ThreatMon

Behind the Breaches

Mapping Threat Actors and their CVE Exploits

@threatmon

@MonThreat

Table of Contents

Introduction

The threat landscape of the cybersecurity industry is constantly evolving, and one of the major risks faced by organizations today is the exploitation of known vulnerabilities by advanced persistent threats (APTs) and ransomware groups. In recent years, we have seen a surge in the number of reported attacks and data breaches caused by these threat actors, highlighting the importance of vulnerability management as a critical component of any cybersecurity strategy.

One of the key challenges in managing vulnerabilities is understanding which ones are most likely to be targeted by attackers. This requires a deep understanding of the tactics, techniques, and procedures (TTPs) used by different APTs and ransomware groups, as well as their preferred methods of exploitation. By analyzing the historical data on past attacks, we can identify trends and patterns in these threat actors' behavior, which can help us better anticipate and prevent future attacks.

This report aims to provide insights into the exploitation habits of various APTs and ransomware groups in the past, with a focus on their use of known vulnerabilities.

What is a CVE?

A CVE, or Common Vulnerabilities and Exposures, is a unique identifier assigned to a publicly disclosed vulnerability in software or hardware. The CVE system was created to provide a standardized way of identifying and tracking known vulnerabilities across different organizations and tools, making it easier for security professionals to exchange information about vulnerabilities and prioritize their response efforts.

Each CVE entry includes a brief description of the vulnerability, information about the affected software or hardware, and details on the severity and impact of the vulnerability. CVE entries are assigned by the CVE Numbering Authority (CNA), a group of organizations and individuals authorized by the CVE Program to assign and manage CVE IDs.

By referencing CVEs in their security advisories and vulnerability disclosures, security researchers, vendors, and other stakeholders can ensure that they are using a common language to describe and track vulnerabilities, which helps to improve the overall security of software and hardware systems.

Who are these Threat Actors?

In the context of cybersecurity, a threat actor refers to an individual, group, or organization that carries out malicious activities with the intention of compromising the confidentiality, integrity, or availability of a target system or network.

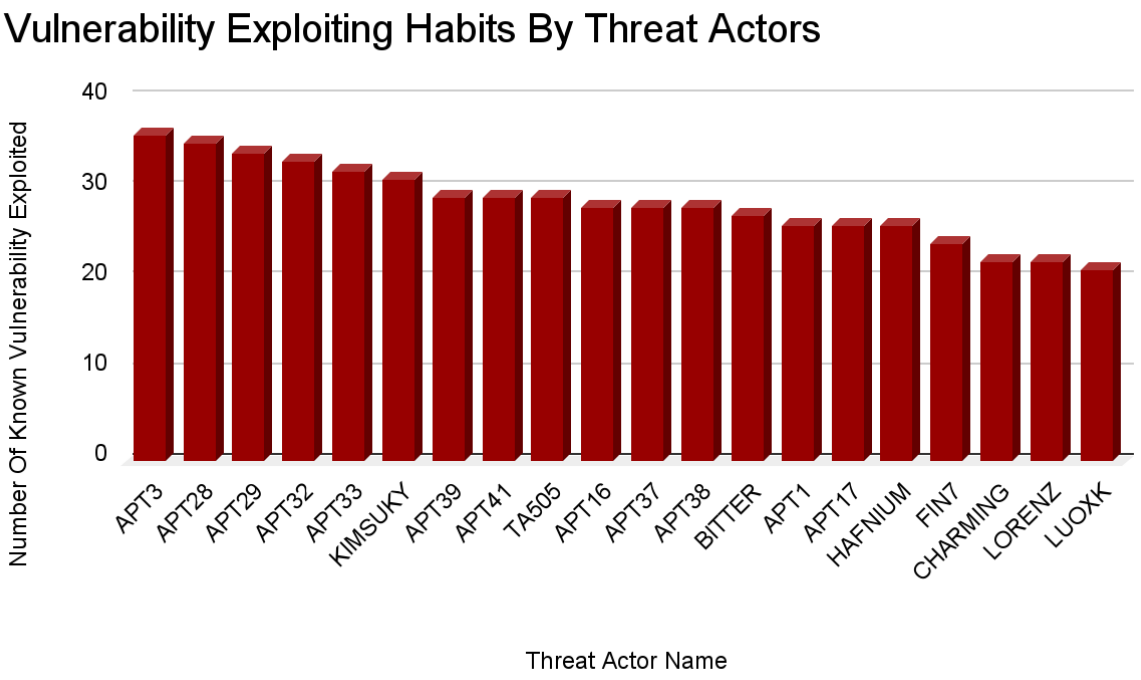
Advanced Persistent Threats (APTs) are typically state-sponsored threat actors that conduct long-term, targeted attacks against specific organizations or individuals, often using sophisticated tactics and techniques to evade detection and gain access to sensitive information. APTs are known for their persistence, which allows them to remain undetected in a target environment for extended periods of time, enabling them to carry out their objectives without being discovered.

