Date of Publication
January 23, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Actors, Attacks, and Vulnerabilities

16 to 22 JANUARY 2023

Summary

Threat Actors

Hive Pro identified three active actors during the past week. The first, **Earth Bogle**, is a notable threat actor known for information theft and espionage. The second, **Kasablanka**, is a Morocco-based cybercrime group that specializes in information theft and espionage. The third actor identified is **APT15**. For more information, refer to the "Actors" section for key takeaways.

Attacks

Last week, we identified seven new malware strains that were active. Five of these were Remote Access Trojans (RATs), namely **NetSupport RAT**, **NjRAT**, **Warzone RAT**, **Loda RAT** and **Orcus RAT**. We also discovered one **Rhadamanthys Stealer** being offered as "Malware-as-a-Service" (MaaS). Additionally, we identified two new malware: **BOLDMOVE Malware** and **Turian Backdoor**. For additional information, please refer to the "Attacks" section for key takeaways.

Vulnerabilities

Last week, we identified 12 vulnerabilities that organizations should be aware of. One of them is the vulnerability (**CVE-2022-47966**) in ManageEngine products which can allow for remote code execution and potential control of the compromised system. Another one is a Chrome vulnerability (**CVE-2022-3656**) which exposes the data of 2.8 billion users. 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

Earth Bogle (NjRAT)

Earth Bogle is a threat group actively spreading malware through public cloud storage sites such as files.fm and failiem.lv, as well as through compromised web servers. The malware, known as NjRAT, is used to gain unauthorized access and control over victim devices. Once installed, NjRAT allows attackers to perform various intrusive actions on compromised devices.

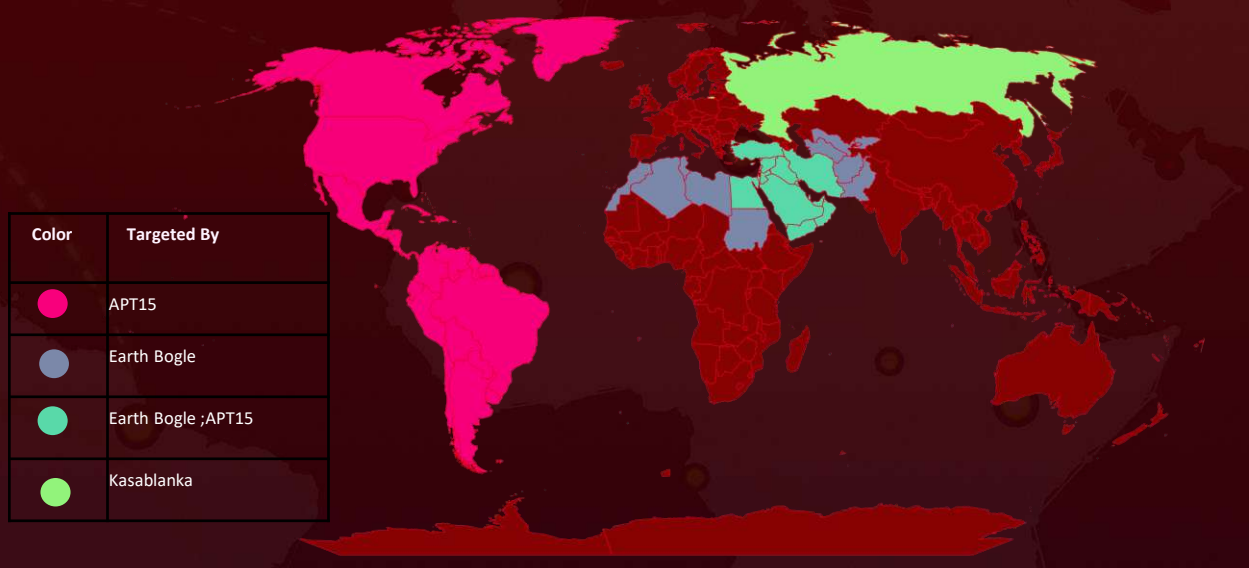
Kasablanka (Warzone & Loda RAT)

The Kasablanka group is a cyber-criminal organization that has specifically targeted Russia between September and December 2022, using various payloads delivered through phishing emails containing socially engineered lnk files, zip packages, and executables attached to virtual disk image files. The group initially employed the commercial Trojan Warzone RAT during early stages of the attack, later switching to Loda RAT.

