SCC DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

SEPTEMBER 2024 - VOL.2

The News

IN THE NEWS THIS WEEK

Quad7 Botnet Expands to Target SOHO Routers and VPN Appliances

The operators of the mysterious Quad7 botnet are actively evolving by compromising several brands of SOHO routers and VPN appliances by leveraging a combination of both known and unknown security flaws. Targets include devices from TP-LINK, Zyxel, Asus, Axentra, D-Link, and NETGEAR. The botnet, which gets its name from the fact it opens TCP port 7777 on compromised devices, has been observed brute-forcing Microsoft 3665 and Azure instances.

READ MORE >

New PIXHELL acoustic attack leaks secrets from LCD screen noise

A novel acoustic attack named 'PIXHELL' can leak secrets from air-gapped and audio-gapped systems, and without requiring speakers, through the LCD monitors they connect to. In a PIXHELL attack, malware modulates the pixel patterns on LCD screens to induce noise in the frequency range of 0-22 kHz, carrying encoded signals within those acoustic waves that can be captured by nearby devices such as smartphones.

READ MORE >

OTHER NEWS HIGHLIGHTS

RansomHub ransomware abuses Kaspersky TDSSKiller to disable EDR software

Mustang Panda Deploys Advanced Malware to Spy on Asia-Pacific Governments

New RAMBO Attack Uses RAM Radio Signals to Steal Data from Air-Gapped Networks

SonicWall Urges Users to Patch Critical Firewall Flaw Amid Possible Exploitation

Microsoft Issues Patches for 79 Flaws, Including 3 Actively Exploited Windows Flaws

The News

TOP OF THE NEWS THIS WEEK

Transport for London confirms customer data stolen in cyberattack

Transport for London (TfL) has determined that the cyberattack on September 1 impacts customer data, including names, contact details, email addresses, and home addresses.

The urban transportation agency had informed the public on September 2 about an ongoing cybersecurity incident, assuring customers that at the time there was no evidence of data being compromised.

Last Friday, TfL staff was still facing system outages and disruptions, including the inability to respond to customer requests submitted via online forms, issue refunds for journeys paid with contactless methods, and more.

A new update on the TfL incident page explains that although the impact on its operations has remained minimal throughout this time, internal investigation uncovered that customer data has been compromised.

"Although there has been very little impact on our customers so far, the situation is evolving, and our investigations have identified that certain customer data has been accessed," reads the status page.

READ MORE >

TOP RELATED ARTICLES

TfL cyber-attack: teenager from Walsall arrested in connection with data breach

Transport for London confirms 5,000 users' bank data exposed, pulls large chunks of IT infra offline

TfL Confirms Customer Data Breach, 17-Year-Old Suspect Arrested

Boy arrested over London transport cyber hack

Geo-Politics

NEWS FROM AROUND THE WORLD

Chinese hackers use new data theft malware in govt attacks

Mustang Panda is a Chinese state-backed hacker group that focuses on cyberespionage operations against government and non-government entities mostly in Asia-Pacific, but organizations in other regions are also within its target scope.

New attacks attributed to China-based cyber espionage group Mustang Panda show that the threat actor switched to new strategies and malware called FDMTP and PTSOCKET to download payloads and steal information from breached networks.

READ MORE

DragonRank, a Chinese-speaking SEO manipulator service provider

The Cisco Talos Blog Intelligence Center has uncovered a Chinese-speaking hacking group, known as DragonRank, engaging in black hat SEO practices to manipulate search engine rankings and promote their clients' internet visibility. The group operates differently from traditional black hat SEO cybercrime groups, focusing on lateral movement and privilege escalation to infiltrate additional servers within the target's network.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Iran-linked hackers target Iraqi government in new campaign

Chinese-made port cranes in US included 'backdoor' modems, House report says

Singapore Police Arrest Six Hackers Linked to Global Cybercrime Syndicate

Experts Identify 3 Chinese-Linked Clusters Behind Cyberattacks in Southeast Asia

Breaches

SECURITY BREACHES THIS WEEK

Fortinet confirms data breach after hacker claims to steal 440GB of files

Cybersecurity giant Fortinet has confirmed it suffered a data breach after a threat actor claimed to steal 440GB of files from the company's Microsoft SharePoint server. The threat actor, known as "Fortib*tch," claims to have tried to extort Fortinet into paying a ransom, likely to prevent the publishing of data, but the company refused to pay.