Ransomware groups, on the other hand, are typically criminal organizations that use malicious software to encrypt a victim's files and demand a ransom payment in exchange for the decryption key. These groups often target organizations in order to maximize the potential payout from a successful attack, and they may use a variety of tactics to gain access to a target system, including phishing emails, exploit kits, and compromised credentials.

Both APTs and ransomware groups are motivated by different objectives - APTs may be driven by political or economic espionage, while ransomware groups are motivated by financial gain. However, they both pose a significant threat to organizations, and their activities can result in serious consequences, including financial losses, reputational damage, and legal and regulatory sanctions.
It is important for organizations to understand the TTPs and motivations of these threat actors in order to develop effective strategies for preventing and responding to their attacks.

Vulnerability Exploiting Habits by Threat Actors

The report is started by first examining the vulnerability exploiting habits of threat actors. The chart below displays the top 20 threat actors that are most matched with CVEs.



At the top of the list of Threat Actors that like to exploit known vulnerabilities are APT3, APT28, and APT29. Now, let's briefly get to know these Threat Actors.

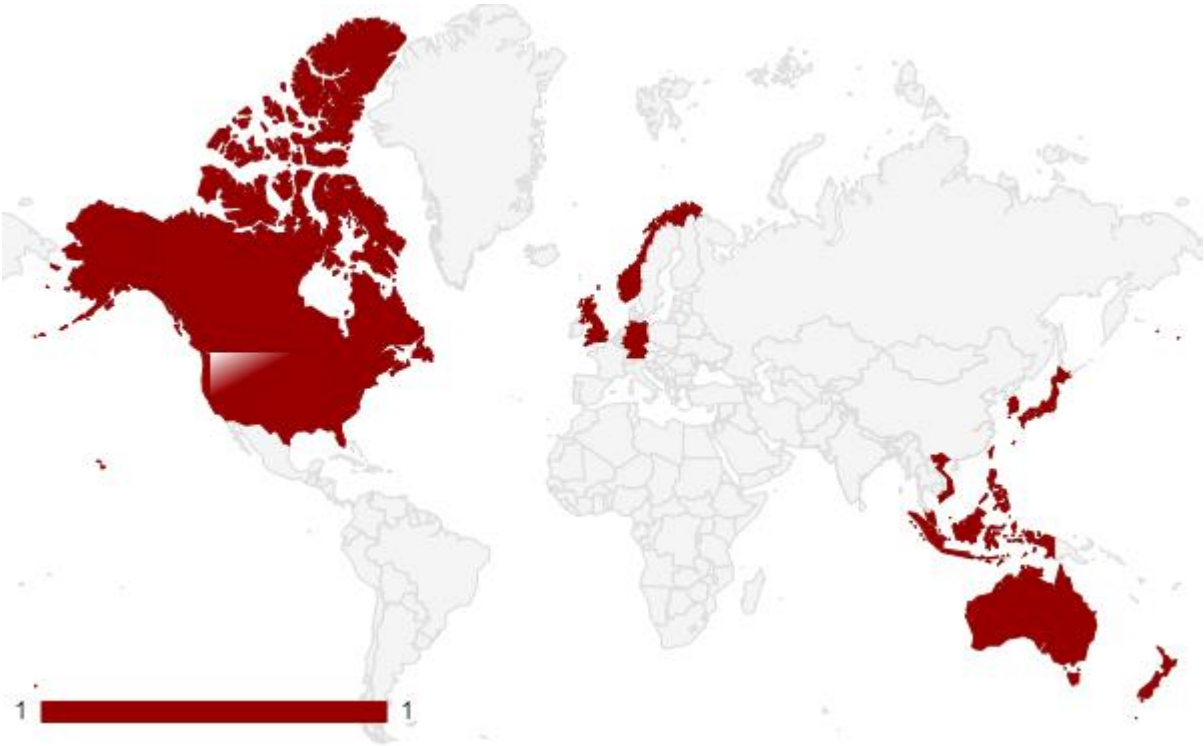
APT3 (aka Gothic Panda)

APT3 is a China-based threat group that researchers have attributed to China's Ministry of State Security. This group is responsible for the campaigns known as Operation Clandestine Fox, Operation Clandestine Wolf, and Operation Double Tap. As of June 2015, the group appears to have shifted from targeting primarily US victims to primarily political organizations in Hong Kong.

