REPORTED **N-central servers with the Legacy API enabled**; Legacy API is off by default. UNKNOWN How the compromised servers came to have it enabled. The chain uses an Apache Axis flaw, **CVE-2026-90436**, to run commands as the `nable` service account. It then abuses the privileged `setLDFileOwner` helper and a symbolic link to make a root-owned script writable, edits that script, and runs it as root through `serverControl`. The payload fetched a script from `157.20.241[.]16` and installed a miner set to use about half the CPU cores. ↗ BleepingComputer MAG212 ANALYSIS Cryptomining is the least of it: root on an RMM server means control of every endpoint it manages. Agent2Shell, if it works as claimed, targets those endpoints directly.

REPORTED N-able's 12 November advisory says it is "restricting certain N-central features and integrations". It has disabled the Intune integration, applied protections to hosted environments, and urges on-premises customers to confirm Legacy API access is disabled and to keep upgrading agents and probes. At that point it said it had seen no compromise using the new flaws; researchers have since reported compromises. ↗ BleepingComputer ↗ N-able status

N-central server check OS: N-central appliance (Linux) Shell: bash Privileges: root / support shell READ-ONLY

```
# Huntback indicators: miner service, staging folders, mining process
systemctl list-units --all --no-pager | grep -i 'xvd'
ls -la /tmp/.xvd /var/tmp/.xvd 2>/dev/null
ps aux | grep -Ei 'xmrig|xvd' | grep -v grep
# Exploit requests in your web access log (path varies by build)
grep -E '/dms/services/ServerUI' <N-CENTRAL-WEB-ACCESS-LOG> | grep -i 'TerminalLineSettings'
# Connections to the reported payload host
ss -tnp | grep '157.20.241.16'
```

Replace `<N-CENTRAL-WEB-ACCESS-LOG>` with your appliance's web log path. Expected clean result: no output from any command. Any hit means full root compromise: take the server off the network and rebuild. **Commands not tested by MAG212 CYBER.** Indicators from Huntback and Previdian via BleepingComputer.

Contain and remediate (in order)

1. **Follow N-able's offline guidance.** REPORTED After the 8 November dump, N-able advised on-premises customers to keep servers offline until it confirms they can safely return, and Huntress repeats that advice. ↗ Huntress If yours is back online, confirm Legacy API is disabled and that the server isn't reachable from the internet.
2. **Run the checks above.** On a hit, isolate the server, preserve disk and logs, rebuild from a known-good install, and rotate every credential and integration secret the server held.
3. MAG212 ANALYSIS **Check managed endpoints** for unexpected scripts or agent tasks pushed since 8 November, and for new remote-access tools.
4. **Watch N-able's status page** for the fix, then apply it immediately, along with the Hotfix 2 agent and probe upgrades.

Verify recovery: Legacy API is off, there's no `xvd` service or miner, CPU use is normal, and the server runs the fixed build once N-able releases it. **Prevention** MAG212 ANALYSIS : this is the second RMM platform in two days. Treat RMM servers as tier zero: no internet exposure without a VPN or allow-list, MFA everywhere, and logs shipped somewhere the server can't reach.

PATCH · CITRIX NETSCALER ADC, GATEWAY AND CONSOLE

03 28 NetScaler flaws, one in every appliance, plus a separate Console bypass

10 critical | No exploitation reported | 12–13 Nov | Evidence: strong (vendor)

EVERY APPLIANCE	HIGHEST SCORE	FIX ADC/GATEWAY	CONSOLE
CVE-2026-120868, packet processing, 9.3	CVE-2026-107412, Gateway/AAA, 9.5	14.1-73.57 · 13.1-64.39 · FIPS 14.1-73.58 / 13.1-37.293	CVE-2026-120869, 9.4 · fix 14.1-74.34

What happened

CONFIRMED Citrix bulletin CTX697305 lists **28 CVEs** in NetScaler ADC and Gateway, almost all memory-safety bugs that Citrix says "can lead to unpredictable or erroneous behavior or Denial of Service". The one that matters to everyone is **CVE-2026-120868** (CVSS 4.0: 9.3), in core packet processing: **all** deployments are affected, "including those deployed with the default configuration". The highest score, 9.5, goes to **CVE-2026-107412**, a set of memory overflows on appliances configured as a **Gateway** (SSL VPN, ICA Proxy, CVPN, RDP Proxy) or **AAA virtual server**. Separately, CTX697320 fixes **CVE-2026-120869** (9.4), an unauthenticated bypass in **NetScaler Console**. ↗ CTX697305 ↗ CTX697320

CONFIRMED Neither bulletin reports exploitation. Credits include JPMorgan Chase's XOR team, CapitalOne and watchTowr, and Citrix says it found several issues itself with AI-assisted code analysis. Secure Private Access hybrid deployments that use NetScaler instances also need the upgrade; Citrix-managed cloud services are patched by Citrix. ↗ Citrix

MAG212 ANALYSIS NetScaler bugs have been weaponised quickly in past years, and watchTowr often publishes technical detail after a patch, so don't treat "not exploited" as "not urgent".

