SCC DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JANUARY 2025 - VOL.3

The News

IN THE NEWS THIS WEEK

Microsoft: Exchange 2016 and 2019 reach end of support in October

Microsoft has reminded admins that Exchange 2016 and Exchange 2019 will reach the end of extended support in October and shared guidance for those who need to decommission outdated servers. Exchange 2016 reached its mainstream end date in October 2020, while Exchange 2019 reached the end of mainstream support on January 9, 2024.

READ MORE

Tycoon 2FA Phishing Kit Upgraded to Bypass Security Measures

A new version of the phishing kit Tycoon 2FA, which uses advanced tactics to bypass multi factor authentication (MFA) and evade detection, has been analyzed by threat researchers at Barracuda. Tycoon 2FA, which first emerged in August 2023, has undergone several updates to enhance its capabilities. The latest version, observed in November 2024, targets Microsoft 365 session cookies to bypass 2FA protections. The creators of the phishing kit have since incorporated several measures to prevent detection by automated tools and security analysts.

READ MORE

OTHER NEWS HIGHLIGHTS

Unsecured Tunneling Protocols Expose 4.2 Million Hosts, Including VPNs and Routers

Cloudflare mitigated a record-breaking 5.6 Tbps DDoS attack

Fake Homebrew Google ads target Mac users with malware

Cisco Fixes Critical Privilege Escalation Flaw in Meeting Management (CVSS 9.9)

Hackers exploit 16 zero-days on first day of Pwn2Own Automotive 2025

The News

TOP OF THE NEWS THIS WEEK

Ransomware Groups Abuse Microsoft Services for Initial Access

Two separate threat actors have been observed abusing Microsoft 365 services and exploiting default Microsoft Teams configurations to initiate conversations with internal users, Sophos warns.

Operating Microsoft 365 tenants, the two hacking groups launched at least 15 attacks over the past three months, likely aiming to compromise organizations for ransomware deployment and data theft.

Tracked as STAC5143 and STAC5777, the attackers leveraged a default Microsoft Teams configuration that allowed them to initiate chats and meetings with internal users, posing as tech support and taking control of the target's machine using legitimate Microsoft tools.

The first STAC5143 attack was observed in November 2024 and it started with a large volume of spam messages that was immediately followed by a Teams call from the attackers, from an account named 'Help Desk Manager'. During the call, the attackers requested remote screen control through Teams, which allowed them to open a command shell, drop files on the system, and execute malware.

READ MORE >

TOP RELATED ARTICLES

Ransomware gangs pose as IT support in Microsoft Teams phishing attacks

Email Bombing, 'Vishing' Tactics Abound in Microsoft 365 Attacks

Microsoft Teams vishing attacks trick employees into handing over remote access

Russian ransomware hackers increasingly posing as tech support on Microsoft Teams

Geo-Politics

NEWS FROM AROUND THE WORLD

CERT-UA Warns of Cyber Scams Using Fake AnyDesk Requests for Fraudulent Security Audits

The Computer Emergency Response Team of Ukraine (CERT-UA) is warning of ongoing attempts by unknown threat actors to impersonate the cybersecurity agency by sending AnyDesk connection requests. The AnyDesk requests claim to be for conducting an audit to assess the "level of security," CERT-UA added, cautioning organizations to be on the lookout for such social engineering attempts that seek to exploit user trust.

READ MORE

Iran and Russia deepen cyber ties with new agreement

A deal signed last week between Iran and Russia includes commitments to deepen the countries' military, security and technological ties. The agreement between the world's two most sanctioned nations aims to elevate "friendly interstate relations between the countries to a new level," according to a statement from the Kremlin. Parts of the agreement specifically address cooperation in cybersecurity and internet regulation.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

PlushDaemon APT Targets South Korean VPN Provider in Supply Chain Attack

Trump Pardons Founder of Silk Road Website

Mandatory MFA, Biometrics Make Headway in Middle East, Africa

DONOT Group Deploys Malicious Android Apps in India

Breaches

SECURITY BREACHES THIS WEEK

HPE investigates breach as hacker claims to steal source code

Hewlett Packard Enterprise (HPE) is investigating claims of a new breach after a threat actor said they stole documents from the company's developer environments. The company has told BleepingComputer that it hasn't found any evidence of a security breach, but it is investigating the threat actor's claims. "HPE became aware on January 16 of claims being made by a group called IntelBroker that it was in possession of information belonging to HPE," spokesperson Clare Loxley told BleepingComputer.

READ MORE >

Major Cybersecurity Vendors' Credentials Found on Dark Web

Thousands of account credentials belonging to major cybersecurity vendors on the dark web have been discovered by threat intelligence firm Cyble.
In a January 22 report where Cyble researchers shared their findings, they said they found credentials for at least 14 security providers. The credentials have been leaked since the start of the year 2025. They were likely pulled from infostealer logs and then sold on cybercrime marketplaces in bulk for as little as $10.

