Date of Publication
January 9, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

2 to 8 JANUARY 2023

Summary

Threat Actors

Hive Pro discovered two actors who have been active in the past week. The first, **Blind Eagle**, is a well-known Colombia threat actor known for information theft and espionage. The second, **Bluebottle**, is a cybercrime group that specializes in financial cyber operations. For further details, see the key takeaway section for Actors.

Attacks

We discovered that eight new malware strains have been active over the last week. Two of these were ransomware, with one being **CatB ransomware** and the other being **MacOS ransomware**. We also observed two remote access trojans (**PupyRAT** and **QuasarRAT**) and one SHC-compiled Linux malware. We even saw old malware, including **IcedID** and **GuLoader**. We also observed an **unidentified** strain of Linux malware and one more new **SHC-compiled** Linux malware. For more information, see the key takeaway section on Attacks

Vulnerabilities

Last week, we discovered seven vulnerabilities that organizations should prioritize. **Five** of these vulnerabilities are security flaws in the Fortinet products, and **one** is a vulnerability in a ZOHO ManageEngine product. Another **one** is in Synology VPN Plus Server. For further details, see 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

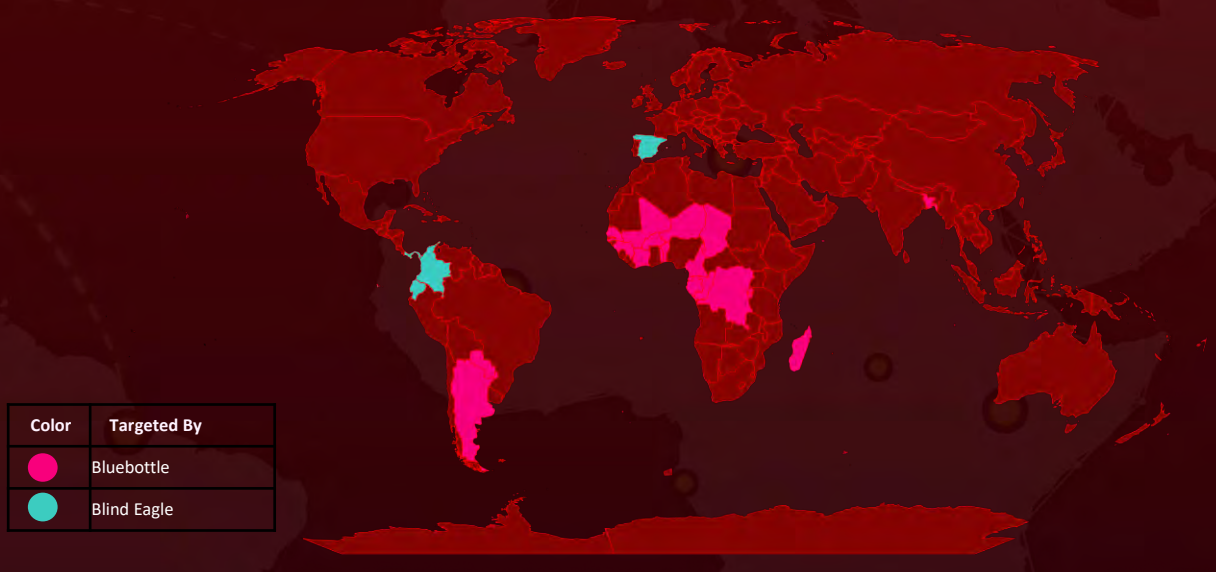
Blind Eagle (QuasarRAT)

Blind Eagle is a threat group that targets individuals in South American countries and uses spear-phishing campaigns to send malicious documents or links. These campaigns deploy a .Net executable written in LHA, which when unpacked reveals a modified version of QuasarRAT. This trojan is designed to access victims' financial accounts and the attack uses a multi-stage method involving the exploitation of mshta.exe and the downloading of Python scripts.

Bluebottle (unattributed)

Bluebottle is a cybercrime group that has been attacking banks in French-speaking African countries. Since at least mid-2019, the group has used various tactics, including living off the land, dual-use tools, and commodity malware, to steal at least $11 million in 30 targeted attacks. Bluebottle uses spear-phishing emails to deliver malware to victims, often disguised as job-related files or delivered in a ZIP file. The group's primary goal is to obtain sensitive data from the banks it targets.

Actor Map



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

Key Takeaways

Actor Details

ICON	NAME	ORIGIN	MOTIVE
	Blind Eagle (APT-C-36)	Colombia	Information theft and Espionage
	Bluebottle	Unknown	Financial Crime

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

Key Takeaways

Attacks

IcedID (unattributed)

The IcedID botnet has been distributing itself through malvertising attacks using Google pay-per-click ads since December 2022. In these attacks, keywords are hijacked to display malicious ads that trick users into downloading the malware. The new IcedID botnet loader is delivered through an MSI file, which drops several files and invokes a malicious loader routine through rundll32.exe.