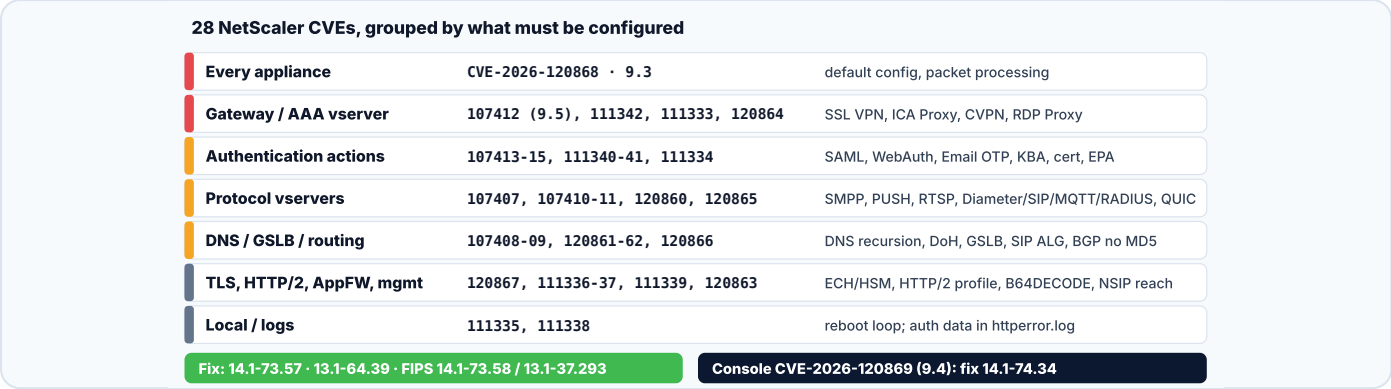


Figure 3 · Which NetScaler CVEs apply to you. One flaw hits every appliance; the rest depend on features. Every node below the fixed build needs the upgrade.
MAG212 CYBER original chart. Data: Citrix CTX697305 and CTX697320 (12–13 Nov 2026).

Who is affected

CONFIRMED NetScaler ADC and Gateway 14.1 before 14.1-73.57, 13.1 before 13.1-64.39, 14.1-FIPS before 14.1-73.58 and 13.1-FIPS/NDcPP before 13.1-37.293. Console 14.1 before 14.1-74.34. The Console flaw needs network access to the Console IP (attack vector "adjacent"). Other notable preconditions include a management-plane flaw exploitable by any untrusted host that can reach the NSIP (CVE-2026-120863), and authentication material written to `/var/log/httperror.log` after logouts (CVE-2026-111338). ↗ Citrix

Build and exposure check OS: NetScaler 13.1 / 14.1 Shell: NetScaler CLI, then shell Privileges: nsroot or read-only admin

READ-ONLY

```
# CLI: running build (run on every node, both HA peers)
show ns version
# shell: features that widen exposure (patterns from CTX697305)
shell
grep -E '^add (vpn|authentication) vserver' /nsconfig/ns.conf
grep -E 'http2 ENABLED|B64DECODE' /nsconfig/ns.conf
exit
```

Compare the build with the fixed versions above; every node below them needs the upgrade regardless of the grep results, because CVE-2026-120868 hits default configurations. The grep results show which extra CVEs apply. **Commands not tested by MAG212 CYBER**; patterns follow CTX697305 and NetScaler docs.

Contain, remediate and verify

1. **Upgrade internet-facing Gateway and AAA appliances first**, then everything else, then Console. Back up the configuration before each upgrade.
2. **Restrict NSIP and Console access** to management networks (this addresses CVE-2026-120863 and CVE-2026-120869 exposure).
3. MAG212 ANALYSIS **Treat old `httperror.log` files as sensitive** (CVE-2026-111338): limit who can read them and consider rotating credentials if they were copied off-box.

