SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

OCTOBER 2024 - VOL.3

The News

IN THE NEWS THIS WEEK

U.S. Charges Two Sudanese Brothers for Record 35,000 DDoS Attacks

Federal prosecutors in the U.S. have charged two Sudanese brothers with running a distributed denial-of-service (DDoS) botnet for hire that conducted a record 35,000 DDoS attacks in a single year, including those that targeted Microsoft's services in June 2023.

The attacks, which were facilitated by Anonymous Sudan's "powerful DDoS tool," singled out critical infrastructure, corporate networks, and government agencies in the United States and around the world, the U.S. Department of Justice (DoJ) said.

READ MORE

Undercover North Korean IT workers now steal data, extort employers

North Korean IT professionals who trick Western companies into hiring them are stealing data from the organization's network and asking for a ransom to not leak it.

Dispatching IT workers to seek employment at companies in wealthier nations is a tactic that North Korea has been using for years as a means to obtain privileged access for cyberattacks or to generate revenue for the country's weapons programs.

READ MORE

OTHER NEWS HIGHLIGHTS

ClickFix Attack: Fake Google Meet Alerts Install Malware on Windows, macOS

More than 5,000 arrested, thousands of websites disrupted in crackdown on illegal gambling during Euro tournament

Insurance giant Globe Life facing extortion attempts after data theft from subsidiary

TrickMo malware steals Android PINs using fake lock screen

China Accuses U.S. of Fabricating Volt Typhoon to Hide Its Own Hacking Campaigns

The News

TOP OF THE NEWS THIS WEEK

Cisco investigates breach after stolen data for sale on hacking forum

Cisco has confirmed to Bleepingcomputer that it is investigating recent claims that it suffered a breach after a threat actor began selling allegedly stolen data on a hacking form.

There are reports that an actor is alleging to have gained access to certain Cisco related files.

This has come from a well-known threat actor “IntelBroker” said that he and two others called “energyweaponuser” and “zjj” breached cisco on June 10, 2024, and stole a large amount of developer data from the company.

Compromised data includes: Github projects, Gitlab Projects, SonarQube projects, Source code, hard coded credentials, Certificates, Customer SRCs, Cisco Confidential Documents, Jira tickets, API tokens, AWS Private buckets, Cisco Technology SRCs, Docker Builds, Azure Storage buckets, Private & Public keys, SSL Certificates, Cisco Premium Products & More!

READ MORE

TOP RELATED ARTICLES

Cisco confirms 'ongoing investigation' after crims brag about selling tons of data

Alleged Cisco data breach could affect Microsoft, Barclays, and SAP developer data

Data sale on the darknet: Cisco investigates possible cyberattack

Cisco investigates possible data breach after IntelBroker attack

Geo-Politics

NEWS FROM AROUND THE WORLD

SideWinder APT Strikes Middle East and Africa With Stealthy Multi-Stage Attack

An advanced persistent threat (APT) actor with suspected ties to India has sprung forth with a flurry of attacks against high-profile entities and strategic infrastructures in the Middle East and Africa.
The activity has been attributed to a group tracked as SideWinder, which is also known as APT-C-17, Baby Elephant, and other names.
The group may be perceived as a low-skilled actor due to the use of public exploits, malicious LNK files and scripts as infection vectors

READ MORE

New FASTCash malware Linux variant helps steal money from ATMs

North Korean hackers are using a new Linux variant of the FASTCash malware to infect the payment switch systems of financial institutions and perform unauthorised cash withdrawal
Previous variants of FastCash targeted windows and IBM AIX system, but a new report by security researcher HaxRob reveals a previously undetected Linux version that target Ubuntu 22.04.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Ukraine tracks emailed bomb threats to Russia-linked group

Hong Kong Crime Ring Swindles Victims Out of $46M

Iran's APT34 Abuses MS Exchange to Spy on Gulf Gov'ts

Chinese Researchers Tap Quantum to Break Encryption

Breaches

SECURITY BREACHES THIS WEEK

Nearly 400 US healthcare institutions hit with ransomware over last year, Microsoft says

In the last fiscal year, 389 U.S.-based healthcare institutions were successfully hit with ransomware, causing “network closures, systems offline, critical medical operations delayed, and appointments rescheduled,” Microsoft said in its annual Digital Defense Report released on Tuesday. The company did not say how many were successfully attacked last year.

READ MORE

Central Tickets Confirms Data Breach as Hacker Leaks Data of 1 Million Users

Marriott and its subsidiary Starwood Hotels have agreed to pay $52 million in fines and create a revamped information security program, in an Federal Trade Commission (FTC)-led settlement with 344 million customers who were impacted by three data breaches occurring between 2014 and 2020.