Aliases: Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0010, TG-0110

TTPs: See it in MITRE ATT&CK Navigator

Vulnerabilities Exploited: CVE-2017-0199, CVE-2021-24098, CVE-2014-6332, CVE-2019-0703, CVE-2017-0143, CVE-2021-36483



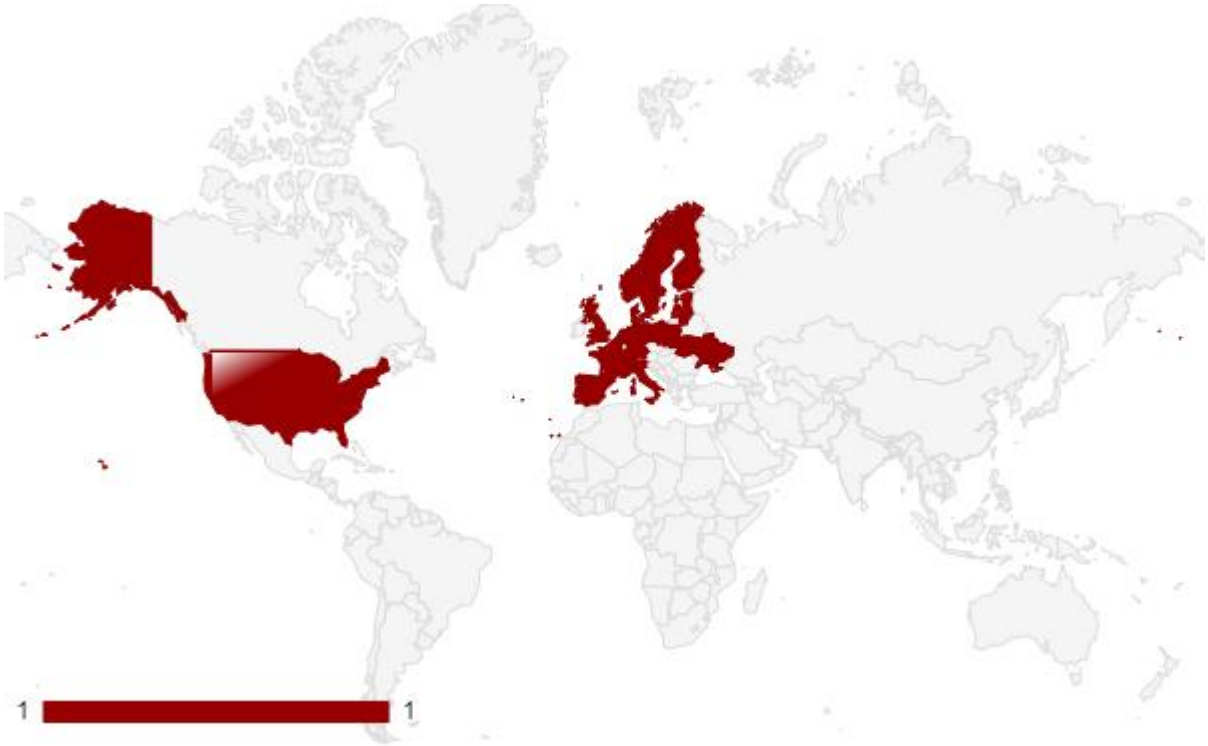
APT28 (aka IRON TWILIGHT)

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.This group has been active since at least 2004.

Aliases: IRON TWILIGHT, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

TTPS: See it in MITRE ATT&CK Navigator

Vulnerabilities Exploited: CVE-2017-0199, CVE-2021-36926, CVE-2021-26425, CVE-2021-34532, CVE-2014-4114, CVE-2016-1247, CVE-2016-0189, CVE-2021-34536, CVE-2021-34537, CVE-2021-26423, CVE-2020-1927



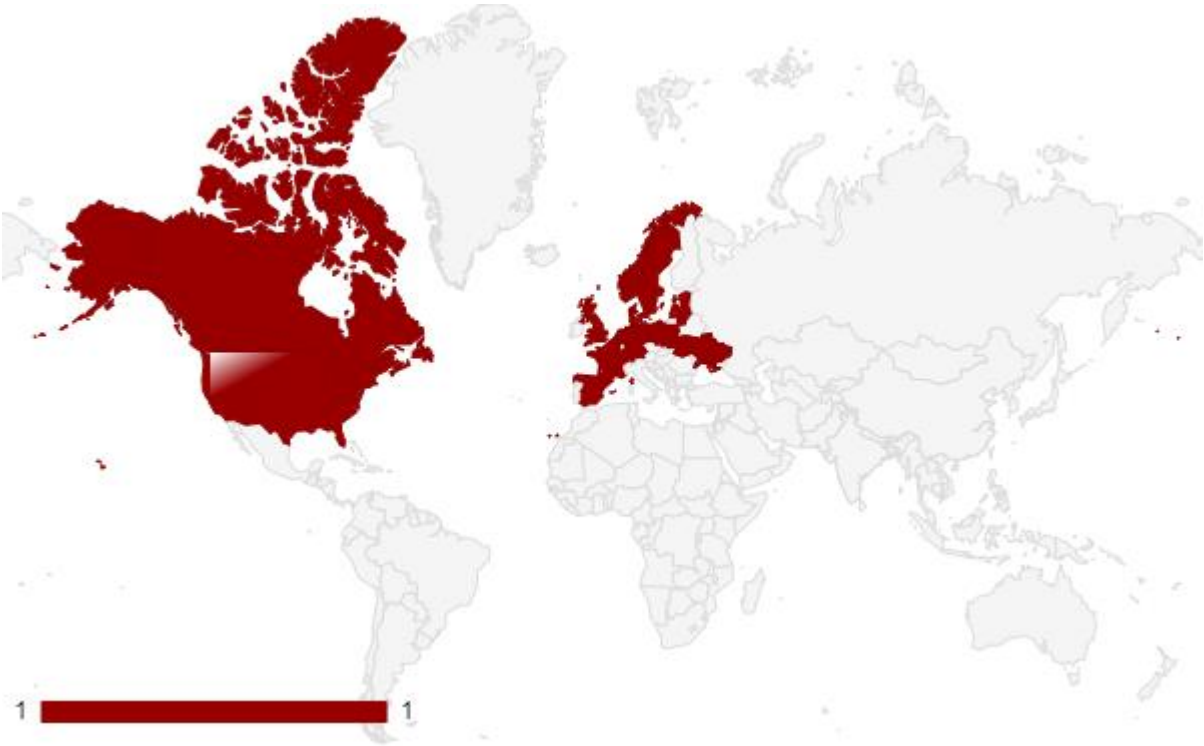
APT29 (aka NOBELIUM)

