SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

JULY 2024 - VOL.3

The News

IN THE NEWS THIS WEEK

Automated Threats Pose Increasing Risk to the Travel Industry

As the travel industry rebounds post-pandemic, it is increasingly targeted by automated threats, with the sector experiencing nearly 21% of all bot attack requests last year. The summer travel season and major European sporting events are expected to drive increased consumer demand for flights, accommodation, and other travel-related services. As a result, Imperva warns that the industry could see a surge in bot activity.

READ MORE >

Threat Actors Ramp Up Use of Encoded URLs to Bypass Secure Email

Email security tools such as Secure Email Gateways (SEGs) often encode URLs that are embedded in emails. This enables the security appliance to scan the URL before the recipient visits the website. Oftentimes when SEGs detect URLs in emails that are already SEG encoded they do not scan the URLs, or the scanning shows only the security tool's scanning page and not the actual destination. As a result, when an email already has SEG encoded URLs the recipient's SEG often allows the email through without properly checking the embedded URLs. Threat actors have abused this for some time, but Q2 of this year, and May in particular, saw an increase in threat actors taking advantage of SEG encoding malicious URLs before sending them to victims.

READ MORE >

OTHER NEWS HIGHLIGHTS

Microsoft links Scattered Spider hackers to Qilin ransomware attacks

Signal downplays encryption key flaw, fixes it after X drama

'Konfety' Ad Fraud Uses 250+ Google Play Decoy Apps to Hide Malicious Twins

Firmware update hides Bluetooth fingerprints

The News

TOP OF THE NEWS THIS WEEK

Notorious FIN7 hackers sell EDR killer to other threat actors

The notorious FIN7 hacking group has been spotted selling its custom "AvNeutralizer" tool aka (AuKill), used to evade detection by killing enterprise endpoint protection software on corporate networks.

FIN7 is believed to be a Russian hacking group that has been active since 2013, initially focusing on financial fraud by hacking organizations and stealing debit and credit cards.

The AuKill tool abuses an outdated version of the driver used by version 16.32 of the Microsoft utility, Process Explorer, to disable EDR processes before deploying either a backdoor or ransomware on the target system. The tool abuses a legitimate, but out-of-date and exploitable, driver. This technique is commonly referred to as a “bring your own vulnerable driver” (BYOVD) attack.

The attackers takes advantage of a driver both created by and signed by Microsoft. The Process Explorer driver "PROCEXP.SYS"

READ MORE ›

TOP RELATED ARTICLES

FIN7 Reboot | Cybercrime Gang Enhances Ops with New EDR Bypasses and Automated Attacks

FIN7 Group Advertises Security-Bypassing Tool on Dark Web Forums

The Stark Truth Behind the Resurgence of Russia’s Fin7

Russia-linked FIN7 hackers sell their security evasion tool to other groups on darknet

Geo-Politics

NEWS FROM AROUND THE WEEK

China-linked APT17 Targets Italian Companies with 9002 RAT Malware

A China-linked threat actor called APT17 has been observed targeting Italian companies and government entities using a variant of a known malware referred to as 9002 RAT. The first campaign Office document, while the second campaign contained a link with both campaigns inviting the victim to install a Skype for Business package from a link of an Italian government-like domain to convey a variant of 9002 RAT.

READ MORE

Hacktivist Groups Target Romania Amid Geopolitical Tensions

Security researchers have observed increased geopolitical DDoS attacks against Romania. The data comes from recent research conducted by ASERT, which also noted that these attacks span various industries and involve multiple hacktivist groups, including CyberDragon and the Cyber Army of Russia among others

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Paris 2024 Olympics to face complex cyber threats

Iranian Hackers Deploy New BugSleep Backdoor in Middle East Cyber Attacks

TAG-100 Uses Open-Source Tools in Suspected Global Espionage Campaign, Compromising Two Asia-Pacific Intergovernmental Bodies

Chinese State Actor APT40 Exploits N-Day Vulnerabilities “Within Hours”

Breaches

SECURITY BREACHES THIS WEEK

Over 400,000 Life360 user phone numbers leaked via unsecured API

A threat actor has leaked a database containing the personal information of 442,519 Life360 customers collected by abusing a flaw in the login API. Known only by their 'emo' handle, they said the unsecured API endpoint used to steal the data provided an easy way to verify each impacted user's email address, name, and phone number.