READ MORE

OTHER SECURITY BREACHES

Central Tickets Confirms Data Breach as Hacker Leaks Data of 1 Million Users

Intel Broker Claims Cisco Breach, Selling Stolen Data from Major Firms

USDoD hacker behind National Public Data breach arrested in Brazil American Water Suffers Network Disruptions After Cyberattack

Pokemon dev Game Freak confirms breach after stolen data leaks online

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-23113 - Thousands of Fortinet instances vulnerable to actively exploited flaw

CVSS SCORE 9.8

CVE-2024-38178 - North Korean ScarCruft Exploits Windows Zero-Day to Spread RokRAT Malware

CVSS SCORE 7.5

LAST WEEKS RECAP

CVE-2024-9680 - Mozilla Firefox Use-after-free in Animation timeline
CVSS Score: (9.8)

CVE-2024-6197 - Open Source Curl Remote Code Execution Vulnerability Threat Assessment
CVSS Score: (8.8)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

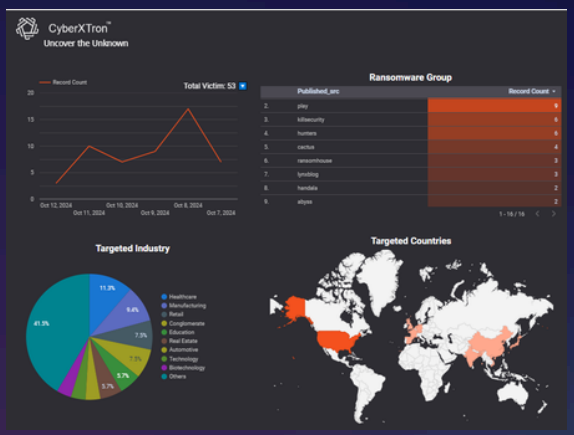
Last week we see ransomhub claim the most ransomware victims with 11 out of 53 down from 176 last week

TARGET INDUSTRIES

Last week saw the most ransomware attacks against the Healthcare 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

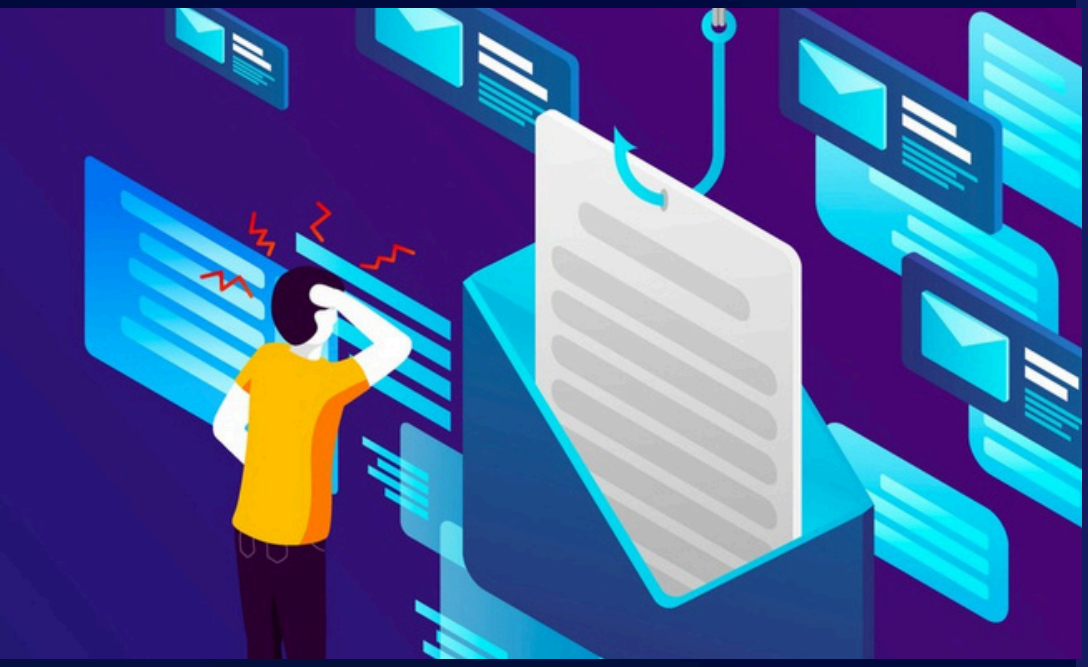
BlackBasta is a ransomware operator and Ransomware- as-a-Service criminal enterprise that first emerged in early 2022 and immediately became one of the most active RaaS threat actors in the world.

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



The Number of Malicious Emails Reaching Inboxes Is Declining

New research shows that less malicious emails are getting past security scanners to the inbox, but also provides details about how phishing emails are becoming increasingly dangerous.

So much of our training is centered around elevating the employee's state of cyber awareness so that when they do come across that sketchy email or that too good to be true web page, they know better.

But it's only one part of a larger cybersecurity effort within an organization. The hope is that security solutions will improve and employees become a less critical component of an organization's cyber defense.

The latest data from HP Wolf Security in their Threat Insights Report for September 2024 shows that less malicious emails are getting to the inbox: only 12% of emails (that's 1 in about 8.5 emails) that are making it to the inbox. That's the good news.

READ MORE

OTHER PHISHING ARTICLES

AI-Enhanced Cyber Attacks Top the List of Potential Threats Facing Data Security

Chinese Threat Actor Targets OpenAI With Spear-Phishing Attacks

"Operation Kaerb" Takes Down Sophisticated Phishing-as-a-Service Platform "iServer"

Sextortion Scammers Attempt to Hit "Close to Home"