APT29 is a threat group that has been attributed to Russia's Foreign Intelligence Service (SVR). They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.

Aliases: IRON RITUAL, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke

TTPS: See it in MITRE ATT&CK Navigator

Vulnerabilities Exploited: CVE-2021-1647, CVE-2022-32060, CVE-2022-34160, CVE-2022-28624, CVE-2022-2191, CVE-2017-0199, CVE-2018-8589, CVE-2017-0143



Vulnerability Exploiting Habits of Well-Known Threat Actors

Some of the well-known threat actors and their habits of exploiting known vulnerabilities will now be examined.

LockBit

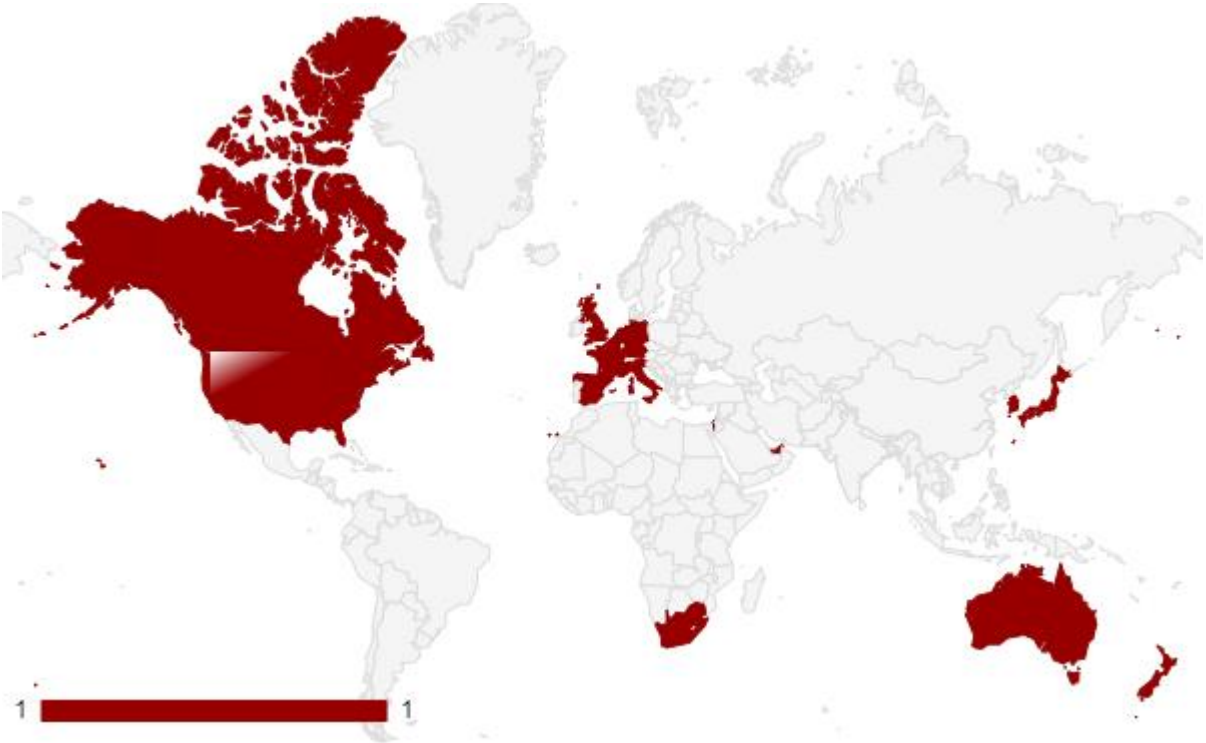
The LockBit Group is a cybercriminal organization that operates a sophisticated ransomware-as-a-service (RaaS) platform called LockBit. The group has been active since at least 2019 and is known for targeting large organizations with ransomware attacks.