According to the threat actor, Life360 has since fixed the API flaw, and additional requests now return a placeholder phone number.

READ MORE

AT&T Confirms Data Breach Affecting Nearly All Wireless Customers

American telecom service provider AT&T has confirmed that threat actors managed to access data belonging to "nearly all" of its wireless customers as well as customers of mobile virtual network operators using AT&T's wireless network. Threat actors unlawfully accessed an AT&T workspace on a third-party cloud platform and exfiltrated files containing AT&T records of customer call and text interactions.

READ MORE

OTHER SECURITY BREACHES

Yacht giant MarineMax data breach impacts over 123,000 people

Critical Exim bug bypasses security filters on 1.5 million mail servers

Email addresses of 15 million Trello users leaked on hacking forum

Rite Aid says June data breach impacts 2.2 million people

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2024-20419 - Cisco Smart Software Manager On-Prem Password Change Vulnerability

CVSS SCORE 10.0

CVE-2024-36401 - Improve handling of XPath expressions

CVSS SCORE 9.8

CVE-2024-27348 - Expedition: Missing Authentication Leads to Admin Account Takeover

CVSS SCORE 9.8

PSV-2023-0122 - Stored Cross Site Scripting on Some Routers

CVSS SCORE 7.1

CVE-2024-4577 - Remote Execution Vulnerability in PHP

CVSS SCORE 9.8

LAST WEEKS RECAP

CVE-2024-6409 - OpenSSH: Possible remote code execution in privsep child due to a race condition in signal handling
7.0 (Medium)

CVE-2024-29510 - Exploiting Ghostscript using format strings
5.5 (Medium)

CVE-2024-5910 - Expedition: Missing Authentication Leads to Admin Account Takeover
9.3 (Critical)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

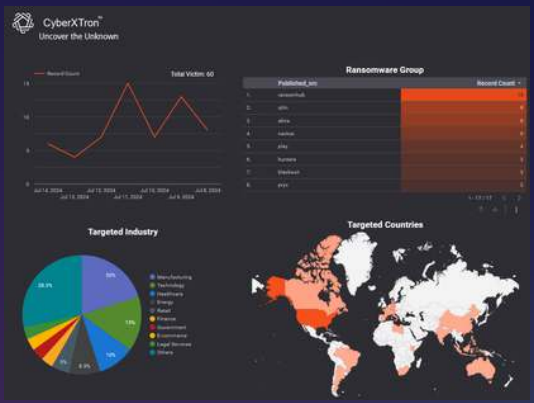
Ransomhub remains is the largest contributor, claiming 15 of these victims, closely followed by qilin and Akira.

TARGET INDUSTRIES

This 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

Beware of the Latest Phishing Tactic Targeting Employees - HR

Researchers have seen a new phishing tactic being employed that impersonates a company's Human Resources (HR) department.

This phishing email is designed to look like an official communication from your company's HR department. It arrives in your inbox with a subject line that grabs attention, urging you to review the employee handbook. See Email HERE!

The email's layout and language further enhance its perceived legitimacy. It opens with a formal greeting and presents a message in a structured format typical of corporate communications. The language used is professional, clear, and direct, mimicking the tone and style that employees would expect from an HR department.

The subject line, "Modified Employee Handbook For All Employees – Kindly Acknowledge," immediately grabs attention and creates a sense of urgency. This tactic is designed to provoke quick action from recipients, prompting them to open the email and engage with its contents without hesitation. Click HERE to view the example Phishing page.

READ MORE >

OTHER PHISHING ARTICLES

Malvertising Campaign Impersonates Microsoft Teams

Facebook Ads for Windows Desktop Themes Push Info-Stealing Malware

New phishing tactic hijacks email protections to mask links

Attackers starting to use spear phishing tactics in bulk phishing campaigns