SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

OCTOBER 2024 - VOL.2

The News

IN THE NEWS THIS WEEK

N. Korean Hackers Use Fake Interviews to Infect Developers with Cross-Platform Malware

Threat actors with ties to North Korea have been observed targeting job seekers in the tech industry to deliver updated versions of known malware families tracked as BeaverTail and InvisibleFerret. The activity cluster, tracked as CL-STA-0240, is part of a campaign dubbed Contagious Interview that Palo Alto Networks Unit 42 first disclosed in November 2023. "The threat actor behind CL-STA-0240 contacts software developers through job search platforms by posing as a prospective employer," Unit 42 said in a new report.

READ MORE

Critical Mozilla Firefox Zero-Day Allows Code Execution

Mozilla has patched a critical security vulnerability in its Firefox Web browser that's being actively exploited in the wild. Tracked as CVE-2024-9680, the vulnerability is a use-after-free issue in Animation timelines, with attackers exploiting it to execute arbitrary code, according to Mozilla's advisory. It carries a CVSSv3 vulnerability-severity rating of 9.8 out of 10 and a low attack complexity (no privileges or user interaction is needed to successfully exploit the flaw), and translates into high risk in the event of a successful attack.

READ MORE

OTHER NEWS HIGHLIGHTS

Gamers Tricked Into Downloading Lua-Based Malware via Fake Cheating Script Engines

Single HTTP Request Can Exploit 6M WordPress Sites

Crypto Hacker Pleads Guilty for Stealing Over $37 Million in Cryptocurrency

Microsoft October 2024 Patch Tuesday fixes 5 zero-days, 118 flaws

Marriott Agrees to Pay $52 million, Beef up Data Security to Resolve Probes Over Data Breaches

The News

TOP OF THE NEWS THIS WEEK

Microsoft Detects Growing Use of File Hosting Services in Business Email Compromise Attacks

Microsoft is warning of cyber attack campaigns that abuse legitimate file hosting services such as SharePoint, OneDrive, and Dropbox that are widely used in enterprise environments as a defense evasion tactic.

The end goal of the campaigns are broad and varied, allowing threat actors to compromise identities and devices and conduct business email compromise (BEC) attacks, which ultimately result in financial fraud, data exfiltration, and lateral movement to other endpoints.

The weaponization of legitimate internet services (LIS) is an increasingly popular risk vector adopted by adversaries to blend in with legitimate network traffic in a manner such that it often bypasses traditional security defenses and complicates attribution efforts.

READ MORE

TOP RELATED ARTICLES

File hosting services misused for identity phishing

Microsoft Sees Increase in Use of Legitimate File Hosting Services in Business Email Compromise Attacks

Microsoft warns top file hosting services hijacked for email scams

SharePoint, OneDrive and Dropbox targeted by BEC attacks

Geo-Politics

NEWS FROM AROUND THE WORLD

Pro-Ukrainian Hackers Strike Russian State TV on Putin's Birthday

Ukraine has claimed responsibility for a cyber attack that targeted Russia state media company VGTRK and disrupted its operations, according to reports from Bloomberg and Reuters.

The incident took place on the night of October 7, VGTRK confirmed, describing it as an "unprecedented hacker attack." However, it said "no significant damage" was caused and that everything was working normally despite attempts to interrupt radio and TV broadcasts.

READ MORE

China's Salt Typhoon Hacks AT&T and Verizon, Accessing Wiretap Data: Report

A sophisticated hacking group known as Salt Typhoon believed to be linked to China, has breached the systems of major U.S. telecom companies AT&T, Verizon, and Lumen Technologies, potentially compromising sensitive government data. This was reported by the Wall Street Journal raising significant national security concerns, as the attackers may have accessed systems used to handle court-authorized wiretapping—critical tools in tracking criminal and national security activities.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Google Blocks Unsafe Android App Sideloading in India for Improved Fraud Protection

Mideast, Turkey Cyber Threats Spike, Prompting Defense Changes

Southeast Asian cyber-fraud industry 'outpacing' law enforcement with new tools: UN

US Warns of Foreign Interference in Congressional Races Ahead of Election

Breaches

SECURITY BREACHES THIS WEEK

DumpForums Claim 10TB Data Breach at Russian Cybersecurity Firm Dr.Web

Pro-Ukrainian hacktivists from DumpForums claim to have breached Russian cybersecurity giant Dr.Web, stealing over 10 TB of sensitive data, including internal projects, client databases, and critical infrastructure access.

Additionally, the hackers claimed to have hacked and extracted data from Dr.Web's corporate GitLab server, where internal developments and projects were stored, including the corporate email server, Confluence, Redmine, Jenkins, Mantis, and RocketChat.

READ MORE

Internet Archive hacked, data breach impacts 31 million users

Internet Archive's "The Wayback Machine" has suffered a data breach after a threat actor compromised the website and stole a user authentication database containing 31 million unique records. News of the breach began circulating Wednesday afternoon after visitors to archive.org began seeing a JavaScript alert created by the hacker, stating that the Internet Archive was breached.