Aliases: ABADDON ,Bysus Group,The Dark Side, HelloKitty, Ragnarok, Thanos Ransomware

Tools: Lockbit, Lockbit 2.0, Lockbit 3.0, Cobalt Strike, Mimikatz, Powershell Empire

Vulnerabilities Exploited: CVE-2021-30116, CVE-2021-21985, CVE-2021-3129, CVE-2019-19781, CVE-2018-8453

Track LockBit's Activities: [ThreatMon Ransomware Monitoring]



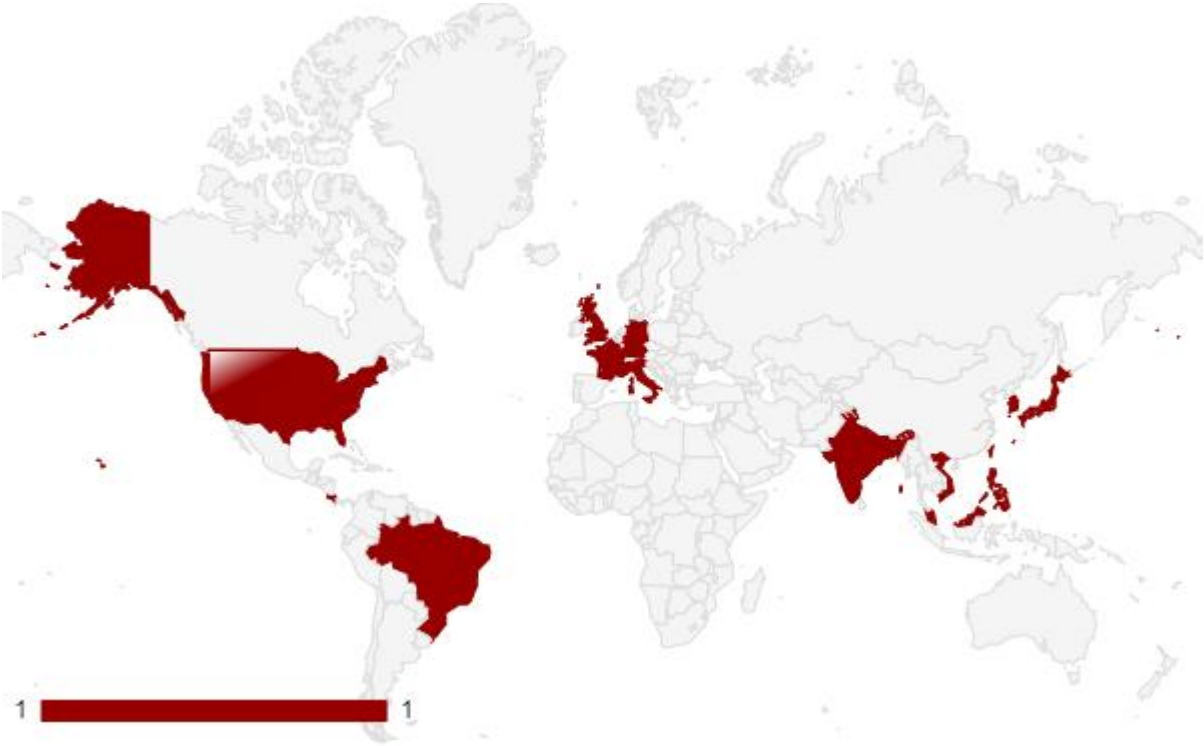
Lazarus Group

Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.

Aliases: Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY

TTPS: See it in MITRE ATT&CK

Vulnerabilities Exploited: CVE-2017-0199, CVE-2018-8174, CVE-2018-4878, CVE-2019-0803, CVE-2019-0859, CVE-2020-1380



Conti

Conti Group is a ransomware group that has been active since late 2019. The group is known for using sophisticated tactics and techniques to carry out ransomware attacks against organizations, including using custom-built malware, exploiting vulnerabilities, and stealing sensitive data before encrypting victim's files.

Aliases: Wizard Spider, TA505 (some sources use this alias to refer specifically to the affiliates or sub-group associated with Conti, rather than the Conti Group itself), Silent Night, Blockbuster, StellarParticle