Verify recovery: both HA peers report the fixed build, HA sync is healthy, VPN and SSO logins work, and a test from an untrusted segment can't reach the Console. **Prevention** MAG212 ANALYSIS : subscribe to Citrix bulletin alerts, and keep a list of which features each appliance uses, so the next precondition check takes minutes.

UPDATE · MICROSOFT 365 / EXCHANGE ONLINE

04

Microsoft 365 outage enters day two with no root cause

Still degraded | No attack found | 12–13 Nov | Evidence: vendor status + press

INCIDENTS	STATUS 14:00 UTC FRI	CAUSE	NEXT
EX1550543 (Exchange Online) · MO1550821 (dependent services)	Service degradation, business and consumer	Not confirmed; secure-connection process overloaded	Post-incident report promised after mitigation

What changed since yesterday

CONFIRMED At 14:00 UTC on Friday (6 a.m. Pacific), Microsoft's public status page still listed Microsoft 365 business and enterprise services as degraded, with "Users may be unable to connect to multiple Microsoft 365 services", and consumer products also degraded. ↗ Microsoft status REPORTED Both incidents remain open. Microsoft says features that depend on Exchange Online are impacted while the rest keep working, has found no malicious activity, and will publish a post-incident report with root cause after mitigation. ↗ SecurityWeek

REPORTED Overnight, Microsoft described a process on the affected servers "that sets up secure connections" becoming overwhelmed, after which the servers stop handling requests. It paused all deployments and configuration changes around 19:06 UTC Thursday, began reverting a recent network change whose timing lines up with the outage, and at 04:57 UTC scaled up virtual machines to absorb a traffic surge. Servers returned to service around midnight UTC failed again under load. Microsoft has not said the network change caused the outage. ↗ LazyAdmin ↗ SOCRadar ↗ WindowsForum

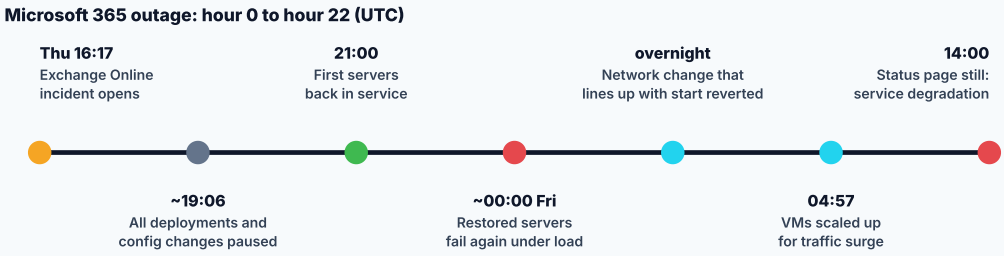


Figure 4 · Microsoft 365 outage, day two. Key moments reported by Microsoft and secondary outlets, UTC. Root cause is not confirmed.

MAG212 CYBER original chart, based on Microsoft's status page, SecurityWeek, LazyAdmin and SOCRadar (12–13 Nov 2026).

What to do now

Track the incident when the admin center won't load OS: Windows / macOS / Linux Shell: PowerShell 7 + Microsoft Graph SDK

Privileges: ServiceHealth.Read.All READ-ONLY

```
Connect-MgGraph -Scopes 'ServiceHealth.Read.All'
Get-MgServiceAnnouncementIssue -ServiceHealthIssueId 'EX1550543' |
  Select-Object Id, Status, Classification, LastModifiedDateTime, Title
Get-MgServiceAnnouncementIssue -ServiceHealthIssueId 'MO1550821' |
  Select-Object Id, Status, LastModifiedDateTime
```

Shows Microsoft's own status and last update time for your tenant. Sign-in may itself fail during the outage; use the public status page if so. **Commands not tested by MAG212 CYBER.**

1. **Users:** don't reset passwords or reinstall Outlook. Mail sent to you is normally delivered once service returns.
2. **IT:** freeze changes to MFA, Conditional Access and mail flow; send one status note a day; keep an out-of-band channel for urgent work.

3. MAG212 ANALYSIS **Security teams:** Defender XDR and Purview were on the affected list, so check for alert backlogs once service returns, and warn staff about outage-themed "re-verify your account" phishing.
4. **Afterwards:** read the post-incident report, check whether the outage qualifies for SLA service credits, and log your business impact.

