SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

SEPTEMBER 2024 - VOL.3

The News

IN THE NEWS THIS WEEK

AT&T pays $13 million FCC settlement over 2023 data breach

The Federal Communications Commission (FCC) has reached a $13 million settlement with AT&T to resolve a probe into whether the telecom giant failed to protect customer data after a vendor's cloud environment was breached three years ago.
The FCC's investigation also examined AT&T's supply chain integrity and whether the telecom giant engaged in poor privacy and cybersecurity practices.

READ MORE

North Korean Hackers Target Cryptocurrency Users on LinkedIn with RustDoor Malware

Cybersecurity researchers are continuing to warn about North Korean threat actors' attempts to target prospective victims on LinkedIn to deliver malware called RustDoor.
The latest advisory comes from Jamf Threat Labs, which said it spotted an attack attempt in which a user was contacted on the professional social network by claiming to be a recruiter for a legitimate decentralized cryptocurrency exchange (DEX) called STON.fi.

READ MORE

OTHER NEWS HIGHLIGHTS

DOJ charges hackers for stealing $230 million in crypto from individual

Federal civil rights watchdog sounds alarm over DOJ, DHS and HUD use of facial recognition technology

Microsoft Edge will flag extensions causing performance issues

FTC exposes massive surveillance of kids, teens by social media giants

Police dismantles phone unlocking ring linked to 483,000 victims

The News

TOP OF THE NEWS THIS WEEK

CISA warns of Windows flaw used in infostealer malware attacks

CISA has ordered US federal agencies to secure their systems against a recently patched windows MSHTML spoofing zero -day bug exploited by the Void Banshee APT hacking group

The vulnerability (CVE-2024-43461) was disclosed during patch Tuesday this month where it was orginally thought this wasn't being exploited in the wild, however on friday microsoft confirmed this was not true and it was being exploited.

It is said that Void Banshee hackers exploited it in zero day attacks to install information stealing malware, by tricking the targets into visiting maliciously creafted webpage or opening a malicious file.

"We released a fix for CVE-2024-38112 in our July 2024 security updates which broke this attack chain," it said. "Customers should both the July 2024 and September 2024 security update to fully protect themselves."

READ MORE

TOP RELATED ARTICLES

Recently patched Windows flaw CVE-2024-43461 was actively exploited as a zero-day before July 2024

Microsoft confirms second 0-day exploited by Void Banshee APT (CVE-2024-43461)

CVE-2024-43461 Detail

Microsoft re-categorizes fixed Trident bug as zero day

Geo-Politics

NEWS FROM AROUND THE WORLD

Phishing Espionage Attack Targets US-Taiwan Defense Conference

A meeting of influential figures in and around the US and Taiwanese defense industries has been targeted by a phishing attack carrying fileless malware. The 23rd US-Taiwan Defense Industry Conference will be held next week in Philadelphia's Logan Square neighborhood. Closed to the press, it will feature speakers from government, defense, academia, and commercial sectors in the US and Taiwan. The focus, according to its website, will be "addressing the future of US defense cooperation with Taiwan, the defense procurement process, and Taiwan's defense and national security needs."

READ MORE

Germany seizes leak site of 'Vanir' ransomware operation

German law enforcement has taken down some of the infrastructure used by a ransomware group deploying a new strain of malware in a small number of attacks.
Officials in the city of Karlsruhe and state of Baden-Württemberg said they took over the leak site used by hackers deploying the Vanir Locker ransomware.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

New Brazilian-Linked SambaSpy Malware Targets Italian Users via Phishing Emails

Microsoft Warns of New INC Ransomware Targeting U.S. Healthcare Sector

New "Raptor Train" IoT Botnet Compromises Over 200,000 Devices Worldwide

Chinese Engineer Charged in U.S. for Years-Long Cyber Espionage Targeting NASA and Military

Breaches

SECURITY BREACHES THIS WEEK

Over 1,000 ServiceNow instances found leaking corporate KB data

Over 1,000 misconfigured ServiceNow enterprise instances were found exposing Knowledge Base (KB) articles that contained sensitive corporate information to external users and potential threat actors.
The exposed information includes personally identifiable information (PII), internal system details, user credentials, access tokens for live production systems, and other essential information depending on the Knowledge Base topic.

READ MORE

Data on nearly 1 million NHS patients leaked online following ransomware attack on London hospitals

People with symptoms of sensitive medical conditions, including cancer and sexually transmitted infections, are among almost a million individuals who had their personal information published online following a ransomware attack that disrupted NHS hospitals in London earlier this year, according to an analysis shared with Recorded Future News.

