Date of Publication
March 20, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

13 to 19 MARCH 2023

Summary

Threat Actors

Over the past week, Hive Pro detected the presence of five active threat actors. The first of these is **Dark Pink APT**, a notorious group with a history of engaging in information theft and espionage. The second actor is **Tick APT**, a Chinese cybercrime organization that primarily focuses on information theft and espionage. The third actor identified is **APT29**, while the fourth is **YoroTrooper**. The fifth actor is the **BianLian ransomware** group. For more information, please refer to the key takeaway section on Threat Actors.

Attacks

Over the past week, a total of fourteen new strains of active malware were detected. Among them were two ransomware variants, namely, **IceFire Ransomware** and **BianLian Ransomware**. In addition, two Remote Access Trojans (RATs) were also discovered, namely **WarzoneRAT** and **LodaRAT**. Furthermore, a new type of malware known as **KamiKakaBot** Malware was also identified, along with nine other types of malware. For more information, please refer to the key takeaway section on Attacks.

Vulnerabilities

Last week, we identified 35 vulnerabilities that organizations should be aware of. Among these, **three** were found in Adobe ColdFusion, while Google Chrome resolved **twenty** vulnerabilities. Furthermore, Microsoft addressed a total of 83 vulnerabilities in its Tuesday patch, with **ten** of them particularly noteworthy. For more information, please refer to the key takeaway section on vulnerabilities.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Threat Actors

Dark Pink APT

The Dark Pink APT group is a threat actor group that has been active in targeting government entities in South Asian countries. the Dark Pink APT group has been using various tactics to gain access to sensitive information, including spear-phishing attacks and exploiting vulnerabilities in software.

Tick APT

Tick, an APT group, attacked an East Asian data-loss prevention software company, compromising update servers and distributing malware, using trojanized installers, to access computers of government and military entities.

APT29

APT29 is a Russian advanced persistent threat (APT) group that primarily engages in cyber espionage. In a recently detected operation targeting EU governments, the group was observed employing phishing emails that carried a malevolent document, leveraging the recent visit of the Polish Foreign Minister to the US as a pretext.

