SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JANUARY 2025 - VOL.2

The News

IN THE NEWS THIS WEEK

Hackers use FastHTTP in new high-speed Microsoft 365 password attacks

Threat actors are utilizing the FastHTTP Go library to launch high-speed brute-force password attacks targeting Microsoft 365 accounts globally.
The campaign was recently discovered by incident response firm SpearTip, who said the attacks began on January 6, 2025, targeting the Azure Active Directory Graph API. The researchers warn that the brute-force attacks have to successful account takeovers 10% of the time.

READ MORE

WP3.XYZ malware attacks add rogue admins to 5,000+ WordPress sites

A new malware campaign has compromised more than 5,000 WordPress sites to create admin accounts, install a malicious plugin, and steal data. The malicious activity uses the wp3[.]xyz domain to exfiltrate data but have yet to determine the initial infection vector.

After compromising a target, a malicious script loaded from the wp3[.]xyz domain creates the rogue admin account wpx_admin with credentials available in the code. The script then proceeds to install a malicious plugin (plugin.php) downloaded from the same domain, and activates it on the compromised website.

READ MORE

OTHER NEWS HIGHLIGHTS

Hackers Hide Malware in Images to Deploy VIP Keylogger and 0bj3ctivity Stealer

Python-Based Malware Powers RansomHub Ransomware to Exploit Network Flaws

Fake CrowdStrike job offer emails target devs with crypto miners

FTC cracks down on GoDaddy for cybersecurity failings

Microsoft January 2025 Patch Tuesday fixes 8 zero-days, 159 flaws

The News

TOP OF THE NEWS THIS WEEK

Google OAuth Vulnerability Exposes Millions via Failed Startup Domains

New security and privacy analysis has revealed how hackers are manipulating Google's search protections to expose hundreds of millions more users to malicious and potentially dangerous extensions

The issue is relatively straightforward: when purchasing a failed startup's domain, anyone can re-create old employee e-mail accounts and use them to access the different SaaS products the startup used.

While re-creating an old employee e-mail account does not provide access to the data stored by Google, it could grant access to data stored on services such as Slack, Zoom, ChatGPT, and others, on HR systems and interview platforms, and to direct messages on chat platforms.

Purchasing such a domain and accessing these services could expose sensitive personal information, internal information, and other sensitive data,

The underlying problem is if a service (e.g., Slack) relies solely on these two claims, ownership changes to the domain won't look any different to Slack. When someone buys the domain of a defunct company, they inherit the same claims, granting them access to old employee accounts.

READ MORE

TOP RELATED ARTICLES

Millions Of Sign-In-With-Google Users Warned Of Data-Theft Vulnerability

Google OAuth Flaw Leads to Account Takeover When Domain Ownership Changes

Millions of Accounts Vulnerable due to Google's OAuth Flaw

Are millions of accounts vulnerable due to Google's OAuth Flaw?

Geo-Politics

NEWS FROM AROUND THE WORLD

North Korean IT Worker Fraud Linked to 2016 Crowdfunding Scam and Fake Domains

A new link has been identified between infrastructure and North Korean threat actors behind a fraudulent IT worker schemes and a 2016 crowdfunding scam.

The IT worker fraud scheme, which came to light in late 2023, involves North Korean actors infiltrating companies in the West and other parts of the world by surreptitiously seeking employment under fake identities to generate revenue for the sanctions-hit nation. It's also tracked under the names Famous Chollima, Nickel Tapestry, UNC5267, and Wagemole.