Tools: Cobalt Strike, Mimikatz, AdFind and BloodHound

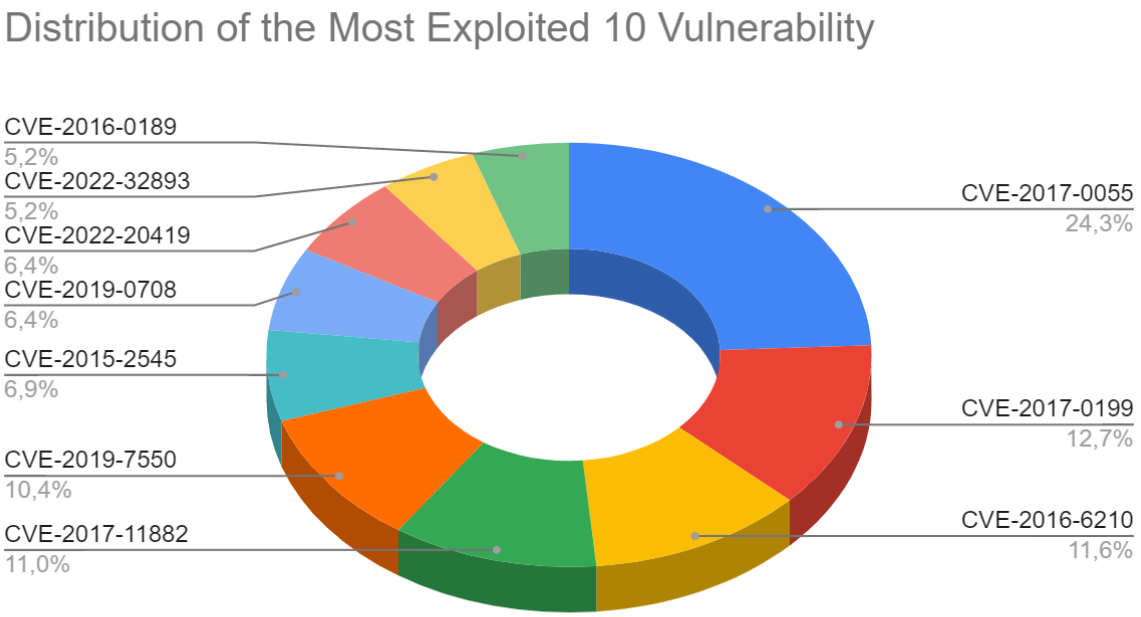
Vulnerabilities Exploited: CVE-2020-1472, CVE-2021-21972, CVE-2021-20016, CVE-2019-19871

Track Conti's Activities: [ThreatMon Ransomware Monitoring]

ThreatMon conducts APT attack simulations and alerts you before Threat Actor's attack. For more : [https://threatmon.io/apt-attack-tests/]

Most Exploited Vulnerabilities

The distribution of the 10 most exploited vulnerabilities is seen here, and some of these vulnerabilities will be examined.



CVE-2017-0055

This is a vulnerability in Microsoft Edge's HTML and JavaScript engines that could allow an attacker to execute arbitrary code in the context of the current user. The vulnerability is caused by the way the browser handles objects in memory.

CVSS V3 Score: 6.1
Attack Vector: Network
MITRE ATT&CK ID: T1134

CVE-2017-0199

This is a remote code execution vulnerability in Microsoft Office that allows attackers to execute arbitrary code on a victim's machine by tricking them into opening a malicious document or webpage.

CVSS V3 Score: 7.8
Attack Vector: Local
MITRE ATT&CK ID: T1204

CVE-2016-6210

This is a vulnerability in the OpenSSH client that could allow an attacker to bypass authentication and gain access to a vulnerable system. The vulnerability is caused by a flaw in the way the client handles challenge-response authentication.

CVSS V3 Score: 5.9
Attack Vector: Network
MITRE ATT&CK ID: T1078

CVE-2017-11882

This is a vulnerability in Microsoft Office's Equation Editor component that allows attackers to execute arbitrary code on a victim's machine by tricking them into opening a malicious document.

CVSS V3 Score: 7.8
Attack Vector: Local
MITRE ATT&CK ID: T1204

CVE-2019-7550

This is a vulnerability in the runc command-line tool used by Docker and other containerization systems that allows an attacker to escalate privileges and gain access to the host system.

CVSS V3 Score: 5.3
Attack Vector: Network
MITRE ATT&CK ID: T1190

CVE-2015-2545

This is a vulnerability in the Microsoft Office Access Connectivity Engine that could allow an attacker to execute arbitrary code on a victim's machine by tricking them into opening a specially crafted file.

CVSS V3 Score: N/A
Attack Vector: Local
MITRE ATT&CK ID: T1204

CVE-2019-0708

Also known as BlueKeep, this is a critical remote code execution vulnerability in Microsoft's Remote Desktop Services that allows attackers to execute code on vulnerable systems without user interaction.

CVSS V3 Score: 9.8
Attack Vector: Network
MITRE ATT&CK ID: T1071

CVE-2022-20419

This is a vulnerability in the HP System Management Homepage (SMH) that could allow an unauthenticated attacker to execute arbitrary code on a vulnerable system.

CVSS V3 Score: 7.3
Attack Vector: Local
MITRE ATT&CK ID: T1204

CVE-2022-32893

This is a remote code execution vulnerability in the Apache Struts web application framework that could allow attackers to execute arbitrary code on a vulnerable system.