READ MORE >

OTHER SECURITY BREACHES

Russian telecom giant Rostelecom investigates suspected cyberattack on contractor

Government IT contractor Conduent says 'third-party compromise' caused outages

PowerSchool hacker claims they stole data of 62 million students

Data on Half a Million Hotel Guests Exposed After Otelier Breach

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2025-0411 - 7-Zip Mark-of-the-Web Bypass Vulnerability

CVSS SCORE 7.0

LAST WEEKS RECAP

CVE-2024-55591 - Fortinet Authentication Bypass in Node.js Websocket Module Vulnerability (CVSS 9.6)

CVE-2025-21298 - Windows OLE Remote Code Execution Vulnerability (CVSS 9.8)

CVE-2025-21307 - Windows Reliable Multicast Transport Driver (RMCAST) Remote Code Execution Vulnerability (CVSS 9.8)

CVE-2025-21311 - Windows NTLM V1 Elevation of Privilege Vulnerability (CVSS 9.8)

CVE-2025-21333, CVE-2025-21334, CVE-2025-21335 - Windows Hyper-V NT Kernel Integration VSP Elevation of Privilege Vulnerability (CVSS 7.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

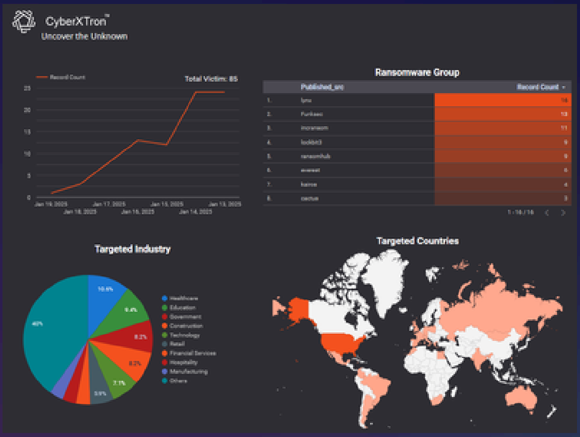
A total of 85 victims in the last week. Top 3 groups are ‘lynx’ (16 Incidents), Funksec (13 Incidents) and incransom (11 Incidents).

TARGET INDUSTRIES

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

TARGET COUNTRY

Only 4 Incidents targeted the United Kingdom with the majority of the incidents affecting the United States.



Ransomware Group

	Published_src	Record Count ▾
1.	lynx	16
2.	Funksec	13
3.	incransom	11
4.	lockbit3	9
5.	ransomhub	9
6.	everest	6
7.	kairos	4
8.	cactus	3

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

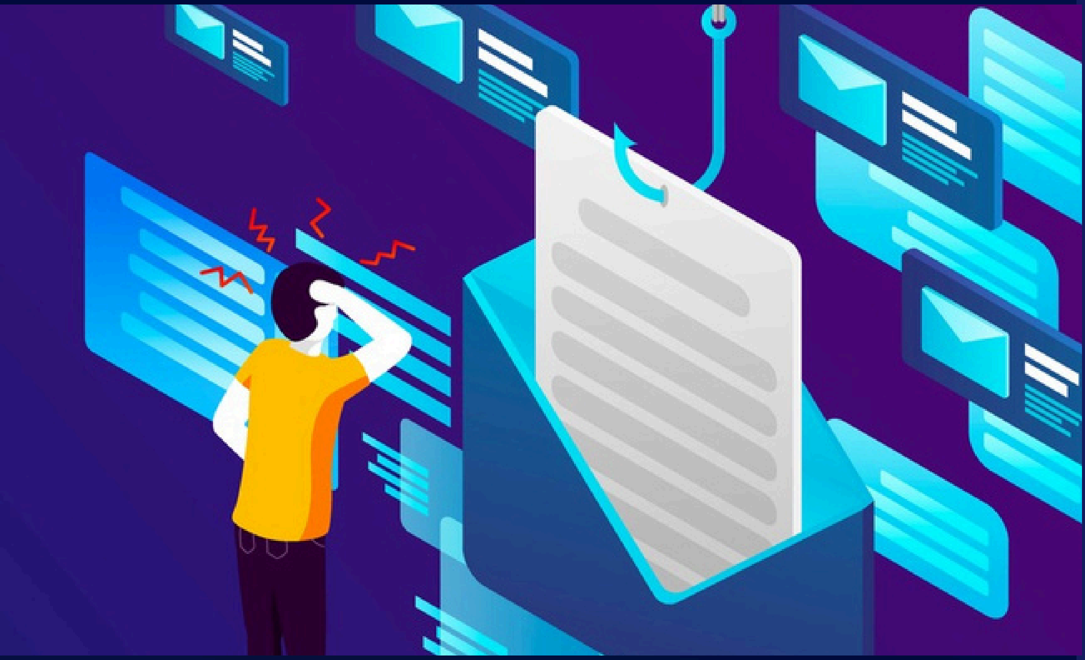
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

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



Phishing Risks Rise as Zendesk Subdomains Facilitate Attacks

A new report by security researchers has revealed how Zendesk's platform can be exploited to facilitate phishing attacks and investment scams, such as romance baiting schemes.

The findings emphasize social engineering vulnerabilities that could allow malicious actors to impersonate trusted companies and put users at risk of data theft and financial loss.

CloudSEK's analysis, published on January 20, shows that Zendesk's system, which allows users to register free subdomains during trial sign-ups, can be manipulated to create URLs resembling legitimate companies. Attackers can then use these subdomains to deliver phishing emails disguised as customer support tickets or other legitimate interactions.

The security firm said that since 2023, it had identified 1912 instances of Zendesk subdomains matching client keywords.

The report highlights that while many instances serve legitimate purposes, some are being registered for malicious activities, including impersonation and scams. Common tactics include using keywords tied to the target brand along with numeric strings to appear authentic.

READ MORE

OTHER PHISHING ARTICLES

Account Compromise and Phishing Top Healthcare Security Incidents

FBI Warns Gmail, Apple Mail, Outlook Users—Emailing These 2 Words Is Dangerous

Threat Actors Abuse Google Translate to Craft Phishing Links

Malvertising Campaign Abuses Google Ads to Target Advertisers