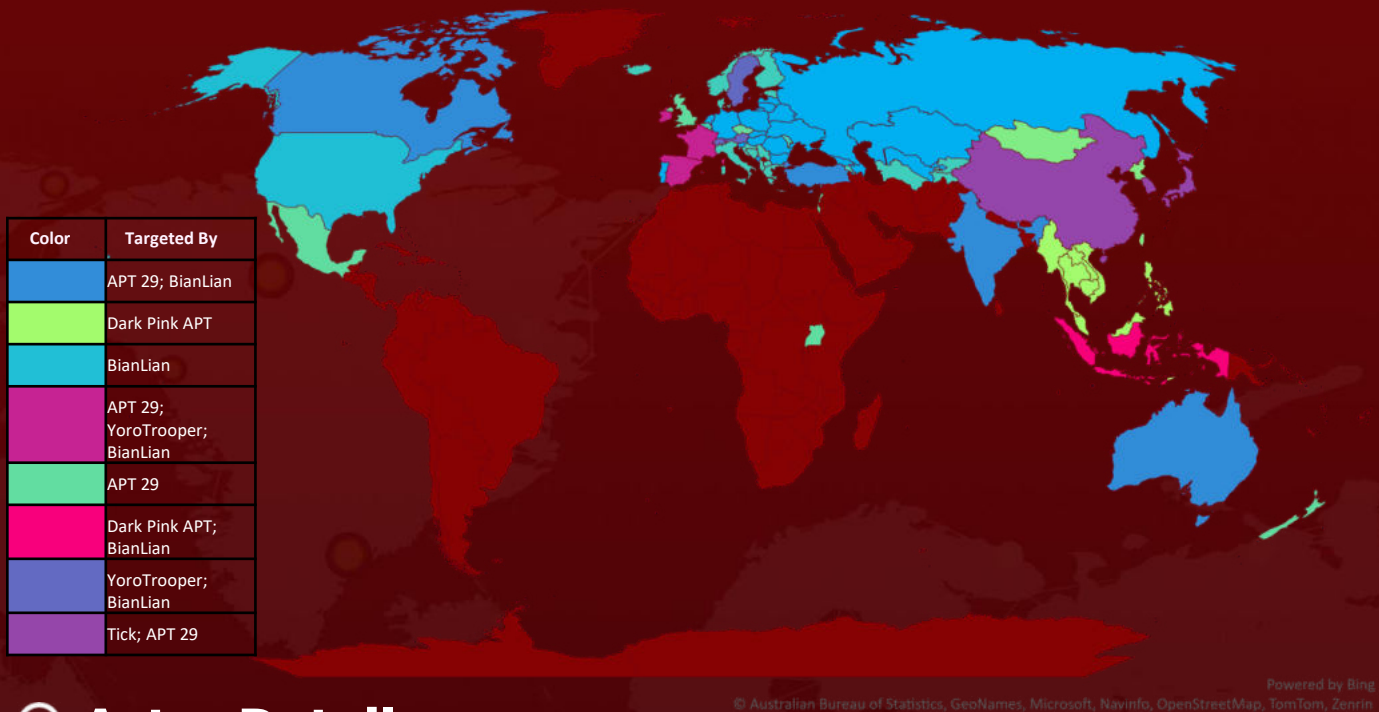
YoroTrooper

A new threat actor named "YoroTrooper," has been conducting espionage campaigns since at least June 2022. The group's main motivation appears to be espionage, and they register malicious domains or typo-squatted domains to trick their victims. The group primarily targets government or energy organizations in Azerbaijan, Tajikistan, Kyrgyzstan, and other Commonwealth of Independent States
(CIS) countries.

BianLian ransomware

BianLian is a ransomware group, that continues to add more victims, displaying a high level of operational security and skill in network penetration. Its shift of focus from ransoming encrypted files to data-leak extortion is also notable. The group has improved its ability to operate the business side of a ransomware organization while maintaining similar Tactics, Techniques, and Procedures (TTPs) to perform their initial access and lateral movement within a victim'snetwork.

Actor Map



Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Dark Pink APT (Saaiwc Group, APT-LY-005)	Unknown	Information theft and Espionage
	Tick(BRONZE BUTLER, CTG-2006, REDBALDKNIGHT, Stalker Panda)	China	Information theft and Espionage
	APT 29 (Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)	Russia	Information theft and Espionage
	YoroTrooper	Unknown	Information theft and Espionage
	BianLian	Unknown	Information theft

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Attacks

GoBruteforcer (unattributed)
A new Golang-based malware called GoBruteforcer has been discovered, which targets web servers running phpMyAdmin, MySQL, FTP, and Postgres services. It uses the Golang programming language, which has become increasingly popular with malware programmers.

KamiKakaBot malware (Dark Pink APT)
A new cyberattack campaign using the KamiKakaBot malware being used to target government entities in ASEAN countries. This malware is designed to steal data from web browsers such as Chrome, Edge, and Firefox, including saved credentials, browsing history, and cookies. It can also, allow the attackers to execute remote code on infected devices.

BlackLotus bootkit (Unattributed)
BlackLotus is a dangerous UEFI bootkit that can take full control of the operating system boot process, allowing it to disable security measures and deploy its own payloads; it exploits a known vulnerability in UEFI Secure Boot and is capable of running on up-to-date Windows 11 systems, and is advertised and sold on underground forums for $5,000 to unknown threat actors.

IceFire ransomware (Unattributed)
The IceFire ransomware strain, previously identified on Windows systems, has now expanded its scope to target Linux enterprise networks of several media and entertainment industry organizations. The IceFire ransomware is being deployed by exploiting a deserialization vulnerability (CVE-2022-47986) in the IBM Aspera Faspex file-sharing software.

