

# THREAT PULSE

Amateurs hack systems;  
professionals hack people  
- Bruce Schneier

THREATS  

---

NEWS  

---

PHISHING

April 2016 - VOL.2

# The News



## OTHER NEWS HIGHLIGHTS

[Docker CVE-2026-34040 Lets Attackers Bypass Authorization and Gain Host Access](#)

[Flowise AI Agent Builder Under Active CVSS 10.0 RCE Exploitation; 12,000+ Instances Exposed](#)

[How LiteLLM Turned Developer Machines Into Credential Vaults for Attackers](#)

## Anthropic's Claude Mythos Finds Thousands of Zero-Day Flaws Across Major Systems

Artificial Intelligence (AI) company Anthropic announced a new cybersecurity initiative called Project Glasswing that will use a preview version of its new frontier model, Claude Mythos, to find and address security vulnerabilities. The model will be used by a small set of organizations, including Amazon Web Services, Apple, Broadcom, Cisco, CrowdStrike, Google, JPMorgan Chase, the Linux Foundation, Microsoft, NVIDIA, and Palo Alto Networks, along with Anthropic, to secure critical software.

The company said it's forming this initiative in response to capabilities observed in its general-purpose frontier model that demonstrate a "level of coding capability where they can surpass all but the most skilled humans at finding and exploiting software vulnerabilities." Because of its cybersecurity capabilities and concerns that they could be abused, Anthropic has opted not to make the model generally available.

Mythos Preview, Anthropic claimed, has already discovered thousands of high-severity zero-day vulnerabilities in every major operating system and web browser. Some of these include a now-patched 27-year-old bug in OpenBSD, a 16-year-old flaw in FFmpeg, and a memory-corrupting vulnerability in a memory-safe virtual machine monitor.

[READ MORE >](#)

# The News

TOP OF THE NEWS THIS WEEK



## Adobe Reader Zero-Day Exploited for Months

The new Reader exploit was detected by Expmon, and an analysis showed that the identified PDF “acts as an initial exploit with the capability to collect and leak various types of information, potentially followed by remote code execution (RCE) and sandbox escape (SBX) exploits”.

The researcher believes the PDF exploits a zero-day vulnerability as the attack has been confirmed to work against the latest version of Adobe Reader. While Li has confirmed that the identified exploit collects user and other data from the compromised system, he was unable to reproduce the complete attack chain and obtain additional payloads that may be used for a sandbox escape or remote code execution.

READ MORE >

## TOP RELATED ARTICLES

[36 Malicious npm Packages Exploited Redis, PostgreSQL to Deploy Persistent Implants](#)

[Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS](#)

[Microsoft Details Cookie-Controlled PHP Web Shells Persisting via Cron on Linux Servers](#)

# Geo-Politics

NEWS FROM AROUND THE WORLD



## Iran-Linked Password-Spraying Campaign Targets 300+ Israeli Microsoft 365 Organizations

An Iran-nexus threat actor is suspected to be behind a password-spraying campaign targeting Microsoft 365 environments in Israel and the U.A.E. amid ongoing conflict in the Middle East. The activity, assessed to be ongoing, was carried out in three distinct attack waves that took place on March 3, March 13, and March 23, 2026, per Check Point.

"The campaign is primarily focused on Israel and the U.A.E., impacting more than 300 organizations in Israel and over 25 in the U.A.E.," the Israeli cybersecurity company said. "Activity associated with the same actor was also observed against a limited number of targets in Europe, the United States, the United Kingdom, and Saudi Arabia." The campaign is assessed to have targeted the cloud environments of government entities, municipalities, technology, transportation, energy sector organizations, and private-sector companies in the region.