Verify recovery: both incidents show as resolved, mail queues drain, and Teams calendars and SharePoint search behave normally. ↗ Our 12 Nov coverage

TAKEDOWN · GOOTLOADER, CASTLERAT, STEALC

05

Operation Endgame hits three malware networks and recovers over 6 million credentials

Victim notifications coming | 12 Nov | Evidence: strong (Europol)

ACTIONED	CREDENTIALS	WORDPRESS	NOTIFICATION
235 servers, 257 domains	Over 6 million identified (6.4M datasets)	681 infected sites remediated	HIBP, DIVD, Shadowserver, NL-NCSC and others

What happened

CONFIRMED Europol says law enforcement and private partners actioned **235 servers and 257 domains** behind three "cybercrime-as-a-service" tools. Germany's BKA dates the action to 9–11 November. Agencies from Bulgaria, Canada, Denmark, Germany, Moldova, the Netherlands, Poland, the UK and the US took part, with Europol's EC3 and Eurojust. Europol mentions no arrests. ↗ Europol ↗ BKA

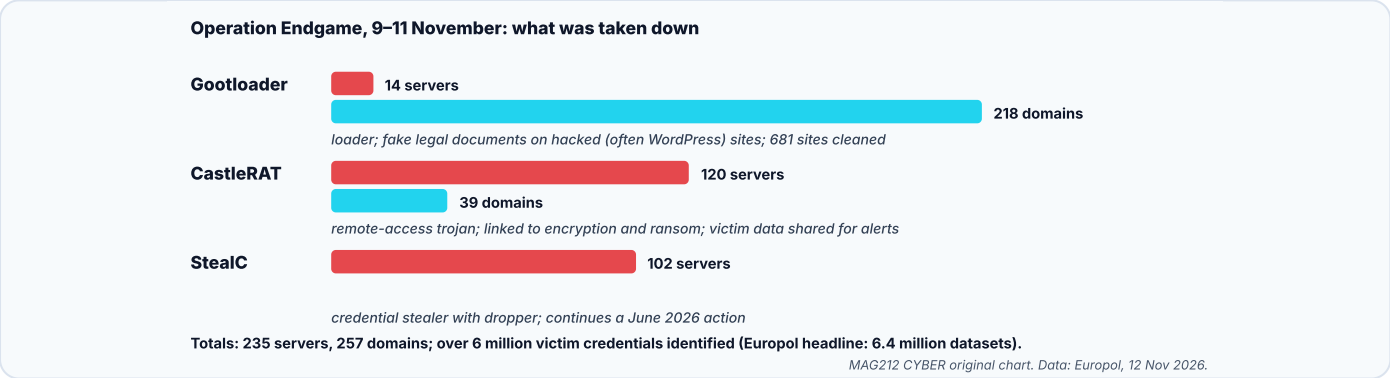


Figure 5 · Operation Endgame by the numbers. Servers and domains actioned per malware family, from Europol's release. *MAG212 CYBER original chart. Data: Europol (12 Nov 2026).*

Who is affected and how the tools work

CONFIRMED **Gootloader** spread through fake legal documents on hacked, often WordPress, sites and led on to ransomware: 14 servers and 218 domains came down and 681 infected websites were cleaned. **CastleRAT**, a remote-access trojan known since 2025, was linked to encrypted data and ransom payments: 120 servers and 39 domains were seized, with victim data shared for alerts. **StealC**, a credential stealer with a dropper, lost 102 servers, continuing a June 2026 action. Victims of stolen CastleRAT credentials will be alerted through HaveIBeenPwned, DIVD, CheckjeHack, NoMoreLeaks, Sekoia, the Shadowserver Foundation and NL-NCSC. ↗ Europol

What to look for and do

1. **Watch the notification channels.** Check your domains with Have I Been Pwned domain search, and your Shadowserver reports if you subscribe.
2. MAG212 ANALYSIS **For each validated hit:** isolate the device, reset passwords from a clean machine, and **revoke sessions and tokens**, because stealers take cookies as well as passwords. Then review MFA methods, mailbox rules and OAuth grants for the account.
3. MAG212 ANALYSIS **Hunt Gootloader:** look for a browser download of a `.zip` followed by `wscript.exe` or `cscript.exe` running a `.js` file, and for new scheduled tasks soon after.

4 **WordPress owners:** Europol urges updated credentials, MFA and patching. Also verify core, plugins and themes against clean copies.

Verify recovery: old sessions are rejected, no new sign-ins from unknown locations, and the rebuilt device is clean.
Prevention: see this issue's awareness lesson on downloading templates safely.