ShadowPy (Tick APT)
ShadowPy is a type of malware that has been known to infect Windows systems. It is classified as a Trojan and is designed to steal sensitive information from infected systems, such as login credentials, financial information, and other personal data.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Netboy (Tick APT)

The Netboy backdoor, also known as "Invader" is a type of malware that allows an attacker to gain unauthorized access to a compromised system and perform various malicious actions, such as stealing data or executing remote commands.

Prometei botnet (Unattributed)

The Prometei botnet, a highly modular botnet with worm-like capabilities that predominantly installs the Monero cryptocurrency miner, has been regularly upgraded and updated since its discovery in 2016, providing a chronic threat to corporates.

Vidar (Unattributed)

Vidar malware is a type of information-stealing malware that is designed to collect sensitive information from infected systems. The malware is typically distributed through spam emails, malicious downloads, or compromised websites, and once it infects a system, it can perform a range of malicious activities.

Ursnif (Unattributed)

Ursnif, also known as Gozi or ISFB, is a sophisticated banking Trojan that is designed to steal sensitive information from infected systems, particularly financial data such as login credentials, credit card numbers, and other banking information.

BatLoader (Unattributed)

BatLoader is a type of malware that is designed to deliver other types of malware onto infected systems. It is typically spread through phishing emails or drive-by downloads, where the victim unknowingly downloads and executes a malicious script.

WarzoneRAT (YoroTrooper)

WarzoneRAT is a remote access trojan (RAT) that is designed to allow attackers to gain unauthorized access to a victim's computer. RATs are a type of malware that allows an attacker to take control of a victim's computer from a remote location.

LodaRAT (YoroTrooper)

LodaRAT is a remote access trojan (RAT) that is designed to allow attackers to gain unauthorized access to a victim's computer. Like other RATs, LodaRAT is typically spread via phishing emails, malicious software downloads, or other social engineering tactics.

*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

BianLian Ransomware (Unattributed)

BianLian is a ransomware, that continues to add more victims, displaying a high level of operational security and skill in network penetration. Its shift of focus from ransoming encrypted files to data-leak extortion is also notable.

DotRunpeX Malware (Unattributed)

DotRunpeX malware attack vectors have been linked to dozens of campaigns. The DotRunpeX is a second-stage infection used to deploy a variety of malware families, most notably stealers, RATs, loaders, and downloaders.

TOP MITRE ATT&CK TTPS:

T1204 User Execution	**T1204.002** Malicious File	**T1059** Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/ Decode Files or Information
T1082 System Information Discovery	**T1203** Exploitation for Client Execution	**T1518** Software Discovery	**T1071** Application Layer Protocol	**T1497** Virtualization/ Sandbox Evasion
T1059.001 Power Shell	**T1083** File and Directory Discovery	**T1036** Masquerading	**T1068** Exploitation for Privilege Escalation	**T1571** Non-Standard Port
T1055 Process Injection	**T1518.001** Security Software Discovery	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1486** Data Encrypted for Impact