CVSS V3 Score: 8.8
Attack Vector: Network
MITRE ATT&CK ID: T1203

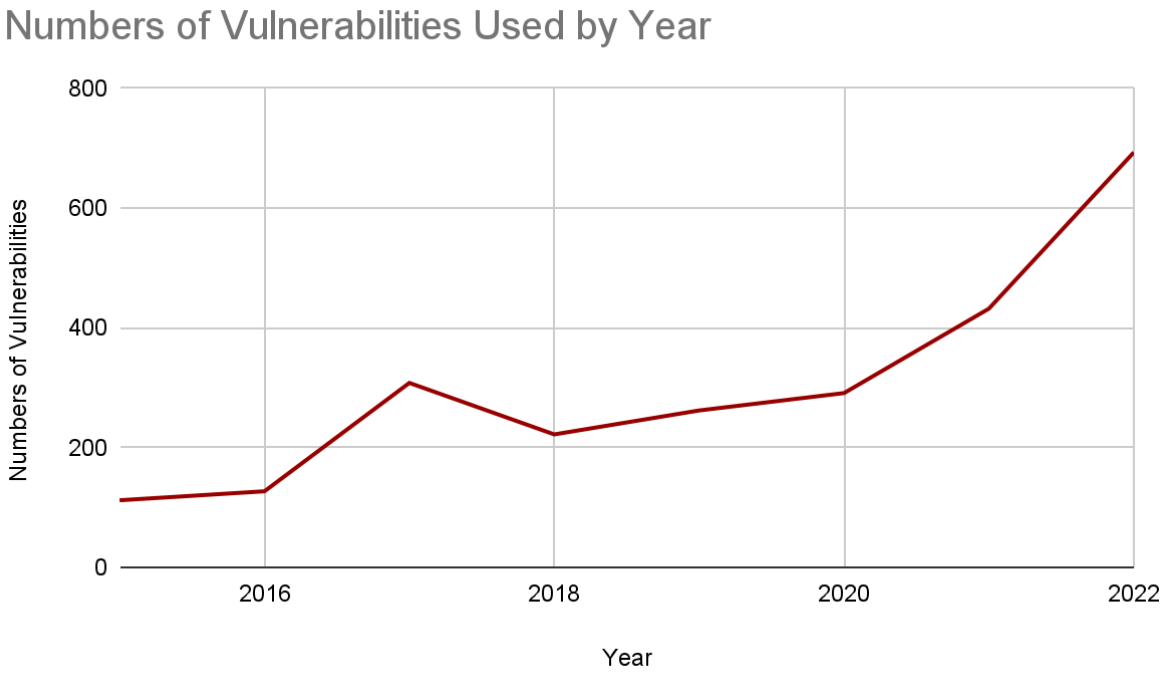
CVE-2016-0189

This is a vulnerability in Microsoft Internet Explorer's scripting engine that could allow an attacker to execute arbitrary code on a victim's machine by tricking them into visiting a malicious website.

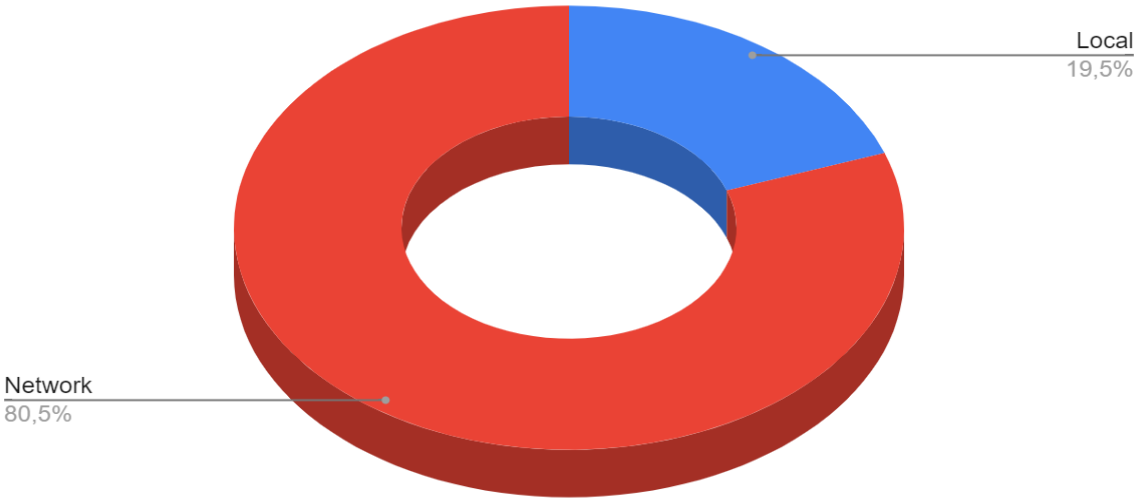
CVSS V3 Score: 7.5
Attack Vector: Network
MITRE ATT&CK ID: T1203

Examination of Data According to CVEs

When the data from 2015 is examined, an **increase** in the usage of CVEs is observed **every year**, with an additional increase being observed only in 2017.