PUBLIC PROOF OF CONCEPT · WINDOWS CLFS AND DEFENDER

06

SignDrop: a public exploit borrows Microsoft Defender's privileges to reach SYSTEM

PoC public | No CVE, no fix yet | Not seen exploited | 13 Nov | Evidence: medium

What happened

REPORTED Researcher Abdelhamid Naceri ("Nightmare Eclipse") released **SignDrop** this week. It lets a **local, standard user** become **SYSTEM** by abusing how the Common Log File System (`clfs.sys`) creates its `.cnpf` authentication file. Cyderes compiled and tested the proof of concept and has seen **no exploitation in the wild**. SecurityWeek asked Microsoft for comment. ↗ SecurityWeek UNKNOWN At our cutoff we found no Microsoft advisory, CVE or fixed build.

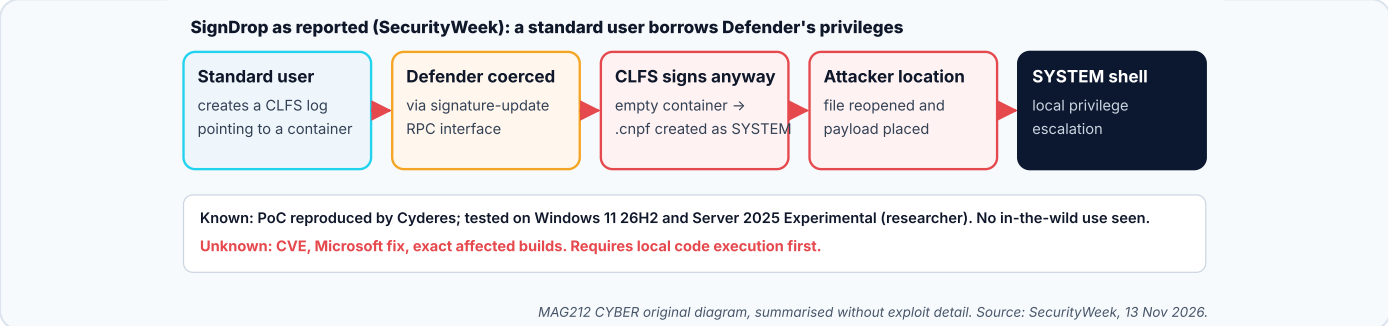


Figure 6 · How SignDrop reaches SYSTEM. A local user points a CLFS log at a chosen path and makes Defender open it. Requires code already running on the machine.
MAG212 CYBER original diagram, based on SecurityWeek (13 Nov 2026) and the researcher's description.

Who is affected and how it works

REPORTED The researcher says he tested it on Windows 11 26H2, Windows 11 26H2 Experimental and Windows Server 2025 Experimental. He claims it works on most Windows installations and that you're "generally vulnerable" if Windows is older than 90 days; neither claim is verified. The trick: if a log's container is empty, CLFS signs it whether or not a signature file exists. A user can point a log at a chosen path, make Defender open it through its signature-update interface, and so get a SYSTEM-owned file created where they choose. ↗ SecurityWeek MAG212 ANALYSIS This doesn't let anyone in from outside: an attacker first needs code running as a user, from phishing or a stolen login. That's exactly when ransomware crews want SYSTEM.

Inventory what you'll need when Microsoft responds OS: Windows 10/11, Server 2019+ Shell: PowerShell 5.1

Privileges: standard user READ-ONLY

```
# OS build and update revision (UBR)
$cv = Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion'
'{0} {1}.{2}' -f $cv.DisplayVersion, $cv.CurrentBuild, $cv.UBR
# Defender platform and engine versions
Get-MpComputerStatus | Select-Object AMProductVersion, AMEngineVersion, AntivirusSignatureLastUpdated
```

Record these per device so you can match them to Microsoft's fix when it ships. **Commands not tested by MAG212 CYBER.**

Contain, remediate and prevent

1 **Keep Windows and Defender platform updates current**, and watch the Microsoft Security Response Center for a SignDrop advisory.

2. MAG212 ANALYSIS **Hunt:** look for Defender processes (`MsMpEng.exe`) creating files in user-writable folders, followed by a new SYSTEM-level process, service or scheduled task started from that location.
3. **Reduce the first step:** no local admin for daily use, application control on workstations, and fast isolation for any machine running unknown code.

Verify recovery: once Microsoft ships a fix, confirm the build and UBR across the fleet and re-run your hunt over the period before patching.

