SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JUNE 2024 - VOL.4

The News

IN THE NEWS THIS WEEK

New Attack Technique Exploits Microsoft Management Console Files

Threat actors are exploiting a novel attack technique in the wild that leverages specially crafted management saved console (MSC) files to gain full code execution using Microsoft Management Console and evade security defences. When a maliciously crafted console file is imported, a vulnerability in one of the MMC libraries can lead to running adversary code, including malware. Attackers can combine this technique with DotNetToJScript to gain arbitrary code execution, which can lead to unauthorized access, system takeover and more.

READ MORE

Hackers target new MOVEit Transfer critical auth bypass bug

Threat actors are already trying to exploit a critical authentication bypass flaw in Progress MOVEit Transfer, less than a day after the vendor disclosed it. The new security issue received the identifier CVE-2024-5806 and allows attackers to bypass the authentication process in the Secure File Transfer Protocol (SFTP) module, which is responsible for file transfer operations over SSH.

READ MORE

OTHER NEWS HIGHLIGHTS

The Different types of insider threats and how to stop them

New Medusa malware variants target Android users in seven countries

Warning: New Adware Campaign Targets Meta Quest App Seekers

Critical GitLab bug lets attackers run pipelines as any user

The News

TOP OF THE NEWS THIS WEEK

Over 110,000 Websites Affected by Hijacked Polyfill Supply Chain Attack

Google has taken steps to block ads for e-commerce sites that use the Polyfill.io service after a Chinese company acquired the domain and modified the JavaScript library ("polyfill.js") to redirect users to malicious and scam sites.

More than 110,000 sites that embed the library are impacted by the supply chain attack.

The original creator of the project, Andrew Betts, urged website owners to immediately remove it, adding that no website today requires any of the polyfills in the polyfill[.]io library and that most features added to the web platform are quickly adopted by all major browsers

Cloudflare has also issued fresh warnings, urging website owners to remove polyfill[.]io as it could be used to inject malicious JavaScript code into users' browsers. It also emphasized that it has never recommended the polyfill[.]io service or authorized their use of Cloudflare's name on their website.

What's more, the website has been taken down by domain registrar Namecheap, although it has since migrated to another domain named polyfill[.]com, according to developer security platform Socket.

READ MORE

TOP RELATED ARTICLES

Polyfill.io supply chain attack hits 100,000+ websites all you need to know

Automatically replacing polyfill.io links with Cloudflare's mirror for a safer Internet

If you're using Polyfill.io code on your site like 100,000+ are remove it immediately

Cloudflare: We never authorized polyfill.io to use our name

Geo-Politics

NEWS FROM AROUND THE WEEK

Chinese Cyberspies Employ Ransomware in Attacks for Diversion

A joint report from SentinelLabs and Recorded Future analysts presents the case of ChamelGang, a suspected Chinese APT that has been using the CatB ransomware strain in attacks that impact high-profile organizations worldwide. ChamelGang has been know to target government organizations and critical infrastructure.

READ MORE

RedJuliett Cyber Espionage Campaign Hits 75 Taiwanese Organizations

A likely China-linked state-sponsored threat actor has been linked to a cyber espionage campaign targeting government, academic, technology, and diplomatic organizations in Taiwan. The group allegedly operate from Fuzhou, China, to support Beijing's intelligence collection goals related to the East Asian country, they are know to target internet-facing appliances such as firewalls, load balancers, and enterprise virtual private network VPN products for initial access, as well as attempting structured query language SQL injection and directory traversal exploits against web and SQL applications

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

ExCobalt Cyber Gang Targets Russian Sectors with New GoRed Backdoor

Julian Assange pleads guilty, leaves courtroom a free man

Crimea warns of internet disruptions following DDoS attacks on local telecom operators

EU blames 'clerical error' after misattributing hacks to wrong Russian spy agency

Breaches

SECURITY BREACHES THIS WEEK

TeamViewer's corporate network was breached in alleged APT hack

On Wednesday, 26 June 2024, the team at TeamViewer detected an irregularity in their internal corporate IT environment. They have warned that its corporate environment was breached in a cyberattack, with a cybersecurity firm claiming it was by an APT hacking group. TeamViewer's internal corporate IT environment is completely independent from the product environment. There is no evidence to suggest that the product environment or customer data is affected.