When the distribution of the attack vectors of the exploited vulnerabilities is examined, it is seen that the ones that are exploited **remotely** are in the majority. Thus, it can be summarized **network based** that CVEs are generally used in order to gain initial access.



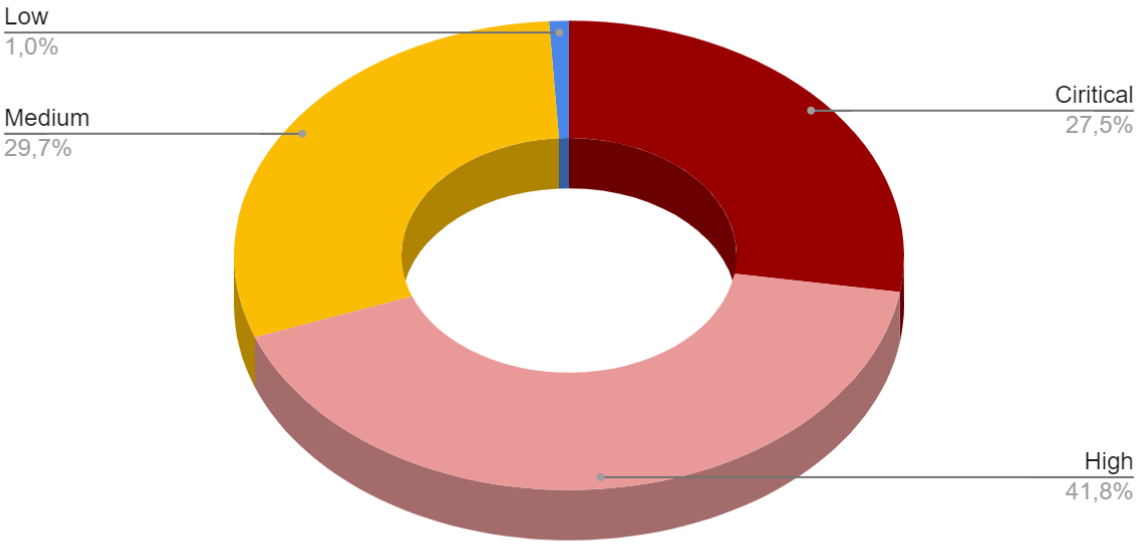
Local attack vector: A local attack vector requires the attacker to have physical access to a device or be able to execute code on the targeted device. For example, a malicious insider or a malware infection on a user's device could be considered a local attack vector.

Network attack vector: A network attack vector occurs when an attacker can exploit a vulnerability in a network-connected device or software to gain access to the device or network remotely. For example, an attacker may use a remote code execution exploit to take over a device or launch a phishing attack to trick users into revealing their login credentials.

So what should be done for mitigation? ThreatMon protects you. ThreatMon, monitors all your assets in real-time, and by detecting the current versions it determines the vulnerabilities in your systems.

For more : https://threatmon.io/vulnerability-intelligence/

When the **severity distributions** of exploited vulnerabilities are examined, it is seen that, as expected, low severity ones are not used much and high severity ones are in the majority.



Glossary and References

ATT&CK: MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is maintained by the MITRE Corporation

ATT&CK Navigator: ATT&CK Navigator is a tool that allows security teams to interactively explore the knowledge base of MITRE ATT&CK.

Cobalt Strike: Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors.
Mitigations and More: https://attack.mitre.org/software/S0154/

Mimikatz: Mimikatz is a credential dumper capable of obtaining plaintext Windows account logins and passwords, along with many other features that make it useful for testing the security of networks.
Mitigations and More: https://attack.mitre.org/software/S0002/

AdFind: AdFind is a free command-line query tool that can be used for gathering information from Active Directory.
Mitigations and More: https://attack.mitre.org/software/S0552/

BloodHound: BloodHound is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.
Mitigations and More: https://attack.mitre.org/software/S0521/

LockBit 3.0: Lockbit is a type of ransomware that encrypts files on an infected system and demands a ransom payment from the victim in exchange for the decryption key. LockBit 3.0 is the latest version of it.
Mitigations and More : https://blogs.vmware.com/security/2022/10/lockbit-3-0-also-known-as-lockbit-black.html

PowerShell Empire: PowerShell Empire is an open-source post-exploitation framework used for penetration testing and offensive security purposes.
Detecting and Mitigations : https://sansorg.egnyte.com/dl/4mdnX7hSOV

- https://attack.mitre.org/
- https://attack.mitre.org/groups/G0022/
- https://attack.mitre.org/groups/G0032/
- https://attack.mitre.org/groups/G0007/
- https://attack.mitre.org/groups/G0016/
- https://malpedia.caad.fkie.fraunhofer.de/details/win.lockbit
- https://malpedia.caad.fkie.fraunhofer.de/details/win.conti
- https://vuldb.com/?actor

ThreatMon

45305 Catalina cs St 150, Sterling VA 20166