ANALYSIS · AGENTIC PENETRATION TESTING

07

AI pentest agents, owned by defenders and by attackers, in the same week

Product launch | 12–13 Nov | Evidence: vendor + our 12 Nov reporting

What happened

CONFIRMED OpenAI announced two Daybreak products at its "Cyber at the Frontier" event on 12 November. **Daybreak Red Team** puts "a coordinated team of agents" to work testing web applications, validating findings from scanners, bug bounties and disclosure reports, and checking whether patches stop the exploit. Agents use source code and app context, and scope is enforced with "isolated environments and Guardian review". ↗ OpenAI REPORTED **Defense Factory** traces vulnerabilities through code and drafts patches as GitHub pull requests that engineers review; nothing deploys automatically. It imports findings from Wiz, Snyk and Endor Labs. Red Team is in early access; Defense Factory is a preview ChatGPT plugin. ↗ SecurityWeek ↗ OpenAI



Figure 7 · Same technique, different consent. OpenAI's Daybreak products and the attacker-run AntiFox platform side by side. *MAG212 CYBER original diagram, based on OpenAI, SecurityWeek and MAG212's 12 Nov reporting.*

Why it matters

MAG212 ANALYSIS One day earlier we reported AntiFox, a self-hosted agentic pentest platform that attackers used to move from an IIS web shell to a stolen AWS secret, making hundreds of API calls in about 30 minutes. ↗ MAG212, 12 Nov The technique is the same on both sides; what differs is **scope, consent and review**. Defenders who adopt these tools should insist on written scope, isolated test environments, logs of every agent action and human review of every patch. They should also expect attackers to test their apps at agent speed: watch for bursts of enumeration and AccessDenied errors, and fix what scanners already flag.

1. **Before buying:** ask how scope is enforced, where code and findings are stored, and who can see agent logs.
2. **Before running:** point agents at staging, not production, and tell your SOC so their traffic isn't mistaken for an attack.
3. **After:** treat AI-drafted patches like any pull request: review, test, then merge.

Defender's Action Desk

Prioritised from today's stories. **MAG212 ANALYSIS** for the ordering; sources are in each article.

- [ ] **NOW** **Check Point:** November Jumbo Hotfix on gateways and management, Mobile Access first; run the gateway and ESXi hunt. → 01
- [ ] **NOW** **N-central:** Legacy API off; check for `xvd.service` and miners; rebuild on a hit. → 02
- [ ] **NOW** **Barracuda (KEV due today):** confirm patch IDs on every ESG and other affected appliance; restrict admin UIs.
- [ ] **TODAY** **NetScaler:** plan upgrades to 14.1-73.57 / 13.1-64.39, Gateway and AAA first; Console to 14.1-74.34; lock NSIP and Console to management networks. → 03
- [ ] **TODAY** **Microsoft 365:** track EX1550543 and MO1550821; freeze identity changes; warn about outage phishing. → 04
- [ ] **THIS WEEK** **Endgame:** check HIBP domain search; revoke sessions for any confirmed stealer victim. → 05
- [ ] **THIS WEEK** **SignDrop:** inventory Windows builds and Defender versions; hunt for Defender writing to user folders. → 06
- [ ] **BY 16 NOV** **eMudhra:** replace emSign/eMudhra certificates before Microsoft removes the roots.

KEV deadlines (federal due dates; a priority signal for everyone)

CVE	Product	Added	Due
CVE-2026-116606 · -111560	**Barracuda ESG and others**	10 Nov	**13 Nov (today)**
CVE-2026-19868	SonicWall SonicOS SSLVPN	6 Nov	20 Nov
CVE-2026-124194 · -125350 · -20320 · -111793	Outlook · Chromium · Cisco BroadWorks · Openwave	10 Nov	24 Nov
CVE-2026-123039 · CVE-2026-90436	Check Point Gaia · Apache Axis (N-central)	**Exploited but not yet in KEV**	

Catalog 2026.11.10; no additions on 11–13 Nov at research time. Source: CISA KEV.

⏳ Pending at the cutoff: check before you act

- **N-able:** no fix for 4EverAble2Shell or Agent2Shell; its status page couldn't be read directly (statements via BleepingComputer).
- **Microsoft:** no root cause, no SignDrop advisory. **Check Point:** the advisory's SK link was still a placeholder.
- **Not opened:** CERT-EU and Canadian Cyber Centre Citrix advisories, the BKA release, Jumbo Hotfix pages (cited from the editor's draft).