APT15 (Turain Backdoor)

APT15 is a Chinese cyber espionage group that launches advanced persistent threat attacks. They have updated their Turian backdoor and targeted government and diplomatic organizations in North and South America, Africa, and the Middle East.

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
	Earth Bogle	Unknown	Information theft and Espionage
	Kasablanka	Morocco	Information theft and Espionage
	APT15 (Playful Taurus,BackdoorDiplomacy, Vixen Panda, KeChang, and NICKEL)	China	Information theft and Espionage

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

Key Takeaways

Attacks

Rhadamanthys Stealer (unattributed)

Rhadamanthys Stealer is a recently discovered and still active malware strain that is being marketed as "malware-as-a-service" (MaaS). It spreads through Google Ads, leading victims to phishing websites that mimic popular software such as Zoom, AnyDesk, Notepad++, and Bluestacks. Additionally, it can also be distributed through spam emails containing malicious attachments.

NetSupport RAT (unattributed)

NetSupport Manager is a remote control tool that can be used by ordinary or corporate users to remotely control systems, but it is being abused by threat actors as it allows external control over specific systems. NetSupport RAT has been observed in numerous attacks on enterprise environments over the years, and Pokemon is just the latest in a long line of creative lures used to distribute and drop NetSupport RAT.

NjRAT (Earth Bogle)

NjRAT, also known as Bladabindi, a remote access trojan (RAT) malware discovered in 2013, used to gain unauthorized access and control over victim devices. It allows attackers to perform various intrusive operations on compromised devices.

Warzone RAT and Loda RAT (Kasablanka)

Warzone RAT and Loda RAT are both types of malware known as Remote Access Trojan (RAT). Both RATs can be used to gain unauthorized access and control over a victim's computer. They allow attackers to steal sensitive information, monitor the infected device, and perform other malicious actions. They can be spread through phishing emails, malicious websites, and infected software downloads.

Turian Backdoor (APT15)

Turian is a backdoor malware that allows an attacker to gain unauthorized access and control over an infected device. The Turian malware is known for being used in targeted attacks and it is able to evade detection by using several persistence mechanisms and anti-debugging techniques. It can be used for various malicious activities such as stealing sensitive information, monitoring the infected device and exfiltrating data. It is typically distributed through spear-phishing emails, infected software and drive-by downloads.

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

BOLDMOVE Malware (unattributed)

BOLDMOVE is a malware that has been identified in a recent attack. It is written in C and has both Windows and Linux variants, with the latter being specifically designed to run on Fortinet devices. It is believed to have been used to gain access to targeted networks without any victim interaction, allowing the attackers to control the timing of the operation and reduce the chances of detection.

Orcus RAT (unattributed)

Orcus RAT is a Remote Access Trojan (RAT) malware that allows an attacker to remotely control infected systems. Recently, a variant of Orcus RAT has been found to be distributed along with XMRig CoinMiner disguised as a cracked version of Hangul Word Processor 2022 in an ongoing campaign. The malware was distributed via file-sharing sites. Orcus RAT is a dangerous malware that can steal sensitive information and perform other malicious actions.

