Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | AUG | Vol.4

The News

In the news week

Actively Exploited Oracle WebLogic Flaw Lets Unauthenticated Attackers Access Critical Data

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a maximum-severity security flaw impacting Oracle HTTP Server and Oracle WebLogic Server to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

The vulnerability, tracked as CVE-2026-21962 (CVSS score: 10.0), allows an unauthenticated attacker with network access via HTTP to compromise Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in. Successful exploitation of the flaw can lead to unauthorized access to the instances or modification of critical data.

"Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in contain an improper access control vulnerability that can result in unauthorized creation, deletion, or modification access to critical data as well as unauthorized access to critical data or complete access to all Oracle HTTP Server and Oracle WebLogic Server Proxy Plug-in accessible data," CISA said.

Read more ›

Other news highlights

14 Trojanized npm Packages Drop RedC2 4.0 Linux Backdoor With AI-Assisted C2

–

Microsoft Defender's Own Driver Can Be Weaponized to Delete Security Software at Boot

–

Cisco Patches Nine Crosswork and Secure Workload Flaws, Five Scoring CVSS 10.0

–

Microsoft Patches Severe Entra ID Flaw (CVSS 10.0) Allowing Remote Code Execution

The News

Top of the news

WordlistLoader Delivers Amatera via ClickFix, SynkLoader Phishes Windows Passwords

Cybersecurity researchers have flagged two new malware families called WordlistLoader and SynkLoader that's used to deliver next-stage payloads and likely sell access to ransomware groups.

According to findings from Gen Digital, WordlistLoader is being used to deliver Amatera Stealer (aka ACR Stealer or AcridRain Stealer) via ClearFake campaigns, which employ the ClickFix (aka FakeCaptcha) technique to dupe victims into running malicious commands under the pretext of completing CAPTCHA verification checks.

"Once the visitor clicks on the 'I'm not a robot' checkbox, they're walked through the well-known ClickFix flow, where a malicious command is copied into their clipboard and the victim is instructed to paste it into the Windows Run dialog and execute it, leading to the download of WordlistLoader that ultimately results in the execution of Amatera," security researcher Vojtěch Krejsa said.

Read more ›

Other news highlights

UAT-10147 Uses AI to Scale Server Attacks, Deploys SPECTRE With EDR Bypass and Linux Rootkit

–

Critical Keycloak Password Reset Flaw Could Let Unauthenticated Attackers Take Over Any Account

–

Weedhack Malware Spreads via Fake Minecraft Clients and SEO Poisoning

–

Attackers Target miniOrange SAML Flaws That Can Grant WordPress Admin Access

Geo-Politics

News from around the world

Mirage2FA Surge Hits 4,500 US and EU Companies, Abusing Microsoft 365 Login Flows

Thousands of companies have been affected by the Mirage2FA campaign from 2024 to 2026. The commercial phishing-as-a-service toolkit targets Microsoft 365 accounts by abusing legitimate login flows and bypassing two-factor authentication. According to ANY.RUN research, 48% of targeted email addresses were potentially compromised. Most of the affected companies are US-based.

Mirage2FA Campaign Scope and Impact

By stealing passwords and session cookies, attackers can gain access to authenticated Microsoft 365 sessions and SSO-connected services. This creates significant identity-related risks for companies, potentially exposing corporate email, trusted business accounts, and other sensitive data.

Once an authenticated Microsoft 365 session is hijacked, a path for impersonation, fraud, and further compromise is created.

Read more ›

Other news highlights

Operation QUICSILVER Targets Myanmar Government and IT with QUICAgent Backdoor

—

TikTok Agrees to $400 Million Settlement in U.S. Child Privacy Lawsuit

—

Pro-Russian hackers claim responsibility for major cyberattack on Norway's public digital services

—

Red Flags That Expose Fake North Korean IT Workers

Breaches

Security Breaches this week

Personal Information Exposed in Apollo Global Data Breach

Private equity giant Apollo Global Management has disclosed a data breach that exposed sensitive personal information.

According to a data breach notice sent to affected individuals, a social engineering attack enabled threat actors to access some of the company's cloud platforms between July 6 and 10.

An investigation is ongoing, but Apollo determined recently that personal information may have been compromised, including names, contact information, and SSNs.

The company has not shared any information about who is behind the attack, but noted that it found no evidence that the compromised personal information was made public or used for fraud. Nevertheless, impacted individuals are being offered identity protection and credit monitoring services.

It's unclear how many individuals are affected by the data breach.

The private equity firm, which has roughly $1.05 trillion of assets under management, appears to be one of the victims of a campaign conducted by a cybercrime group tracked as UNC6671 and BlackFile.

Read more ›

Other news highlights

ReliaQuest Confirms ShinyHunters Hack, but Says Impact Was Limited

–

FBI, DOJ Seize Chinese Hacker Infrastructure on US Soil

–

Cyberattack Disrupts Boston Scientific's Global Operations

–

Attackers Targeted Over 100 US Water Systems in July Hacks

Vulnerabilities

Vulnerabilities & Exploits

[CVE-2026-69836](#) - Deserialization of untrusted data in Microsoft Entra ID allows an unauthorized attacker to execute code over a network.

[CVSS score: 10.0](#)

[CVE-2026-20030](#) - Cisco Crosswork, improper neutralization of special elements used in a SQL command issues that are grouped under the Common Weakness Enumeration

[CVSS score: 10.0](#)

Last weeks recaps

[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 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 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

ZeroTokens Phishing Platform Steers Attacks in Real Time

A phishing platform dubbed ZeroTokens allows attackers live visibility into victim sessions and the ability to change subsequent prompts in real time, allowing attacks to adapt in real time while targeting credentials and financial information.

The platform allowed an operator to monitor information entered by victims and steer individual phishing flows while separately using the harvested data against the genuine institution.

Abnormal AI published its analysis of the campaign on August 25. It found that more than 45,000 messages were sent to over 24,000 recipients across more than 700 organizations. Some 24,000 messages were sent on a single peak day, according to the research.

The campaign used ten sender domains and nine abused SendGrid accounts. Messages passed SPF, DKIM and DMARC checks and used W-8BEN tax-documentation reviews as a believable pretext for recipients with US securities holdings.

The phishing site reproduced the targeted financial institution and could present up to eight stages modeled on its verification process. As victims entered information, ZeroTokens reported the session state to its platform and allowed an operator to choose which screen appeared next.

Read more ›

Other news highlights

Def Con Attendees Targeted by Persistent Phishing Campaign

–

MaaS Campaign Combines ClickFix, ErrTraffic and Cruciferra

–

ReliaQuest Rejects Compromise Claims After ShinyHunters Incident

–

Fake Codex Download Uses Google Sites to Deliver macOS Malware