FEATURE: SUPPLY CHAIN UNDER SIEGE

GlassWorm Dismantled -- But the Developer Toolchain Is Still Broken

June 1, 2026 | uMercs Intelligence Team

On May 26, CrowdStrike, Google, and the Shadowserver Foundation simultaneously took down all four command-and-control channels for GlassWorm -- a Russian-linked supply chain operation poisoning developer tooling since October 2025. The coordinated timing was deliberate: cutting all channels at once denied operators any pivot window. Infected endpoints were redirected to a benign sinkhole IP.

GlassWorm's model was disciplined and patient. Trojanized VS Code extensions hit both the Microsoft VS Code Marketplace and Open VSX. Malicious packages were pushed to npm and PyPI. Over 300 GitHub repositories were compromised across the campaign. The malware skipped CIS countries and contained Russian-language comments -- standard state-adjacent tells.

The takedown disrupts the operation. It does not fix the underlying problem. Open-source registries have no mandatory code review, no identity verification for publishers, and minimal tooling to detect malicious updates post-publication. GlassWorm operators can resurface under new accounts tomorrow. The infrastructure is gone. The attack surface is not.

Developers with GlassWorm-infected environments had credentials, API tokens, SSH keys, and 2FA secrets at risk -- along with every repository they touched. CI/CD pipeline manipulation and code signing key exposure are direct downstream consequences.

What to do now:

- Check for beacon traffic to sinkhole 164.92.88[.]210 -- indicates infection
- Audit VS Code extensions against known GlassWorm IOCs
- Rotate API tokens and SSH keys for any potentially exposed developer
- Implement dependency pinning and hash verification for npm and PyPI packages
- Restrict VS Code Marketplace installs to an approved, audited allowlist

OFFENSIVE SECURITY: WHY YOUR RED TEAM IS FLYING BLIND

AI-Assisted Attackers Are Outpacing Manual Red Team Cadences

June 1, 2026 | uMercs Intelligence Team

CERT-In's new 12-hour patch guidance is a signal most security teams are not ready to act on -- and the reason is straightforward: their red team cadence has not kept up with attacker tooling. Annual or quarterly penetration tests were already inadequate. Against adversaries using AI to compress weaponization timelines from days to hours, they are operationally irrelevant.

GREYVIBE's operational use of LLMs is not an outlier. It is a preview. The same AI infrastructure available to nation-state actors is accessible to organized criminal groups at commodity pricing. Recon that previously required skilled operators and days of manual effort now runs autonomously. Attack chains that required custom tooling are now generated on demand.

The gap this creates is not a vulnerability gap -- it is a visibility gap. Organizations are not seeing their own attack surface the way adversaries see it. A red team engagement that runs once a year and covers a scoped subset of infrastructure tells you what was exploitable on the day it was tested. It tells you nothing about what is exploitable today.

Continuous offensive security validation -- running the same techniques adversaries use, at the same pace -- is the only model that closes this gap. AI-assisted pen testing agents do not replace human operators. They extend coverage to the parts of the attack surface that manual cadences cannot reach.

RANSOMWARE BRIEF

Interlock: 1.7M Patients, 44 Lawsuits

Kettering Health -- a 14-hospital Ohio system -- completed breach notifications covering 1.7 million patients following the May 2025 Interlock ransomware attack. The group exfiltrated 941 GB and published it after no ransom was paid. The system now faces 44 civil lawsuits. All 600 patient care systems were shut down. Healthcare remains the highest-value ransomware target by ransom paid per incident.

GEO-INTEL

GREYVIBE: AI Integrated Into Russian Ops

WithSecure identified GREYVIBE, a previously undocumented Russian group active since August 2025, targeting Ukrainian private, government, and military orgs. LLMs are operational components -- not experiments -- in their reconnaissance and targeting workflows. Assessed to be collecting intelligence for active military operations.

CERT-In separately warned that AI is compressing time from disclosure to exploitation, recommending 12-hour patch cycles for critical internet-facing systems.

PATCH PRIORITY

CVE-2026-0257 -- PAN-OS GlobalProtect

Auth bypass. CVSS 7.8. Active exploitation confirmed.

CVE-2026-8732 -- WP Maps Pro

Admin account creation. 2,858 attacks in first 24 hours.

CVE-2026-32996/32997 -- Veeam Backup

RCE in backup infrastructure. Ransomware groups target backups first.

Gogs -- Zero-Day (No Patch)

Unpatched RCE. Authenticated user can exploit. Disable open registration now.

BY THE NUMBERS

138 Microsoft CVEs patched in May Patch Tuesday

30 classified Critical

300+ GitHub repos compromised by GlassWorm

941 GB data exfiltrated in Kettering Health breach

12 hrs CERT-In recommended patch window for critical systems

2,858 attacks on WP Maps Pro in first 24 hours

CVE SPOTLIGHT: CRITICAL WINDOWS DNS RCE

CVE-2026-41096: Unauthenticated Remote Code Execution in Windows DNS Client

June 1, 2026 | uMercs Intelligence Team

May's Patch Tuesday delivered 138 fixes -- 30 classified Critical -- but the one demanding immediate action is CVE-2026-41096: CVSS 9.8, unauthenticated RCE in the Windows DNS Client. No user interaction. No elevated privileges required. An attacker on the same network -- or positioned to send crafted DNS responses -- can execute arbitrary code on affected systems.

The Windows DNS Client runs on every domain-joined Windows machine by default. Exploitation does not require prior authentication, making this both a lateral movement and initial access vector in the same CVE. Microsoft assessed exploitation as 'more likely' -- Redmond's way of saying working exploits exist or will shortly.