Unidentified Malware (unattributed)

An unidentified strain of Linux malware is exploiting vulnerabilities in WordPress plugins to compromise sites by injecting malicious JavaScripts. These JavaScripts are run sequentially until one of them succeeds in compromising the site. The malware targets both 32-bit and 64-bit Linux systems and allows the attacker to execute commands remotely.

CatB Ransomware (unattributed)

CatB is a ransomware that uses DLL hijacking to evade detection. It injects itself into the Microsoft Distributed Transaction Coordinator (MSDTC) service, a legitimate Windows process, and uses that process to encrypt the victim's files. This makes it harder for security scanners to identify the ransomware, as it is not running as a standalone process and may not show the typical behavior of ransomware.

SHC-compiled Linux malware (unattributed)

A new strain of Linux malware that installs a CoinMiner has been discovered. This malware, which was developed using the Shc compiler, is thought to be spreading through dictionary attacks on poorly secured Linux SSH servers. After gaining access to a system, the malware installs various types of malware, including the Shc downloader, XMRig CoinMiner, and a Perl-based DDoS IRC Bot.

Pupy RAT (unattributed)

The Pupy RAT malware is using the technique of DLL side-loading to avoid detection by disguising itself as the legitimate WerFault.exe process. It is delivered through an ISO image that contains a malicious DLL file, a shortcut file, and an Excel file. When the shortcut file is opened, the WerFault.exe process is run, which then uses DLL side-loading to execute the malicious DLL file.

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

MacOS Ransomware(unattributed)

KeRanger, a ransomware discovered in 2016, was distributed through a compromised version of the popular BitTorrent client Transmission. In 2018, FileCoder, another ransomware, was distributed through malicious advertisements on websites. MacRansom, a ransomware discovered in 2019, is spread through malicious email attachments. And EvilQuest, a ransomware discovered in 2020, is distributed through malicious apps available for download on the internet. These ransomware are included in recent MacOS ransomware.

QuasarRAT (Blind Eagle)

QuasarRAT is a remote access trojan (RAT) that allows an attacker to remotely control and access a victim's computer. It can be used to steal sensitive information and perform various malicious activities. QuasarRAT is distributed through malicious email attachments, infected software installers, and compromised websites. It can record keystrokes, take screenshots, and execute arbitrary code.

GuLoader (Bluebottle)

GuLoader is a highly advanced malware downloader that was first detected in 2019. It uses polymorphic shellcode to bypass typical security measures and includes many anti-analysis measures, making it difficult to detect and defend against. GuLoader employs a multi-stage deployment strategy that includes a VBS dropper file, a bundled payload stored in the registry, and a PowerShell script. It also maps all embedded DJB2 hash values against every API used by the malware.

TOP MITRE ATT&CK TTPS:

T1204 User Execution	**T1027** Obfuscated Files or Information	**T1190** Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1036** Masquerading
T1588 Obtain Capabilities	**T1574** Hijack Execution Flow	**T1543** Create or Modify System Process	**T1518** Software Discovery	**T1486** Data Encrypted for Impact

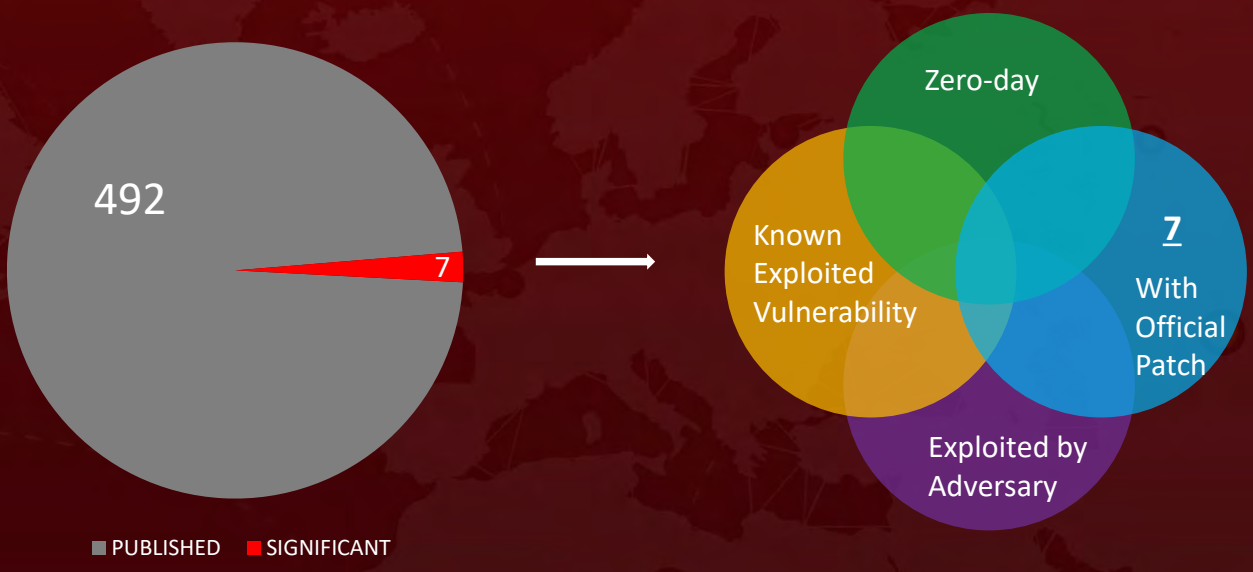
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Seven Notable Mentions