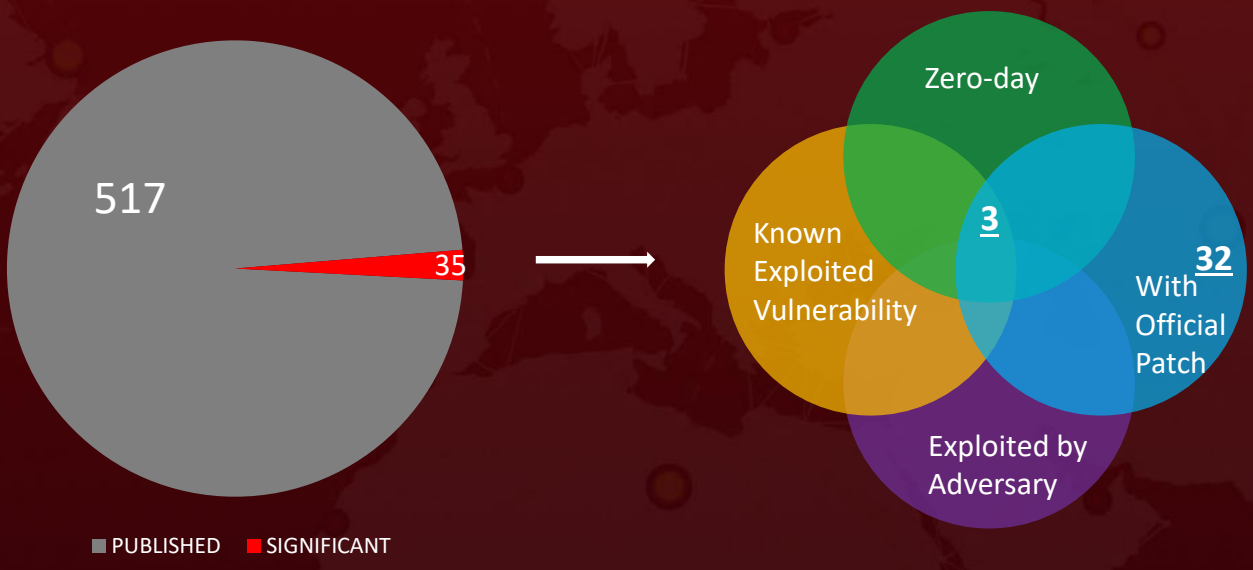
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Thirty-Five Notable Mentions

Out of the 35 security vulnerabilities discovered across various applications, ten were found in multiple Microsoft applications, including two zero-day vulnerabilities (CVE-2023-24880 and CVE-2023-23397). These vulnerabilities could potentially allow remote code execution, privilege escalation, information disclosure, spoofing, security feature bypass, and denial of service. In addition, three vulnerabilities were identified in Adobe ColdFusion, including one zero-day (CVE-2023-26360) that could result in arbitrary code execution and memory leaks. Furthermore, Google Chrome addressed twenty issues related to arbitrary code execution that could potentially lead to the exposure of sensitive information.



*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **35 significant vulnerabilities** and block the indicators related to the threat actor **DarkPink APT, Tick APT, APT 49, YoroTrooper and BianLian** and malware, **KamiKakaBot, BianLian Ransomware, IceFire Ransomware Malware, Warzone RAT, LodaRAT and nine other malware.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **35 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware, **KamiKakaBot, BianLian Ransomware, IceFire Ransomware Malware, Warzone RAT, LodaRAT, and nine other malware** in Breach and Attack Simulation(BAS).

Threat Advisories

Check out the links below for more extensive remediation and security precautions.

New GoBruteforcer Malware Targeting Web Servers Running Popular Services

Chrome 111 addresses an array of security flaws

New KamiKakaBot Malware Targeting Government Entities in ASEAN Countries

BlackLotus UEFI Bootkit Exploits Windows 11 vulnerability

IceFire Ransomware Strikes Linux-Powered Enterprise Networks

Tick Launches Attack on East Asian Data-Loss Prevention Software Company

Microsoft fixed 83 vulnerabilities including two zero-day vulnerabilities

Revamped Prometei Botnet Version Infects Over 10,000 Systems

Adobe Addressed a Zero-day Vulnerability in ColdFusion 2021 and 2018

Malware Impersonating Websites Spread via Google Ads

APT 29 Launches Malevolent Campaign Targeting Governments

New YoroTrooper Threat Actor Targeting Government and Energy Organizations

BianLian ransomware ramps up data-leak extortion and improves operational security

Outlook Vulnerability Exploited by Russian Hackers Since April 2022

DotRunpeX Novel Injector Delivers Multiple Malware Strains

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.

REPORT GENERATED ON

March 20, 2023 • 6:00 AM

More at www.hivepro.com