Awareness lesson: "Need a contract template? Go to the source"

For employees, teachers and students

Gootloader, one of the networks taken down this week, spread by posting fake legal documents on hacked websites that ranked in search results. ↗ Europol

- Get templates from your legal team, an approved library, or a publisher's site you type in yourself.
- If a "document" arrives as a `.zip` with a script inside, don't open it.
- Already opened something odd? Tell IT now; speed matters more than blame.

For leaders and owners

"Firewalls, RMM servers and email are the keys to the building." **MAG212 ANALYSIS**

Ask this week: Who can reach our hypervisor and RMM consoles? Are firewall logs stored somewhere the firewall can't change? What do we do when Microsoft 365 is down for a day?

Write the answers down and test one.

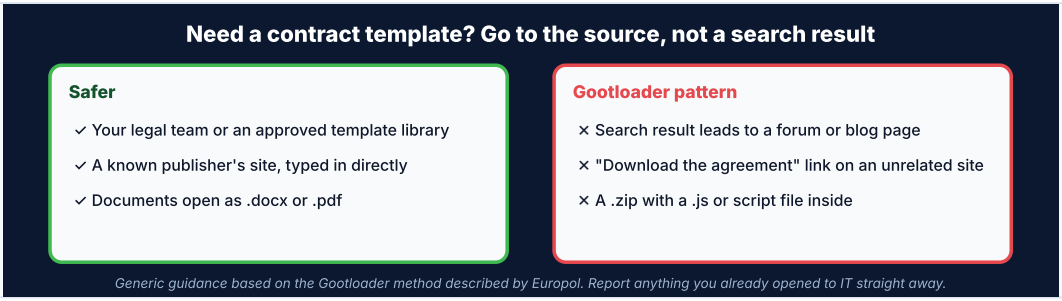


Figure 8 · Safe template versus Gootloader pattern. Where a real template comes from, and what a Gootloader download looks like. Generic guidance.
Conceptual MAG212 CYBER original illustration.

Briefly noted

- **Maersk.** REPORTED Maersk has confirmed data theft amid a $5 million extortion attempt (headline only). ↗ SecurityWeek
- **SilentAir.** REPORTED Hackers dubbed SilentAir intercepted calls and SMS from inside mobile networks (headline only). ↗ SecurityWeek
- **Node2Shell.** CONFIRMED The Brotli decompression flaw CVE-2026-111497 (KEV since 27 October) is also fixed in Check Point's November Jumbo Hotfix. ↗ Check Point

Source register

Every source behind this issue; titles link to the source. "No" means MAG212 didn't open it, and claims from it rest on other sources listed. "Headline only" items are reported, not verified. Links not re-fetched at publication. Corrections: cyber.mag212.com.

1 Check Point Blog: Security Advisory — Active Exploitation of PHP2Shell and Local Privilege Escalation
12 Nov 2026 · Primary (vendor) · Opened: Yes

2 Check Point Research: PHP2Shell Exploitation on Check Point Gateway
12 Nov 2026 · Primary (researcher) · Opened: Yes

3 Check Point: R81.20 Jumbo Hotfix Take 174
Nov 2026 · Primary (vendor) · Opened: No (cited by editor draft)

4 Check Point: R82.10 Jumbo Hotfix Take 52
Nov 2026 · Primary (vendor) · Opened: No (cited by editor draft)

5 SecurityWeek: PHP2Shell Exploited in Destructive Check Point Gateway Attacks
12 Nov 2026 · Trade press · Opened: Headline only

6 BleepingComputer: New N-able 4EverAble2Shell zero-day exploited hours after PoC released
12 Nov 2026 · Trade press (quotes N-able advisory, Previdian, Huntback) · Opened: Yes

7 SecurityWeek: Hackers Exploit New N-central Zero-Day Hours After PoC Publication
13 Nov 2026 · Trade press · Opened: Search extract

8 SecurityWeek: N-able Takes N-central Offline as Researcher Drops Over 30 Zero-Days
10 Nov 2026 · Trade press · Opened: Search extract

9 N-able: N-central status and advisories (uptime page)
9–12 Nov 2026 · Primary (vendor) · Opened: No (script-only page; quoted via #6)

10 SOCRadar: 4EverAble2Shell at a glance
13 Nov 2026 · Analysis · Opened: Search extract

11 Citrix CTX697305: NetScaler ADC and NetScaler Gateway Security Bulletin
12 Nov 2026 (upd. 13 Nov) · Primary (vendor) · Opened: Yes