Among the seven vulnerabilities, one was found in ZOHO ManageEngine products, which is identified as CVE-2022-47523 and is an SQL injection vulnerability by an unauthenticated attacker. A vulnerability in Synology VPN Plus Server, named CVE-2022-43931 could allow attackers to execute arbitrary commands, launch denial-of-service (DoS) attacks, and read arbitrary files on affected systems. The remaining five vulnerabilities affect Fortinet products by execution of OS commands and drive-by-download attacks.



*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 **7 significant vulnerabilities** and block the indicators related to the threat actor **Blind Eagle, Bluebottle** and malware, **IcedID, SHC-compiled Linux malware, GuLoader, CatB, KeRanger, FileCoder, MacRansom, EvilQuest Ransomware,** and **Pupy RAT, QuasarRAT.**

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 **7 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware **IcedID, SHC-compiled Linux malware, GuLoader, CatB, KeRanger, FileCoder, MacRansom, and EvilQuest Ransomware,** and **Pupy RAT, QuasarRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

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

Malware Distribution via Google PPC by IcedID Botnet Distributors

Linux malware leverages plugin exploits to backdoor WordPress sites

Synology addresses the RCE vulnerability that affects VPN Plus servers

A New Emerging CatB Ransomware Using DLL Hijacking to Evade Detection

Several vulnerabilities are addressed by Fortinet across its product range

Threat Actors Using WerFault.exe to Deploy Pupy RAT

Linux Malware Using SHC Compiler Installs CoinMiner and DDoS Bots

Zoho Addresses SQL Injection Vulnerability in ManageEngine Products

Blind Eagle Hackers resurfaced with a formidable infection chain

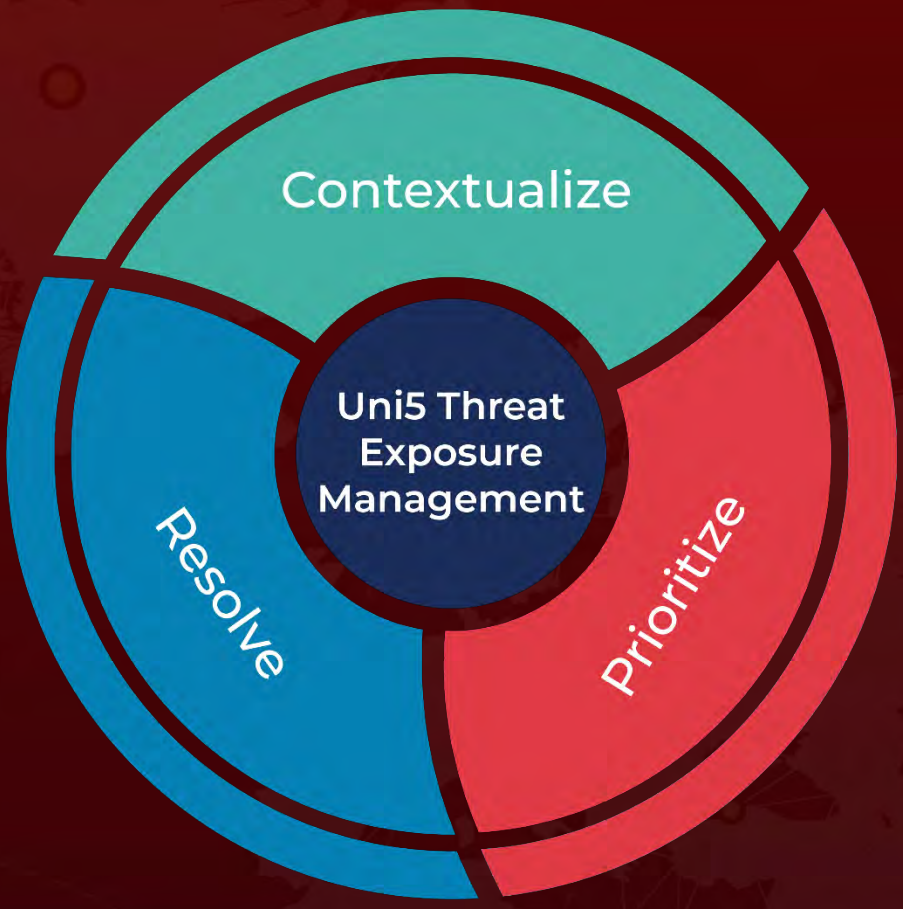
Bluebottle Group Continues Attacks on Banks in Francophone Africa

The Dangers of macOS Ransomware A Closer Look at KeRanger, FileCoder, MacRansom, and EvilQuest

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

January 09, 2023 • 6:00 AM

More at www.hivepro.com