READ MORE

Russian espionage and financial theft campaigns have ramped up, Ukraine cyber agency says

Most of the cyberattacks targeting Ukraine over the past year were for espionage, financial theft, or to inflict psychological damage, researchers at Ukraine's State Service for Special Communications and Information Protection found. The majority of these campaigns were attributed to three Russia-linked hacker groups, tracked as UAC-0010, UAC-0006, and UAC-0050.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

US, Japan and S. Korea urge crypto industry to take action against North Korean hackers

DOJ deletes China-linked PlugX malware off more than 4,200 US computers

No new funding in EU plan to tackle ransomware attacks against hospitals

China's Salt Typhoon spies spotted on US govt networks before telcos, CISA boss says

Breaches

SECURITY BREACHES THIS WEEK

Hackers leak configs and VPN credentials for 15,000 FortiGate devices

A new hacking group has leaked the configuration files, IP addresses, and VPN credentials for over 15,000 FortiGate devices for free on the dark web, exposing a great deal of sensitive technical information to other cybercriminals.

The data was leaked by the "Belsen Group," a new hacking group first appearing on social media and cybercrime forums this month. To promote themselves, the Belsen Group has created a Tor website where they released the FortiGate data dump for free to be used by other threat actors.

READ MORE

Telefonica Breach Exposes Jira Tickets, Customer Data

Four threat actors posted an exfiltrated Jira database on the BreachForums Dark Web hacking community last week, claiming that it contains nearly 470,000 lines of internal ticketing data and more than 5,000 PDFs, Word documents, PowerPoints, and other documents. Three of the four threat actors in question are believed to be a part of the Hellcat ransomware group.

READ MORE

OTHER SECURITY BREACHES

University of Oklahoma isolates systems after 'unusual activity' on IT network

OneBlood confirms personal data stolen in July ransomware attack

UK domain registry Nominet confirms breach via Ivanti zero-day

Fitness App Leads To Massive Security Breach On French Nuclear Submarines

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-55591 - Fortinet Authentication Bypass in Node.js Websocket Module Vulnerability

CVSS SCORE 9.6

CVE-2025-21298 - Windows OLE Remote Code Execution Vulnerability

CVSS SCORE 9.8

CVE-2025-21307 - Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability

CVSS SCORE 9.8

CVE-2025-21311 - Windows NTLM V1 Elevation of Privilege Vulnerability

CVSS SCORE 9.8

CVE-2025-21333, CVE-2025-21334, CVE-2025-21335 - Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability

CVSS SCORE 7.8

LAST WEEKS RECAP

CVE-2025-0282 - Ivanti Connect Secure, PolicySecure & ZTA Gateways Stack Overflow Vulnerability (CVSS 9.0)

CVE-2025-0291 - Type Confusion in V8 in GoogleChrome (CVSS 8.0)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

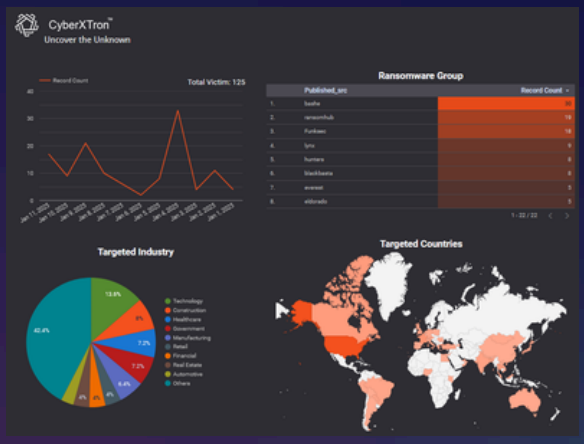
A total of 125 victims in the last week, top 3 groups are Bashe (30 Incidents), Ransomhub (19 Incidents) and Funsek (18 Incidents).

TARGET INDUSTRIES

Last Week saw the most ransomware attacks against the Technology industry as the highest hit.

TARGET COUNTRY

Only 3 Incidents targeted the United Kingdom with the majority of the incidents affecting the United States.



Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

TOP THREAT ACTORS

LockBit

LockBit is a ransomware-as- a-service (RaaS) group that has been active since September 2019. LockBit has developed several variants of ransomware products to perform encryption

RansomHub

RansomHub, a new Ransomware-as-a-Service (RaaS) that has rapidly become one of the largest ransomware groups currently operating, is very likely an updated and rebranded version of the older Knight ransomware.

