Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | AUG | Vol.3

The News

In the news week

TWINLOOT Abuses SharePoint and Teams to Steal Credentials and Move Across Networks

Threat actors have begun leveraging a newly identified malware framework known as TWINLOOT, which abuses trusted Microsoft 365 services for command-and-control (C2), credential theft, and lateral movement across victim networks. Researchers discovered the activity during an investigation into an ongoing campaign in July 2026.

The malware is a modular Python-based implant that operates through legitimate Microsoft services, including SharePoint Online for tasking and data exfiltration, Microsoft Teams TURN relays for interactive access, and the victim's own Edge browser to disguise malicious communications as normal activity.

According to Ontinue, attackers gain initial access through Microsoft Teams social engineering attacks, impersonating IT support staff and convincing users to execute malicious PowerShell commands. Once deployed, TWINLOOT can harvest credentials via fake lock screens, establish persistence, execute commands, and enable stealthy movement throughout compromised environments.

Read more ›

Other news highlights

Mustang Panda Adds Signed Windows Rootkit to CoolClient Backdoor for Stealth

–

Forminator WordPress Flaw Can Enable Unauthenticated RCE via Malicious PHP Uploads

–

Evooo1Bot Linux Botnet Exploits Known Flaws to Turn Edge Devices Into SOCKS5 Proxies

–

Shadow hVNC Lets Hackers Operate a Second Windows Desktop Invisible to the Victim

The News

Top of the news

StopAndProtect Uses Nearly 2,000 Hacked WordPress Sites to Spread Malware and Steal Data

Researchers have uncovered a large-scale cybercrime operation dubbed StopAndProtect, which leverages nearly 2,000 compromised WordPress websites to distribute malware, manage infected systems, and store exfiltrated data. The campaign uses ClickFix-style social engineering attacks to trick users into executing malicious PowerShell commands that initiate a multi-stage infection process.

The malware toolkit includes ransomware, credential stealers, lock-screen malware, propagation mechanisms, and data collection components. In many cases, attackers focus on stealing sensitive files, screenshots, activity logs, and credentials rather than deploying ransomware. The compromised WordPress sites serve as malware-hosting infrastructure, command-and-control (C2) servers, and repositories for stolen data.

According to Check Point Research, the operation has compromised more than 6,000 unique IP addresses and primarily targets Windows users. The findings demonstrate how threat actors can exploit poorly maintained websites to create distributed infrastructure supporting malware delivery, surveillance, data theft, and ransomware operations

Read more ›

Other news highlights

Chrome DevTools Technique Enables Authenticated Session Hijacking in Live Windows Browsers

–

Novel macOS Infostealer AmnesiaStealer Spread via ClickFix

–

SAP Commerce Cloud CVE-2026-58231 Targeted in Exploitation Attempts Days After Patch

–

Snowflake GitHub Actions Flaw Lets Crafted Issues Trigger Command Injection

Geo-Politics

News from around the world

Suspected China-Nexus Actor Exploits VMware vCenter Flaw, Deploys Babuk-Derived Ransomware

Researchers have attributed the exploitation of a critical VMware vCenter vulnerability, tracked as CVE-2026-59310 (CVSS 9.8), to a suspected China-linked threat actor. The flaw, which allows remote code execution via a directory traversal weakness, has been exploited since shortly after public disclosure and is estimated to have impacted 361 unique victim IP addresses across 47 countries.

According to QUIRSO, the threat actor used the vulnerability to gain root-level access to vulnerable vCenter appliances, deploy backdoors, create privileged accounts, establish persistence, and install reverse SSH tools for remote access. Researchers also observed web shells, credential theft techniques, and abuse of scheduled tasks to maintain control over compromised systems.

In at least one case, the intrusion led to the deployment of a Babuk-derived ransomware payload targeting ESXi hosts. However, researchers believe the ransomware may have been used primarily to disrupt investigations and conceal broader post-compromise activity.

Read more ›

Other news highlights

SilkParasite Espionage Campaign Targets Central Asian Governments with Five New RATs

—

Trump Memo Paves Way for U.S. Firms to Hack and Disrupt Foreign Crime Groups

—

China-Linked Jewelbug Uses XG-Web for Government Espionage and Crypto Fraud

—

US Charges 17 Iranian Hackers Over Theft of 31.5TB of Academic Data

Breaches

Security Breaches this week

Shell, Philips and GE Among 50 Firms Affected by Data Breach

The Clop ransomware group has reportedly exploited a zero-day vulnerability (CVE-2026-12569) in a product lifecycle management (PLM) platform, impacting nearly 50 organisations in a large-scale supply chain attack. Victims reportedly include Shell, Philips, GE, and Fiserv, with attackers gaining access to sensitive corporate systems and data.

