SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

April 2026 - VOL.4

The News

IN THE NEWS THIS WEEK

Malicious KICS Docker Images and VS Code Extensions Hit Checkmarx Supply Chain

Cybersecurity researchers have warned of malicious images pushed to the official "checkmarx/kics" Docker Hub repository.

In an alert published today, software supply chain security company Socket revealed that unknown threat actors managed to have overwritten existing tags, including v2.1.20 and alpine, while also introducing a new v2.1.21 tag that does not correspond to an official release. The Docker repository has been archived as of writing.

"Analysis of the poisoned image indicates that the bundled KICS binary was modified to include data collection and exfiltration capabilities not present in the legitimate version," Socket said.

"The malware could generate an uncensored scan report, encrypt it, and send it to an external endpoint, creating a serious risk for teams using KICS to scan infrastructure-as-code files that may contain credentials or other sensitive configuration data."

READ MORE

OTHER NEWS HIGHLIGHTS

Anthropic Won't Let You Run Mythos. But Claude Is Already in Your Salesforce.

Google Patches Antigravity IDE Flaw Enabling Prompt Injection Code Execution

SGLang CVE-2026-5760 (CVSS 9.8) Enables RCE via Malicious GGUF Model Files

The News

TOP OF THE NEWS THIS WEEK

Microsoft Patches Critical ASP.NET Core CVE-2026-40372 Privilege Escalation Bug

Microsoft has released out-of-band updates to address a security vulnerability in ASP.NET Core that could allow an attacker to escalate privileges.

The vulnerability, tracked as CVE-2026-40372, carries a CVSS score of 9.1 out of 10.0. It's rated Important in severity. An anonymous researcher has been credited with discovering and reporting the flaw.

"Improper verification of cryptographic signature in ASP.NET Core allows an unauthorized attacker to elevate privileges over a network," Microsoft said in a Tuesday advisory. "An attacker who successfully exploited this vulnerability could gain SYSTEM privileges."

READ MORE

TOP RELATED ARTICLES

Mirai Variant Nexcorium Exploits CVE-2024-3721 to Hijack TBK DVRs for DDoS Botnet

Three Microsoft Defender Zero-Days Actively Exploited; Two Still Unpatched

Google Blocks 8.3B Policy-Violating Ads in 2025, Launches Android 17 Privacy Overhaul

Geo-Politics

NEWS FROM AROUND THE WORLD

Harvester Deploys Linux GoGra Backdoor in South Asia Using Microsoft Graph API

The threat actor known as Harvester has been attributed to a new Linux version of its GoGra backdoor deployed as part of attacks likely targeting entities in South Asia.

"The malware uses the legitimate Microsoft Graph API and Outlook mailboxes as a covert command-and-control (C2) channel, allowing it to bypass traditional perimeter network defenses," the Symantec and Carbon Black Threat Hunter Team said in a report shared with The Hacker News.

The cybersecurity company said it identified artifacts uploaded to the VirusTotal platform from India and Afghanistan, suggesting that the two countries may be the target of the espionage activity.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Lotus Wiper Malware Targets Venezuelan Energy Systems in Destructive Attack

Mustang Panda's New LOTUSLITE Variant Targets India Banks, South Korea Policy Circles

Researchers Detect ZionSiphon Malware Targeting Israeli Water, Desalination OT Systems

Breaches

SECURITY BREACHES THIS WEEK

Data Breaches at Healthcare Organizations in Illinois and Texas Affect 600,000

The data breach tracker operated by the US Department of Health and Human Services (HHS) was updated this week to add three healthcare-related cybersecurity incidents impacting a significant number of people.

The biggest breach was disclosed by the North Texas Behavioral Health Authority, affecting 285,000 individuals.

The organization, which provides resources for mental health and substance abuse, revealed in March 2026 that it had detected a network intrusion in October 2025. An investigation showed that unauthorized individuals may have accessed and exfiltrated files containing personal information, including SSNs.

The second healthcare organization for which the HHS disclosed the number of affected individuals this week is Southern Illinois Dermatology, with 160,000 victims.

The Salem, Illinois-based skincare provider said in a data breach notice that it became aware of a cybersecurity incident in late November 2025. An investigation completed in early March showed that files storing personal information were compromised.

READ MORE

OTHER SECURITY BREACHES

Next.js Creator Vercel Hacked

Data Breach at Tennessee Hospital Affects 337,000

Vulnerabilities Organizations Warned of Exploited Cisco, Kentico, Zimbra Vulnerabilities

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-40372 - Improper verification of cryptographic signature in ASP.NET Core allows an unauthorized attacker to elevate privileges over a network.

