SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

AUGUST 2024 - VOL.3

The News

IN THE NEWS THIS WEEK

Cybercriminals Exploit Popular Software Searches to Spread FakeBat Malware

Cybersecurity researchers have uncovered a surge in malware infections stemming from malvertising campaigns distributing a loader called FakeBat. "These attacks are opportunistic in nature, targeting users seeking popular business software," the Mandiant Managed Defense team said in a technical report. "The infection utilizes a trojanized MSIX installer, which executes a PowerShell script to download a secondary payload."

READ MORE

Microsoft Apps for macOS Exposed to Library Injection Attacks

Eight Microsoft applications for macOS are vulnerable to library injection attacks, potentially allowing adversaries to steal app permissions and breach sensitive data, according to new research by Cisco Talos. The impacted Microsoft apps include popular services like Microsoft Teams, Outlook, PowerPoint and Word, with eight CVE numbers assigned.

READ MORE

OTHER NEWS HIGHLIGHTS

GiveWP WordPress Plugin Vulnerability Puts 100,000+ Websites at Risk

Ransomware Victims Paid $460 Million in First Half of 2024

Microsoft Patches Critical Copilot Studio Vulnerability Exposing Sensitive Data

Major Backdoor in Millions of RFID Cards Allows Instant Cloning

Google Fixes High-Severity Chrome Flaw Actively Exploited in the Wild

The News

TOP OF THE NEWS THIS WEEK

New Phishing Technique Bypasses Security on iOS and Android to Steal Bank Credentials

Anti-malware vendor ESET is warning of a new phishing tactic targeting iOS and Android users with web applications mimicking legitimate banking software to bypass security protections and steal login credentials.

On both iOS and Android platforms, ESET warns that cybercriminals used Progressive Web Applications (PWA), which are websites bundled to look like stand-alone applications, while on Android they also used WebAPKs, which appear to be installed from Google Play.

Built using web application technologies, PWAs can run on various platforms and device types, and do not require the user to allow third-party app installation.

As part of the observed attacks, iOS users were instructed to add the PWA to home screens, while Android users had to confirm certain custom pop-ups in the browser before the application was installed.

READ MORE

TOP RELATED ARTICLES

Phishing in PWA Applications: A New Method Targeting Mobile Users

New banking-targeted phishing scheme involves progressive web apps

Novel Phishing Method Used in Android/iOS Financial Fraud Campaigns

Android and iOS users targeted with novel banking app phishing campaign

Geo-Politics

NEWS FROM AROUND THE WORLD

US warns of Iranian hackers escalating influence operations

The U.S. government is warning of increased effort from Iran to influence upcoming elections through cyber operations targeting Presidential campaigns and the American public. In a joint statement from the Office of the Director of National Intelligence (ODNI), the FBI, and the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. says that Iran carried out cyberattacks in an attempt to gain access to sensitive information related to U.S. elections.

READ MORE

New macOS Malware TodoSwift Linked to North Korean Hacking Groups

Cybersecurity researchers have uncovered a new macOS malware strain dubbed TodoSwift that they say exhibits commonalities with known malicious software used by North Korean hacking groups. "This application shares several behaviors with malware we've seen that originated in North Korea (DPRK) — specifically the threat actor known as BlueNoroff — such as KANDYKORN and RustBucket," Kandji security researcher Christopher Lopez said in an analysis.

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Chinese Threat Actors Use MSI Files to Bypass Windows, VT Detection

Hackers deployed new malware against university in Taiwan

'Pro-Palestine' hacking group banned on X as US criticizes Iran over cyberattacks

Moscow detains scientist suspected of carrying out DDoS attacks on Russia

Breaches

SECURITY BREACHES THIS WEEK

National Public Data Says Breach Impacts 1.3 Million People

National Public Data (NPD) has confirmed suffering a data breach following reports of 2.9 billion personal information records being compromised, but the company says the incident only affects 1.3 million people in the US. Last week the firm published information on the leak. The information is vague, and there is some difficulty in accessing the URL.