Running alongside it: CVE-2026-42898, CVSS 9.9 RCE in Microsoft Dynamics 365 on-premises -- the highest score this month. And CVE-2026-40361 in Microsoft Word achieves RCE via the preview pane. No file open required. Effective phishing vector against targets who think not opening attachments protects them.

Also confirmed: two Microsoft Defender vulnerabilities (CVE-2026-41091 and CVE-2026-45498) with active exploitation. Your endpoint protection tool was being exploited in the wild. Patched in the June 3 fixes. Confirms the pattern from Apex One last month -- security tooling is now an active attack surface, not a defense.

GOGS ZERO-DAY: NO PATCH, ACTIVE RISK

Rapid7 disclosed an unpatched critical RCE in Gogs, the open-source self-hosted Git service. Any authenticated user can exploit it via pull requests with malicious branch names. Default deployments ship with open registration -- unauthenticated attacker creates an account, enables rebase merging, and achieves RCE as the server process. No patch exists. Disable open registration and restrict rebase permissions now.

PATCH TUESDAY SUMMARY: MAY 2026

138 total CVEs. 30 Critical. Key patches beyond the DNS RCE: BitLocker bypass (YellowKey, Windows 11 and Server 2022/2025), Windows Netlogon stack overflow (network-based RCE, no auth), SharePoint RCE (CVE-2026-45659), and PuTTY vulnerability (CVE-2026-4115). If your organization runs any of these -- patching is not optional this cycle.

CVE CARDS

CVE-2026-41096
Windows DNS Client RCE | CVSS 9.8
Unauthenticated RCE via crafted DNS response. All domain-joined Windows systems. No interaction required. Every Windows machine in scope. Patch immediately.

CVE-2026-42898
Microsoft Dynamics 365 RCE | CVSS 9.9
Code injection in Dynamics 365 on-premises. Highest CVSS this month. Top priority after DNS if you run on-prem Dynamics.

CVE-2026-40361
Microsoft Word Preview Pane RCE | CVSS 8.4
RCE triggered via preview pane -- victim does not open the file. Disable preview pane as interim mitigation.

CVE-2026-0257
PAN-OS GlobalProtect Auth Bypass | CVSS 7.8
Authentication bypass enabling unauthorized VPN connections. Actively exploited. Affects GlobalProtect with auth override cookies enabled.

DEFENDER CHECKLIST: JUNE 2026

Priority actions this month:

1. Patch CVE-2026-41096 (Windows DNS Client) -- CVSS 9.8, unauthenticated RCE, all Windows systems in scope
2. Patch CVE-2026-42898 (Dynamics 365 on-prem) -- CVSS 9.9, code injection
3. Patch PAN-OS GlobalProtect (CVE-2026-0257) -- active exploitation confirmed
4. Audit VS Code extensions and npm/PyPI packages for GlassWorm IOCs
5. Check for outbound connections to 164.92.88[.]210 (GlassWorm sinkhole)
6. Rotate developer credentials: API tokens, SSH keys, 2FA secrets
7. Disable Word preview pane as interim mitigation for CVE-2026-40361
8. Disable Gogs open registration -- no patch exists, exposure is immediate
9. Patch Veeam Backup (CVE-2026-32996/32997) -- ransomware targets backup first
10. Apply June 3 Defender patches (CVE-2026-41091, CVE-2026-45498) -- both actively exploited

CYBER TIP: YOUR SECURITY TOOLS ARE THE TARGET

Three months running, security tooling has been the attack vector: Apex One in May, Defender this week, GlassWorm targeting developer environments directly. The pattern is intentional. Security tools get implicit trust, run with elevated privileges, and bypass inspection by design. Attackers know this.

Treat your security stack like any other third-party software: audit it, scope its privileges, monitor its network activity, and patch it first -- not last. A security tool with admin rights and an unpatched RCE is a liability, not a defense.

The same logic applies to developer tooling. Your IDE extensions and package manager have the same access to your codebase as your most privileged developer. GlassWorm proved that trust gets operationalized.

THREAT CONTEXT

AI Is Compressing Patch Windows

CERT-In issued guidance recommending 12-hour patch cycles for critical internet-facing systems. The driver: AI tools are accelerating time-to-exploit. A vulnerability that once took days to weaponize can now be converted in hours. The math on patch windows has changed permanently.

GREYVIBE is already using LLMs operationally. AI chatbot campaigns are redirecting security searches to cryptojacking malware in real time. The tools are cheap, accessible, and deployed at multiple sophistication levels.

ABOUT UMERCS

uMercs delivers offensive security engagements built around AI-assisted pen testing, red team operations, and continuous security validation. Our AI pen test agents cover web application, external network, internal network, and Active Directory attack surfaces.

We work with organizations that need security testing at the speed and scale that manual-only programs cannot support. If your patch windows are shrinking and your attack surface is growing -- that is the environment we are built for.

Contact: info@umercs.com | umercs.com

SOURCES

The Hacker News: Weekly Recap, June 1, 2026
CrowdStrike: GlassWorm Takedown, May 27, 2026
SC World / CrowdStrike: Patch Tuesday Analysis, May 2026
HIPAA Journal: Kettering Health Breach Notifications, 2026
WithSecure: GREYVIBE Threat Actor Profile, June 2026
Rapid7: Gogs Zero-Day Disclosure, June 2026
Microsoft Security: Defender CVE Advisories, June 3, 2026
CERT-In: Vulnerability Patch Timeline Framework, June 2026

THIS MONTH IN INFOSEC

"Our red team found four critical vulnerabilities."
"Great. When do we patch them?"

"Patch Tuesday is in three weeks."
"CERT-In says we have twelve hours."

"So who do we listen to?"
"Whoever gets here first. You should probably start running."

-- This panel was written in under 12 hours. The patch probably was not.