TOP MITRE ATT&CK TTPS:

T1059 Command and Scripting Interpreter	**T1056** Input Capture	**T1204** User Execution	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1071 Application Layer Protocol	**T1068** Exploitation for Privilege Escalation	**T1055** Process Injection	**T1547** Boot or Logon Autostart Execution	**T1486** Data Encrypted for Impact
T1027 Obfuscated Files or Information	**T1049** System Network Connections Discovery	**T1036** Masquerading	**T1203** Exploitation for Client Execution	**T1509** Non-Standard Port

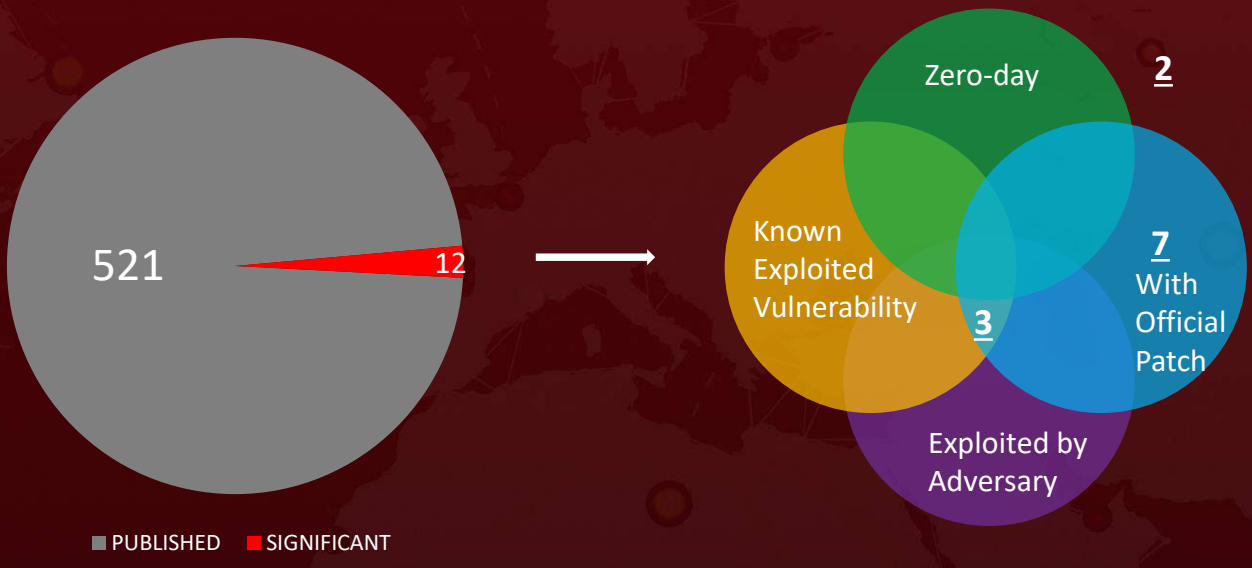
*for detailed insights on each of the actors, attacks, vulnerabilities, targeted locations, and sectors click on the highlighted phrase.

Key Takeaways

Vulnerabilities

Twelve Notable Mentions

Out of the 12 vulnerabilities, one (CVE-2022-46169) was discovered in Cacti and allows for command injection and remote code execution. Two vulnerabilities were found in Cisco small business routers, which allow for bypassing authentication and executing arbitrary commands on the affected device's operating system. Another vulnerability (CVE-2022-47966) in ManageEngine products allows for remote code execution and potential control of the compromised system. A Chrome vulnerability (CVE-2022-3656) exposes the data of 2.8 billion users. GitLab addressed two new CE and EE vulnerabilities. Additionally, an unauthenticated remote code execution vulnerability in Control Web Panel (CWP) could allow attackers to run arbitrary operating system commands.