READ MORE

Neiman Marcus confirms data breach after Snowflake account hack

Luxury retailer Neiman Marcus confirmed it suffered a data breach after hackers attempted to sell the company's database stolen in recent Snowflake data theft attacks, the company says that the breach impacted 64,472 people. The types of personal information affected varied by individual, and included information such as name, contact information, date of birth, and Neiman Marcus or Bergdorf Goodman gift card number(s) (without gift card PINs).

READ MORE

OTHER SECURITY BREACHES

Multiple WordPress Plugins Compromised: Hackers Create Rogue Admin Accounts

BlackSuit ransomware gang claims attack on KADOKAWA corporation

Evolve Bank confirms data breach after brazen LockBit claims

Taj Hotel Group investigates potential data breach impacting 1.5 million customers

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-27867 - AirPods Firmware Update 6A326

UNDER ANALYSIS

CVE-2024-28995 - SolarWinds Serv-U Local File Disclosure Directory Transversal

CVSS SCORE 8.6

LAST WEEKS RECAP

CVE-2024-29824 - An unspecified SQL Injection Vulnerability - Ivanti EPM 2022
9.6 (Critical)

CVE-2024-38428 - Critical vulnerability in wget
10.0 (Critical)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

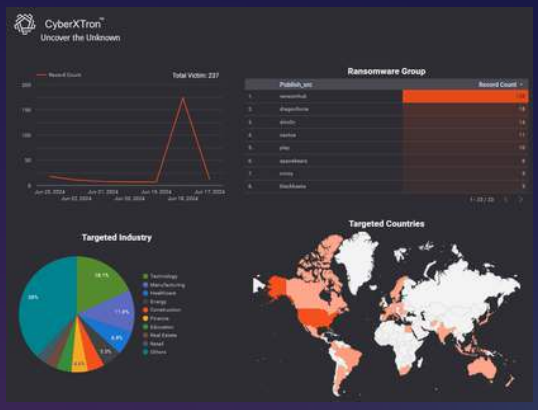
RansomHub saw a major increase with a whopping 135 counts of attacks and a new name on the board (dragonforce) has seen 18 attacks last week.

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.



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

Cl0p

The Cl0p Ransomware Group are a hacking organisation that has Russian-speaking members and emerged in early 2019 and is associated with the greater TA505 threat group

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

SCAM OF THE WEEK:
School Board Election Phishing

In this week's scam, cybercriminals targeted candidates in a local election. During any election season, many candidates post information about themselves online or on social media sites. Scammers can use this information to craft targeted attacks on the candidates. In the specific attacks mentioned below, the scammers pretended to be another election candidate. This type of attack is known as Business Email Compromise (BEC).

In one of the attacks, the scammers emailed an election candidate. In the email, they impersonated someone else who was also running for election. The scammers explained that they needed the victim to purchase $500 in Apple gift cards and send them via email. When this didn't work, the scammers later sent a separate email that appeared to come from DocuSign. This email contained an attachment that directed the victim to a fake login screen that prompted them to enter their user credentials in order to continue. If the victim had fallen for either of these scams, the scammers would have been able to steal both money and login credentials from the victim.

READ MORE

OTHER PHISHING ARTICLES

FBI warns of fake law firms targeting crypto scam victims

Military-themed Email Scam Spreads Malware to Infect Pakistani Users

Tricky Fake Invoice Phishing Attack Uses Search to Deliver Malware

Facebook, Meta, Apple, Amazon Most Impersonated in Phishing Scams