BlackBasta

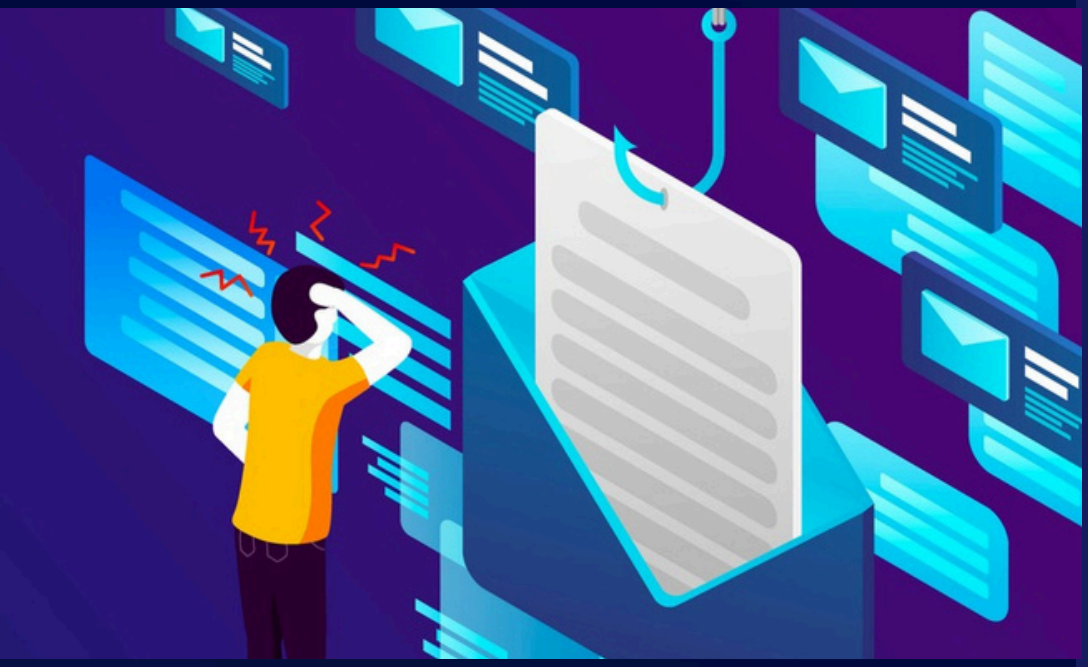
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

Play

The group focuses on multi- extortion in that they encrypt target organizations' data, but also threaten to post the data to their public TOR-based sites.

Phishing

PHISHING NEWS THIS WEEK



Google Ads Users Targeted in Malvertising Scam Stealing Credentials and 2FA Codes

A new malvertising campaign is targeting individuals and businesses advertising via Google Ads by attempting to phish for their credentials via fraudulent ads on Google.

The campaign consists of stealing as many advertiser accounts as possible by impersonating Google Ads and redirecting victims to fake login pages.

It's suspected the end goal of the campaign is to reuse the stolen credentials to further perpetuate the campaigns, while also selling them to other criminal actors on underground forums.

The newly identified campaign specifically singles out users who search for Google Ads on Google's own search engine to serve bogus ads for Google Ads that, when clicked, redirect users to fraudulent sites hosted on Google Sites.

These sites then serve as landing pages to lead the visitors to external phishing sites that are designed to capture their credentials and two-factor authentication (2FA) codes via a WebSocket and exfiltrated to a remote server under the attacker's control.

READ MORE

OTHER PHISHING ARTICLES

AI Alone is Not Bulletproof: Weaknesses in AI/ML Email Security

Hackers Spoof Social Security Administration to Deliver ScreenConnect Remote Access Tool

Phishing texts trick Apple iMessage users into disabling protection

Phishing Campaign Abuses Legitimate Services to Send PayPal Requests