12 Citrix CTX697320: NetScaler Console Security Bulletin for CVE-2026-120869
12 Nov 2026 · Primary (vendor) · Opened: Yes

13 CERT-EU Security Advisory 2026-020 (Citrix NetScaler)
12 Nov 2026 · Government CERT · Opened: No (cited by editor draft)

14 Canadian Centre for Cyber Security: Citrix security advisory AV26-1150
12 Nov 2026 · Government CERT · Opened: No (cited by editor draft)

15 NetScaler developer docs: show ns version
current · Primary (vendor docs) · Opened: No (cited by editor draft)

16 Microsoft service health status (status.cloud.microsoft)
13 Nov 2026 14:00 UTC · Primary (vendor) · Opened: Yes

17 SecurityWeek: Microsoft 365 Outage Disrupts Outlook, Exchange Online and Teams (updated)
13 Nov 2026 · Trade press · Opened: Search extract

18 LazyAdmin: Microsoft 365 Outage — Current Status and SLA Credits
13 Nov 2026 · Practitioner blog · Opened: Search extract

19 SOCRadar: Microsoft Outlook Outage — What You Need to Know
13 Nov 2026 · Analysis · Opened: Search extract

20 WindowsForum: Microsoft 365 Outage — Server Health Checks, Network Rollback and an Unconfirmed Root Cause
13 Nov 2026 · Community analysis · Opened: Search extract

21 MAG212 CYBER: Microsoft 365 Outage (12 Nov coverage)
12 Nov 2026 · Own coverage · Opened: Yes

22 Europol: 6.4 million victim datasets secured in international operation against malware networks
12 Nov 2026 · Primary (law enforcement) · Opened: Yes

23 BKA press release on Operation Endgame (Presseportal)
12 Nov 2026 · Primary (law enforcement) · Opened: No (cited by editor draft)

24 Have I Been Pwned (victim notification partner)
current · Service · Opened: No

25 SecurityWeek: Nightmare Eclipse Drops Windows Zero-Day Exploit SignDrop
13 Nov 2026 · Trade press · Opened: Yes

26 Threadlinqs intel TL-2026-5950 (SignDrop)
Nov 2026 · Threat intel · Opened: No (cited by editor draft)

27 OpenAI: Daybreak Red Team
12 Nov 2026 · Primary (vendor) · Opened: Yes

28 OpenAI: Daybreak Defense Factory
12 Nov 2026 · Primary (vendor) · Opened: No

29 OpenAI: Cyber at the Frontier
12 Nov 2026 · Primary (vendor) · Opened: No

30 SecurityWeek: OpenAI Unveils Daybreak Red Team, Defense Factory Security Tools
13 Nov 2026 · Trade press · Opened: Yes

31 MAG212 CYBER: AntiFox AI pentest platform in real intrusions (12 Nov)
12 Nov 2026 · Own coverage · Opened: Yes

32 CISA Known Exploited Vulnerabilities catalog (GitHub mirror, v2026.11.10)
10 Nov 2026 · Government · Opened: Yes

33 CISA KEV catalog (web)
current · Government · Opened: No

34 MAG212 CYBER: SCKit ScreenConnect MSP campaign (12 Nov)
12 Nov 2026 · Own coverage · Opened: Yes

35 SecurityWeek: Maersk Confirms Data Theft Amid $5 Million Extortion Attempt
Nov 2026 · Trade press · Opened: Headline only

36 SecurityWeek: SilentAir Hackers Intercept Calls, SMS From Inside Mobile Networks
13 Nov 2026 · Trade press · Opened: Headline only

37 Barracuda Trust Center advisory (KEV pair due 13 Nov)
10 Nov 2026 · Primary (vendor) · Opened: Yes (11 Nov edition)

38 Huntress: N-able Disables Cloud Services Following Disclosure of "Able2Shell" Exploit Chains
9–10 Nov 2026 · Security vendor · Opened: Search result 13 Nov

MAG212 CYBER

DAILY CYBER INTELLIGENCE

Get tomorrow's briefing before your first coffee

Verified stories, the three actions that matter, and clear labels for what's confirmed, reported and still unknown. Free.

Subscribe free →

cyber.mag212.com/subscribe-free

Verified, not viral
Primary sources first, conflicts flagged, nothing invented.

Built for defenders
Versions, fixes, log locations and ordered remediation steps.

For every team
Network engineers, MSPs, school IT, IT managers and owners.

Editor: **El Mostafa Ouchen** · cyber.mag212.com · Issue MAG212_CYBER_Daily_2026-11-13