READ MORE

Toyota confirms third-party data breach impacting customers

Toyota confirmed that customer data was exposed in a third-party data breach after a threat actor leaked an archive of 240GB of stolen data on a hacking forum. "We are aware of the situation. The issue is limited in scope and is not a system wide issue," Toyota told BleepingComputer when asked to validate the threat actor's claims.

READ MORE

OTHER SECURITY BREACHES

Microchip Technology discloses cyberattack impacting operations

Hacker locks Unicoin staff out of Google accounts for 4 days

Carespring Data Breach Exposes Personal and Medical Information of Nearly 77,000 Patients

City of Flint Scrambling to Restore Services Following Ransomware Attack

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-38206 - Microsoft Copilot Studio Information Disclosure Vulnerability

CVSS SCORE 8.5

CVE-2024-38175- Azure Managed Instance for Apache Cassandra Elevation of Privilege Vulnerability

CVSS SCORE 9.6

CVE-2024-4577 - PHP CGI Argument Injection vulnerability

CVSS SCORE 9.8

CVE-2024-7971 - Type confusion in V8 in Google Chrome

CVSS SCORE 8.8

CVE-2024-43477 - Entra ID Elevation of Privilege Vulnerability

CVSS SCORE 7.5

LAST WEEKS RECAP

CVE-2024-38200 - Microsoft Office Spoofing Vulnerability
6.5 (Medium)

CVE-2024-38063- Windows TCP/IP Remote Code Execution Vulnerability
9.8 (Critical)

CVE-2024-28986 - SolarWinds Web Help Desk Java Deserialization Remote Code Execution Vulnerability
9.8 (Critical)

CVE-2024-38109 - Azure Health Bot Elevation of Privilege Vulnerability
9.1 (Critical)

CVE-2024-7593 - Incorrect implementation of an authentication algorithm in Ivanti vTM
9.8 (Critical)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

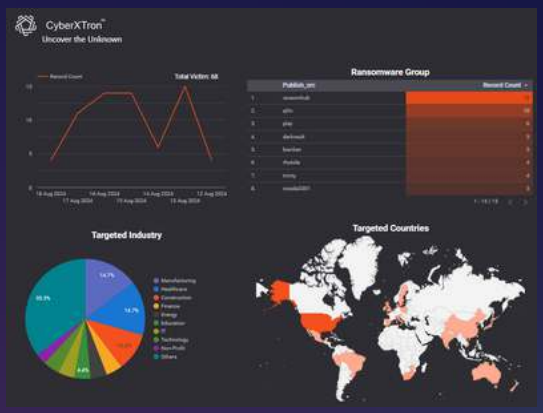
Last week there were a total of 68 ransomware victims with the ‘ransomhub’ group claiming the most victims with 18.

TARGET INDUSTRIES

Last week saw the most ransomware attacks against the Manufacturing and 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

Iranian Group TA453 Launches Phishing Attacks with BlackSmith

The Iranian-linked threat actor TA453 (also known as Charming Kitten) has been observed launching a sophisticated phishing attack using a PowerShell-based malware toolkit dubbed “BlackSmith.”

The campaign, observed by Proofpoint, began in July 2024 and targeted a prominent Jewish figure through a series of emails spoofing the Institute for the Study of War (ISW).

Posing as the ISW’s Research Director, TA453 invited the target to participate in a podcast, a tactic aimed at building trust. Once rapport was established, the group sent a malicious link disguised as a legitimate podcast URL, ultimately delivering the BlackSmith malware.

“TA453 uses many different social engineering techniques to try and convince targets to engage with malicious content,” Proofpoint explained.

“Like multi-persona impersonation, sending legitimate links to a target and referencing a real podcast from the spoofed organization can build user trust. When a threat actor builds a connection with a target over time before delivering the malicious payload, it increases the likelihood of exploitation.”

READ MORE

OTHER PHISHING ARTICLES

U.K. Management Almost Twice as Likely to Fall for Phishing Attacks Versus Entry-Level Employees

Ransomware Group Known as ‘Royal’ Rebrands as BlackSuit and Is Leveraging New Attack Methods

Crypto phishing attack drains $55M from whale’s wallet

Blind Eagle Hackers Exploit Spear-Phishing to Deploy RATs in Latin America