READ MORE

OTHER SECURITY BREACHES

New Android Malware Ajina.Banker Steals 2FA Codes, Spreads via Telegram

Ivanti warns of another critical CSA flaw exploited in attacks

Binance Warns of Rising Clipper Malware Attacks Targeting Cryptocurrency Users

Hackers Exploit Default Credentials in FOUNDATION Software to Breach Construction Firms

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-38812 - Critical RCE Vulnerability Fixed in VMware vCenter Server and Cloud Foundation

CVSS SCORE 9.8

CVE-2024-38112 - Windows MSHTML Platform Spoofing Vulnerability

CVSS SCORE 7.5

LAST WEEKS RECAP

CVE-2024-29847 - Ivanti EPM deserialization of untrusted data vulnerability
CVSS Score: (10.0)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

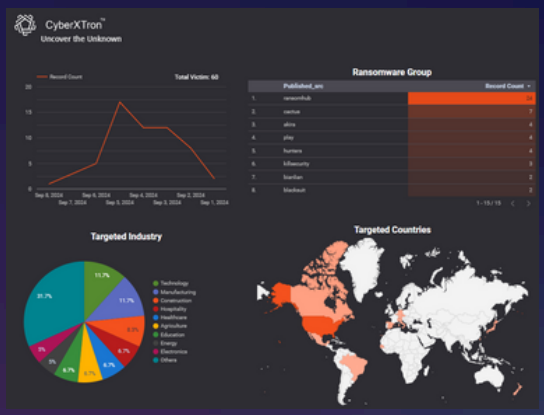
Last week we seen a continuous trend where RansomHub took the top spot with a total of 15 victims out of 75

TARGET INDUSTRIES

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

TARGET COUNTRY

The United States has consistently held the top position as the primary target. With 49 of the 75 attacks.



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

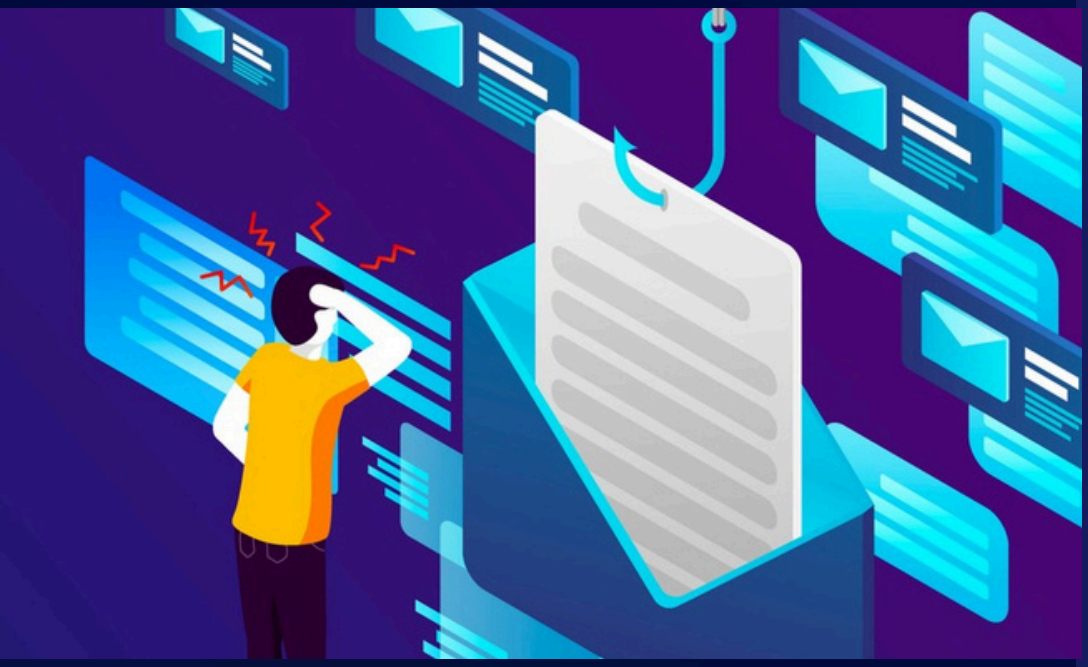
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

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



17 arrested in takedown targeting phishing service with nearly 500,000 victims

Europol on Thursday said authorities disrupted an international phishing campaign that ensnared 483,000 victims, mainly from Spanish-speaking countries.

Law enforcement in Spain, Argentina, Chile, Colombia, Ecuador and Peru last week conducted 17 arrests and seized more than 900 items, including phones, electronic devices, cars and weapons. The administrator of the phishing platform, an Argentinian national who had operated it for the last five years, is in custody, Europol said.

The phishing-as-a-service platform known as iServer had more than 2,000 users, who provided phone unlocking services to other criminals in possession of stolen phones.

According to cybersecurity company Group-IB, which originally tipped off Europol to the operation in 2022, iServer was primarily used by Spanish-speaking criminals in North and South America, but also expanded into Europe and other areas because it helped low-skilled cybercriminals harvest credentials to unlock phones.

READ MORE

OTHER PHISHING ARTICLES

U.S. Government Indicts Chinese National For Alleged Spear Phishing Attacks

North Korean Hackers Target Software Developers With Phony Coding Tests

SANS Releases Guide to Address Rise in Attacks on Manufacturing and Industrial Control Systems

BEC Scams Have Caused $55 Billion in Losses Over the Past Ten Years