READ MORE

OTHER SECURITY BREACHES

ADT says hacker stole encrypted internal employee data after compromising business partner

LEGO's website hacked to push cryptocurrency scam

American Water Suffers Network Disruptions After Cyberattack

238,000 Comcast Customers Hit by FBCS Ransomware Attack

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-9680 - Mozilla Firefox Use-after-free in Animation timeline

CVSS SCORE 9.8

CVE-2024-43572 - Microsoft Management Console Remote Code Execution Vulnerability

CVSS SCORE 7.8

CVE-2024-43583 - Winlogon Elevation of Privilege Vulnerability

CVSS SCORE 7.8

CVE-2024-6197 - Open Source Curl Remote Code Execution Vulnerability Threat Assessment

CVSS SCORE 8.8

LAST WEEKS RECAP

CVE-2024-7024 - Chrome, Improper Restriction of Operations within the Bounds of a Memory Buffer
CVSS Score: (9.3)

CVE-2024-6592 - WatchGuard Firebox Single Sign-On Agent Protocol Authorization Bypass
CVSS Score: (9.1)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

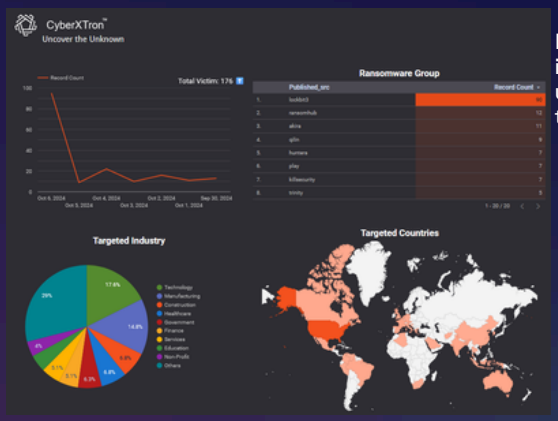
Last week we see Lockbit3 claim the most ransomware victims with 90 out of 176 (51%)

TARGET INDUSTRIES

Last week saw the most ransomware attacks against the Technology and Manufacturing industries.

TARGET COUNTRY

The United States has consistently held the top position as the primary target.



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

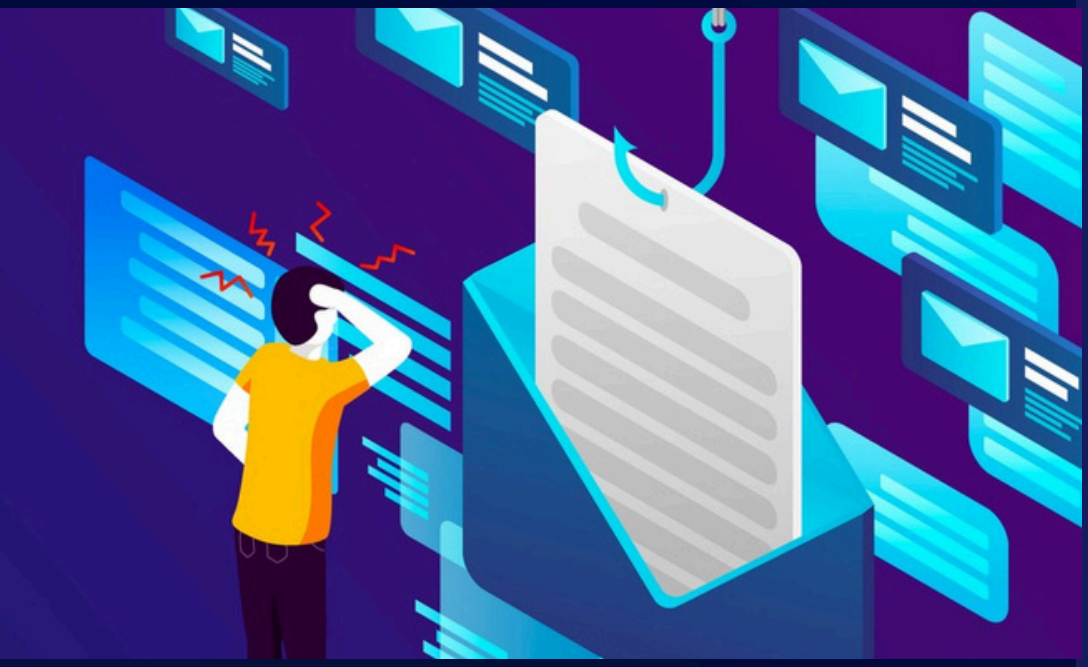
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

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



New Mamba 2FA bypass service targets Microsoft 365 accounts

An emerging phishing-as-a-service (PhaaS) platform called Mamba 2FA has been observed targeting Microsoft 365 accounts in AiTM attacks using well-crafted login pages.

Additionally, Mamba 2FA offers threat actors an adversary-in-the-middle (AiTM) mechanism to capture the victim's authentication tokens and bypass multi-factor authentication (MFA) protections on their accounts.

Mamba 2FA is currently sold to cybercriminals for $250/month, which is a competitive price that positions it among the most alluring and fastest-growing phishing platforms in the space.

Mamba 2FA was first documented by Any.Run analysts in late June 2024, but Sekoia reports that it has been tracking activity linked to the phishing platform since May 2024. Additional evidence shows that Mamba 2FA has been supporting phishing campaigns since November 2023, with the kit being sold on ICQ and later on Telegram.

Following Any.Run's report of a campaign backed by Mamba 2FA, the operators of the phishing kit made several changes to their infrastructure and methods to increase the stealthiness and longevity of the phishing campaigns.

READ MORE

OTHER PHISHING ARTICLES

Mounting Phishing Attacks Enabled by AI, Deepfakes

Free Phishing Platform Has Created More than 140,000 Spoofed Websites

Storm-1575 Threat Actor Deploys New Login Panels for Phishing Infrastructure

Multistep phishing attack aims to collect login credentials and personal info