[READ MORE >](#)

## HIGHLIGHTS FROM AROUND THE WORLD

[China-Linked Storm-1175 Exploits Zero-Days to Rapidly Deploy Medusa Ransomware](#)

[Russian State-Linked APT28 Exploits SOHO Routers in Global DNS Hijacking Campaign](#)

[Iran-Linked Hackers Disrupt U.S. Critical Infrastructure by Targeting Internet-Exposed PLCs](#)

# Breaches

SECURITY BREACHES THIS WEEK



## OTHER SECURITY BREACHES

[European Commission Confirms Data Breach Linked to Trivy Supply Chain Attack](#)

[T-Mobile Sets the Record Straight on Latest Data Breach Filing](#)

## Wynn Resorts Says 21,000 Employees Affected by ShinyHunters Hack

High-end casino and hotel operator Wynn Resorts says more than 21,000 individuals are affected by the recently disclosed data breach. Wynn Resorts confirmed in late February that hackers had obtained employee data.

The admission came after the notorious ShinyHunters cybercrime group claimed to have stolen more than 800,000 records containing personally identifiable information, including SSNs.

The hackers later removed Wynn from their leak website. This suggested that it had decided to pay a ransom, but the Las Vegas-based company declined to comment when contacted by SecurityWeek at the time.

“The threat actor has stated that all data has been deleted,” Wynn said in its notification to impacted individuals, which further reinforces the theory that a ransom has likely been paid.

The hackers had reportedly sought a ransom of more than 22 bitcoin (roughly \$1.5 million).

[300,000 People Impacted by Eurail Data Breach](#)

READ MORE >

# Vulnerabilities



Fortinet FortiClient EMS Zero-Day: CVE-2026-35616  
(Active Exploitation Underway)

CVSS SCORE 9.8

Docker CVE-2026-34040 Lets Attackers Bypass  
Authorization and Gain Host Access

CVSS SCORE 8.8

## LAST WEEKS RECAP

CVE-2026-21992 -  
Critical Vulnerability in  
Oracle Identity Manager  
and Web Services  
Manager **CVSS Score:**  
**(9.8)**

CVE-2026-3055 -  
NetScaler  
Vulnerability Poised  
for Exploitation  
**CVSS Score: (9.3)**

# Ransomware



## TOP THREAT ACTORS

### 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.

### Akira

Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to \$42 million by April 2024.

### Clon

Clon ransomware first emerged in 2019, when it became a prevalent threat to organizations and businesses. Clon ransomware encrypts the victims files and threatens to leak the confidential information if no ransom is paid.



### OVERVIEW

A total of 138 new victims were reported across various ransomware groups this Week.

### TARGET INDUSTRIES

The Manufacturing sector was the primary focus, representing 21.7% of all victims.

### TARGET COUNTRY

The USA was the top victim country, with a total of 76 affected entities.

### TOP GROUP

The Akira was the most active, claiming 28 victims.



Dive into this interactive report to uncover hidden trends [HERE!](#)

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

# Phishing

PHISHING NEWS THIS WEEK



## OTHER PHISHING ARTICLES

[Microsoft Warns of WhatsApp-Delivered VBS Malware Hijacking Windows via UAC Bypass](#)

[DPRK-Linked Hackers Use GitHub as C2 in Multi-Stage Attacks Targeting South Korea](#)

[CERT-UA Impersonation Campaign Spread AGEWHEEZE Malware to 1 Million Emails](#)

## APT28 Deploys PRISMEX Malware in Campaign Targeting Ukraine and NATO Allies

The Russian threat actor known as APT28 (aka Forest Blizzard and Pawn Storm) has been linked to a fresh spear-phishing campaign targeting Ukraine and its allies to deploy a previously undocumented malware suite codenamed PRISMEX.

"PRISMEX combines advanced steganography, component object model (COM) hijacking, and legitimate cloud service abuse for command-and-control," Trend Micro researchers Feike Hacquebord and Hiroyuki Kakara said in a technical report.

The campaign is believed to be active since at least September 2025. The activity has targeted various sectors in Ukraine, including central executive bodies, hydrometeorology, defense, and emergency services, as well as rail logistics (Poland), maritime and transportation (Romania, Slovenia, Turkey), and logistical support partners involved in ammunition initiatives (Slovakia, Czech Republic), and military and NATO partners.

READ MORE >