CVSS SCORE 9.1

CVE-2026-34197 - Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ

CVSS SCORE 8.8

LAST WEEKS RECAP

CVE-2026-34621 - Successful exploitation of the flaw could allow an attacker to run malicious code on affected installations
CVSS Score: (8.6)

CVE-2026-34197 - is a remote code execution vulnerability in Apache ActiveMQ Classic that has been hiding in plain sight for 13 years
CVSS Score: (8.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

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

TARGET INDUSTRIES

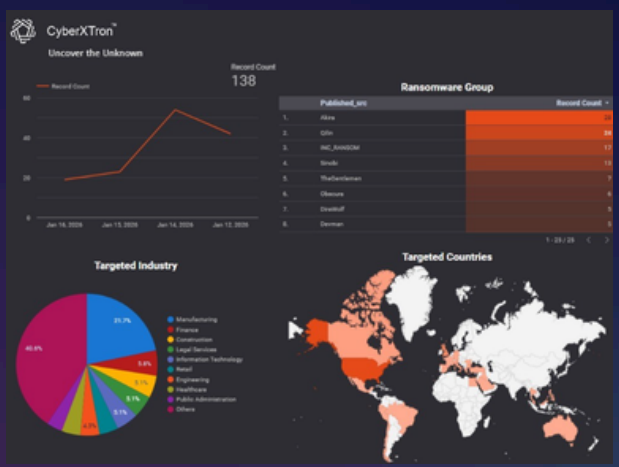
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

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

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

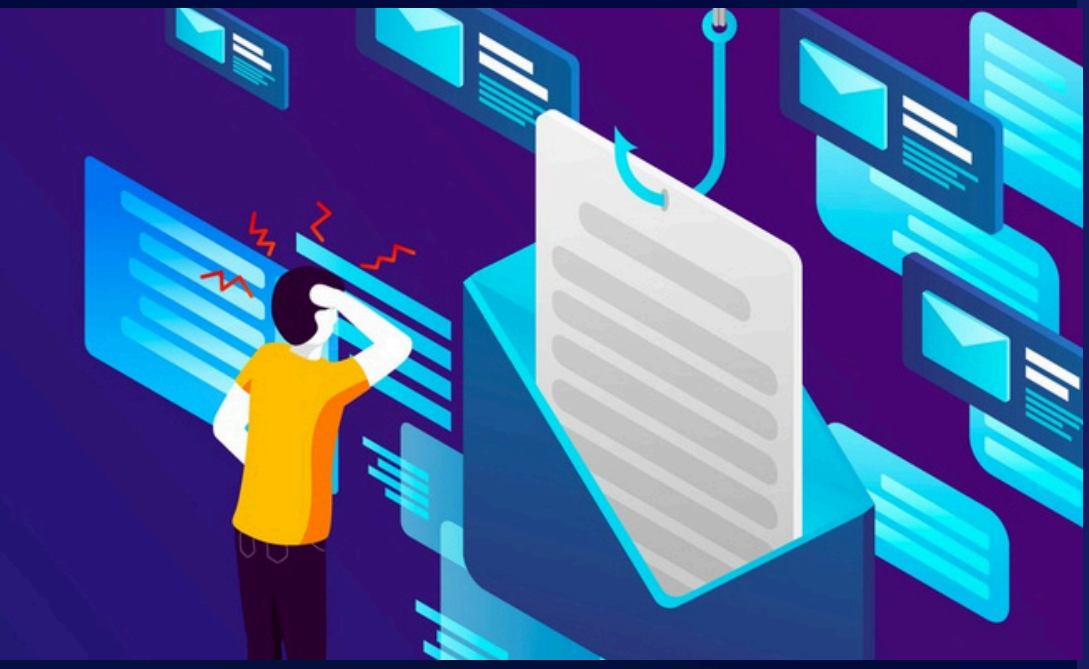
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

Clop

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

Phishing

PHISHING NEWS THIS WEEK



Apple account change alerts abused to send phishing emails

Apple account change notifications are being abused to send fake iPhone purchase phishing scams within legitimate emails sent from Apple's servers, increasing legitimacy and potentially allowing them to bypass spam filters.
A reader shared an email with BleepingComputer that appeared to be a standard Apple security notification that stated their account information had been updated.
However, embedded within the message was a phishing lure claiming that an $899 iPhone purchase had been made via PayPal, along with a phone number to call to cancel the transaction.

READ MORE

OTHER PHISHING ARTICLES

New ATHR vishing platform uses AI voice agents for automated attacks

Surge in Silent Subject Phishing Attacks Targets VIP Users

Researchers Uncover ProxySmart Software Powering 90+ SIM Farms