*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 **12 significant vulnerabilities** and block the indicators related to the threat actor **Earth Bogle, Kasablanka, APT15** and malware, **Rhadamanthys Stealer, BOLDMOVE Malware, Turian Backdoor, NetSupport RAT, NjRAT, Warzone RAT, Loda RAT,** and **Orcus RAT.**

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 **12 significant vulnerabilities**
- Testing the efficacy of their security controls by simulating the attacks related to and malware **Rhadamanthys Stealer, BOLDMOVE Malware, Turian Backdoor, NetSupport RAT, NjRAT, Warzone RAT, Loda RAT, and Orcus RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

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

Google Chrome Vulnerability Exposes Data of 2.5 Billion Users

NetSupport RAT employs phishing campaigns that incorporate Pokemon lures

Middle East targeted by Earth Bogle using NjRAT malware

GitLab releases new CE and EE versions to address integer overflow vulnerabilities

Kasablanka Group Launches Phishing Campaigns Targeting Russian Government Entities

APT15 enhanced its arsenal with an updated variant of the Turian backdoor

New BOLDMOVE Backdoor uses FortiOS vulnerability for initial access

Korean Word Processor Scam Alert Orcus RAT Lurking in Cracked Versions

Control Web Panel OS Command Injection Exploitation Increases After POC Release

Rhadamanthys: A New Evasive Information Stealer

A Critical Vulnerability That Affects ManageEngine Products

Cisco Small Business Routers Vulnerable to Authentication Bypass and Remote Code Execution

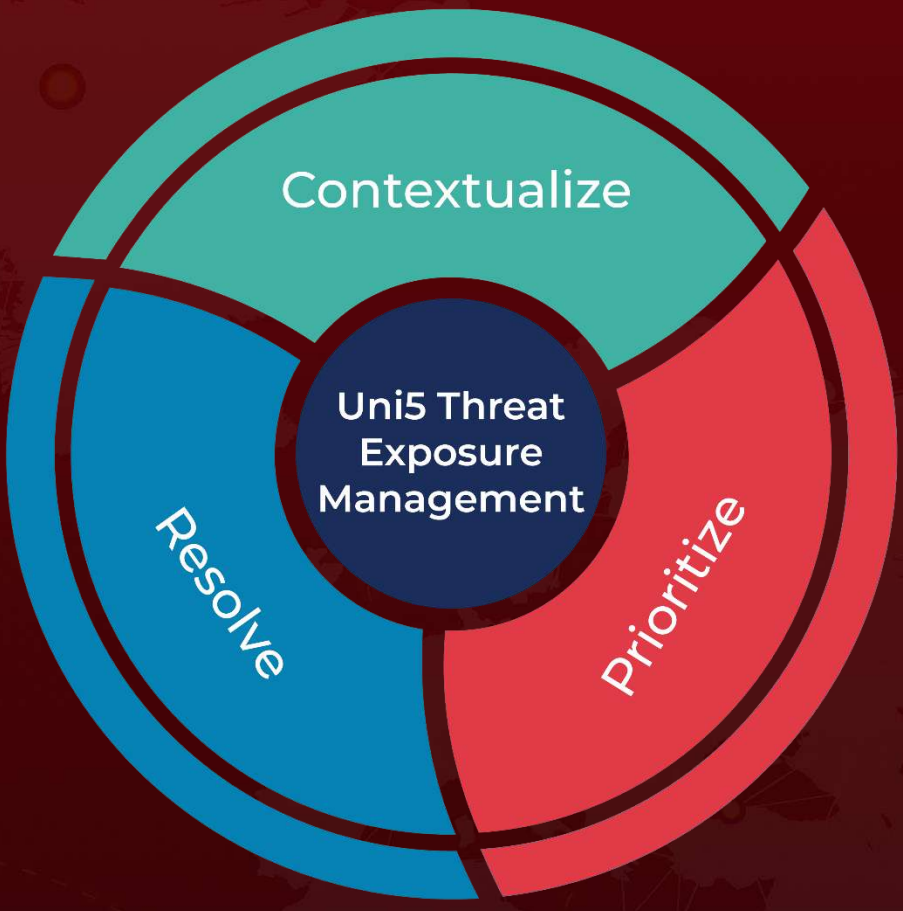
The Vulnerability Discovered in the Cacti Open-Source RRD tool

A new EmojiDeploy attack has been found in an Azure service

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 23, 2023 • 5:00 AM

More at www.hivepro.com