Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | AUG | Vol.1

The News

In the news week

Over 250 ClickFix Domains Use Browser Fingerprinting to Hide macOS Malware Lures

A macOS ClickFix operation spanning more than 250 front-end domains now fingerprints visitors before deciding whether to show them a malware lure, a change Microsoft Threat Intelligence tracked on infrastructure it had been watching for weeks.

The server-side gate hides the malicious page from crawlers and sandboxes while presenting selected Mac users with a fake software download. Microsoft said the wider cluster distributed MacSync and Atomic Stealer (AMOS); the chain it analyzed through the gate ended in AMOS.

The attack still requires the user to copy and run an obfuscated command in Terminal. That command retrieves scripts and launches an infostealer targeting credentials, browser data, authentication stores, cryptocurrency wallets, and sensitive files. Microsoft has not disclosed victim numbers, targeted sectors, or the identity of the operators.

Users should not follow any website, CAPTCHA, chat, or download instruction that asks them to paste text into Terminal.

Read more ›

Other news highlights

Veeam, Terraform MCP, Django Patch Critical Flaws, Led by CVSS 10.0 Cross-Tenant Bug

–

Fake Adobe and Zoom Updates Install ScreenConnect for Persistent Remote Access

–

Google Deletes 3 ADK AI Workflows After Malicious GitHub Issue Could Trigger Privileged Agent

–

CISA Adds Exploited N-able N-central Flaw to KEV After Customer Compromises

The News

Top of the news

Kali365 Weaponizes Microsoft Authentication Against US Companies: New Enterprise Risk

Kali365 is turning a legitimate Microsoft login into a gateway to corporate data.
The phishing kit targets US organizations with attacker-controlled device codes that victims approve on Microsoft's real authentication page. Once access and refresh tokens are issued, attackers may retain access to email, documents, and cloud resources, creating a direct path to data exposure, financial fraud, operational disruption, and costly incident response.Kali365 is a device code phishing kit built to abuse legitimate Microsoft authentication. ANY.RUN telemetry records more than 80 public sessions linked to the campaign each week, with the United States emerging as its main geographic target.
One of these sandbox sessions shows a SharePoint-themed lure used to draw the victim into the authentication flow.Based on the research, the attack unfolds in three main stages:
Lure: The victim is presented with a page impersonating a trusted business service such as SharePoint, OneDrive, or DocuSign.
Microsoft authentication: The page redirects the victim to Microsoft's legitimate device login portal and asks them to enter an attacker-provided code.
OAuth access: Once the victim completes authentication, attackers may obtain access and refresh tokens that provide continued access to Microsoft 365 email, documents, and cloud resources.

Read more ›

Other news highlights

Leaked n8n API Tokens Exposed Live Instances to Credential Theft

–

Critical Gitea Flaw Let Unauthenticated Attackers Read Server Files via Org-Mode Markup

–

New OVSwrap Linux Kernel Flaw Lets Local Users Gain Root via Open vSwitch

–

Trojanized npm Packages Employ NullReceiver Tactic to Decode C2 IP from Blockchain

Geo-Politics

News from around the world

Chinese Threat Actor Uses Leaked DarkSword Kit to Deploy GHOSTBLADE on iOS

An unknown Chinese-speaking threat actor has been observed running a campaign targeting Apple iOS devices by leveraging a publicly leaked version of the DarkSword exploit kit.

Attack surface management platform Censys said it identified the threat actor running more than 100 web properties, most of which are fake Amazon Web Services (AWS) sign-in pages on a domain that also hosts the exploit toolkit.

"The hosting concentrates in Hong Kong but reaches into Japan, the United States, and Europe," Censys researcher Aidan Holland said in an analysis published on July 31, 2026.

DarkSword, discovered and detailed earlier this year by Google Threat Intelligence Group (GTIG), iVerify, and Lookout, refers to a full-chain exploit kit that is believed to have been used by commercial surveillance vendors and suspected state-sponsored actors in disparate campaigns targeting Saudi Arabia, Turkey, Malaysia, and Ukraine since at least November 2025.

Read more ›

Other news highlights

Suspected Chinese-Speaking Hackers Target Central Asian Governments With OctLurk and SilkLurk

—

Russia blocks over 20 popular VPNs in major internet crackdown

—

Russian spies hijack hotel WiFi worldwide to infect travelers with malware, Microsoft warns

—

Polish retail giant Żabka breached via external service provider: data up for sale

Breaches

Security Breaches this week

PNLD Breach Exposes U.K. Police and Government Contact Details on Dark Web

The Police National Legal Database (PNLD) has confirmed that police, government and customer contact information was compromised and published on the dark web.
The data included names, organisations and work email addresses belonging to police officers, police staff, criminal justice professionals, government partners and customers.
The incident, identified on July 26, also exposed some names and email addresses belonging to people who had submitted questions through Ask the Police. That exposure could make phishing messages targeting named officers appear more convincing, according to UK government guidance.
PNLD said, "There is no evidence to suggest that passwords or other security credentials have been compromised." The service provides legal information, products and services to UK police forces and criminal justice organisations. It is not the Police National Computer or the Police National Database, is not a crime-recording system, and does not hold confidential information about victims, witnesses or offenders.

Read more ›

Other news highlights

Angola's Largest Telco Breached Hours Before IPO

–

Interpol Leverages Global System to Curtail Fraud Payments

–

Cyberattack Hits Liechtenstein's Register of People Behind Companies and Foundations

–

River Bank Says Hackers Deleted Data Stolen in Ransomware Attack

Vulnerabilities

Vulnerabilities & Exploits

CVE-2026-58073 - A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to impersonate a managed agent and obtain that agent's credentials.

CVSS score: 9.5

CVE-2026-58048 - Improper preservation of SQL mode when renaming databases in cPanel allows execution of SQL in root context.

CVSS score: 9.4

Last weeks recaps

CVE-2026-59309 - VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. Broadcom has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.3.

–

CVE-2026-63077 - In JetBrains TeamCity before 2026.1.3, 2025.11.7 unauthenticated remote code execution was possible via the agent polling protocol

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

Hijacked Hotel Wi-Fi Pushes Fake Updates to Deliver Surveillance Malware

A fake browser update served over hijacked hotel Wi-Fi has been used to deliver CornFlake, a remote access trojan (RAT) that can capture webcam images, microphone audio, and keystrokes, Microsoft said in its latest report.
Researchers track the operation as CaptiveCrunch and attribute it to Storm-2945. It assesses Storm-2945 to be an operational sub-cluster of Midnight Blizzard, also known as APT29 and Cozy Bear. The U.S. and U.K. governments attribute the broader actor to Russia's Foreign Intelligence Service (SVR).
On the compromised networks ReliaQuest investigated, the captive portal gateway also served as the DNS resolver assigned to connected devices. Administrative control of that gateway let the attackers forge Domain Name System (DNS) answers and redirect the resulting traffic. They could then redirect a laptop's automatic connectivity check to a fake browser or operating system update.

Read more ›

Other news highlights

HollowFrame Loader Deploys Matryoshka Backdoor in Spear-Phishing Attack on Law Firm

–

SilverFox Targets Japanese Manufacturer with 3-Driver BYOVD Chain and ValleyRAT

–

DOUBLECUP Uses ClickFix and Cached PNGs to Deliver CountLoader and DeviceManager RAT

–

Russian Hackers Exploit Microsoft OWA Flaw to Keep Mailbox Access After Credential Rotation