READ MORE

Turkish minister confirms vast personal data breach of millions

Transport and Infrastructure Minister Abdulkadir Uraloğlu has confirmed that the personal data of millions Turkish citizens were stolen and said, “It is true that some information was unfortunately obtained in a certain way during the pandemic process. Unfortunately, it could not be prevented in that process.”

READ MORE

OTHER SECURITY BREACHES

Cleveland Police officer facing the sack for data breaches

Popular French retailers confirm hackers stole customer data

Payment gateway data breach affects 1.7 million credit card owners

Ransomware attack forces high school in London to close and send students home

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-29847 - Ivanti EPM deserialization of untrusted data vulnerability

CVSS SCORE 10.0

CVE-2024-32840, CVE-2024-32842, CVE-2024-32843, CVE-2024-32845, CVE-2024-32846, CVE-2024-32848, CVE-2024-34779, CVE-2024-34783, and CVE-2024-34785 - Ivanti EPM Multiple unspecified SQL injection vulnerabilities

CVSS SCORE 9.1

CVE-2024-45112 - Adobe Reader Arbitrary code execution

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2023-38831 - RARLAB WinRAR Code Execution Vulnerability
7.8 (Medium)

CVE-2024-38811 - VMware Fusion code execution vulnerability
8.1 (High)

CVE-2024-7261 - Zyxel secure routers allows OS command execution via cookie
9.8 (Critical)

CVE-2024-32896 - Android Pixel Privilege
7.8 (High)

CVE-2024-20469 - Cisco Identity Services Engine Command Injection Vulnerability
6.0 (Low)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

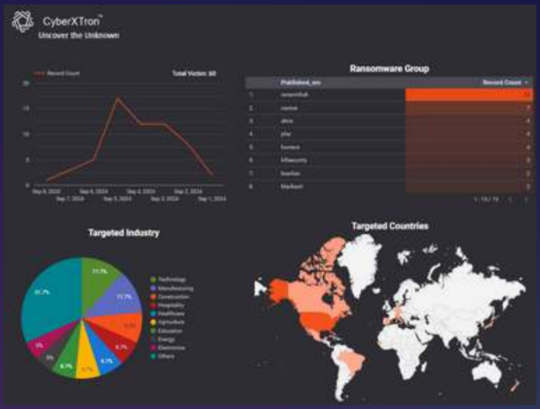
Last week we seen a continuous trend where RansomHub took the top spot with a total of 24 victims out of 60

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.



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

Mind your header! There's nothing refreshing about phishers' latest tactic

Palo Alto's Unit 42 threat intel team has identified attackers abusing refresh entries in HTTP headers to the tune of circa 2,000 large-scale phishing campaigns between May and July this year, although the practice has been observed throughout the year.

Embedding malicious URLs in a web page's response header, in this case, means visitors to the web pages are automatically redirected to malicious ones. Once this is accomplished, attackers will typically spoof the login pages of well-known vendors to steal the user's passwords.

The attack starts out like any other phishing-based incident. An email is sent to a target containing a link that typically mimics a legitimate or compromised domain, making the job of spotting one more difficult.

Should a user click that link (failure number one), they'll be directed to one page which the attacker has already instructed to redirect to another after a period of, say, a few seconds – although it could be done immediately too. Because the refresh field was populated with the code that redirects visitors to alternative URLs, this process is not only executed automatically against the user's will, but also before the initial web page is even loaded, since the response header is handled before HTML content loads.

READ MORE

OTHER PHISHING ARTICLES

Sextortion scams now use your "cheating" spouse’s name as a lure

Research Identifies Prevalence of Brand Impersonation in Three-Year Cross-Industry Analysis

DuckDuckGo and Bing users warned of Etherscan phishing website

Beware of Work Email Security Alert that Steals Your Login Credentials