According to Clop, the breach resulted in the theft of 89GB of data from Shell, 15.5GB from Philips, and 391GB from GE. The stolen information is believed to include engineering documentation, project blueprints, and other proprietary business data. Shell, Philips, and GE have all confirmed they are investigating the alleged compromise.

The incident demonstrates how a single zero-day vulnerability in a widely used enterprise platform can provide threat actors with simultaneous access to multiple high-profile organisations through a shared software dependency.

Read more >

Other news highlights

Sakura Internet hack exposes data of up to 1.36 million accounts

–

Healthtech firm CareCloud data breach impacts 3.7 million patients

–

1.6M RingCentral accounts' data dumped after ShinyHunters extortion attack

–

LockBit Claims Breach of German Local Government Authority

Vulnerabilities

Vulnerabilities & Exploits

CVE-2026-55040 – Microsoft SharePoint is affected by a weak authentication vulnerability that could allow an unauthorised attacker to bypass security controls over a network. Successful exploitation may enable access to files and modification of data. The flaw has been observed being exploited by threat actors following the public release of proof-of-concept (PoC) exploit code

CVSS score: 9.1

CVE-2026-59310 – VMware vCenter is affected by a path traversal vulnerability that could allow a remote attacker with network access to execute arbitrary code on vulnerable systems. Successful exploitation may lead to full system compromise.

CVSS score: 9.8

Last weeks recaps

CVE-2026-33824 – Microsoft Internet Key Exchange (IKE) Service Extensions is affected by a double-free vulnerability that could allow remote code execution.

CVSS 9.8

–

CVE-2026-65400 – Apple macOS is affected by an improper authentication vulnerability that could allow an attacker on the same network to access Screen Sharing services without valid credentials.

CVSS 9.8

Ransomware

Weekly Ransomware Roundups

Overview
In July 2026, ransomware activity recorded a total of 954 victims globally, marking a 34.9% increase from the 707 victims reported in June 2026

Target industries
In July 2026, ransomware activity recorded a total of 954 victims globally, marking a 34.9% increase from the 707 victims reported in June 2026

Target country
The United States remained the most targeted country in July 2026, accounting for 318 victims and approximately 33% of globally attributed incidents

Top Group
TheGentlemen recorded 177 victims, taking the top position after trailing Qilin last month. The group operates a fully featured RaaS platform offering affiliates a 90% revenue share — among the highest in the underground market — a structure designed specifically to draw experienced operators away from competing program

Top Threat Actors

The Gentlemen

The Gentlemen (also tracked as Storm-2697) is a fast-growing, financially motivated Ransomware-as-a-Service (RaaS) and double-extortion threat group active since mid-2025.

–

Qilin

Qilin is a ransomware-as-a-service operation linked to Russia, encrypting and stealing data for ransom. Active since October 2022, it has targeted organizations like The Big Issue and Yanfeng.

–

DeadLock

DeadLock is a financially motivated ransomware group active since mid-2025. The group is known for utilizing decentralized infrastructure—such as Polygon blockchain smart contracts—to dynamically manage command-and-control proxy URLs and evade traditional network blocking.

Phishing

Phishing news this week

MaaS Campaign Combines ClickFix, ErrTraffic and Cruciferra

Researchers have identified a malware-as-a-service (MaaS) campaign that combines ClickFix social engineering techniques, the ErrTraffic traffic distribution service, and the Cruciferra malware loader to deliver malware while actively disabling security tools. The campaign leverages compromised WordPress websites to host malicious content and lure victims into executing attacker-controlled PowerShell commands.

According to eSentire, the attack chain used ErrTraffic-generated fake reCAPTCHA, Cloudflare Turnstile, and BSOD prompts to trick users into running malicious commands. Once executed, additional payloads sideloaded the Cruciferra loader, which then deployed the Remus information stealer using process hollowing techniques and legitimate Microsoft-signed binaries.

Cruciferra is marketed as an EDR-killing malware loader and was observed abusing a vulnerable driver to terminate antivirus and endpoint detection processes. Researchers noted that the campaign highlights how threat actors can combine multiple MaaS offerings to outsource malware delivery, social engineering, and defence evasion capabilities.

Read more ›

Other news highlights

Mirage2FA Campaign Steals Microsoft 365 Sessions After MFA Completion

–

Novel macOS Infostealer AmnesiaStealer Spread via ClickFix

–

Initial Access Brokers have Shifted to High-Value Targets and Premium Pricing

–

ClickFix Phishing Campaign Masquerading as a Claude Installer