SYNRADAR VULNERABILITY THREAT REPORT

AUGUST 2023

Prepared By SynRadar

Amigosec Consulting Pvt Ltd

info@synradar.com

Vulnerability Threat Report

[1st August 2023 – 28th August 2023]

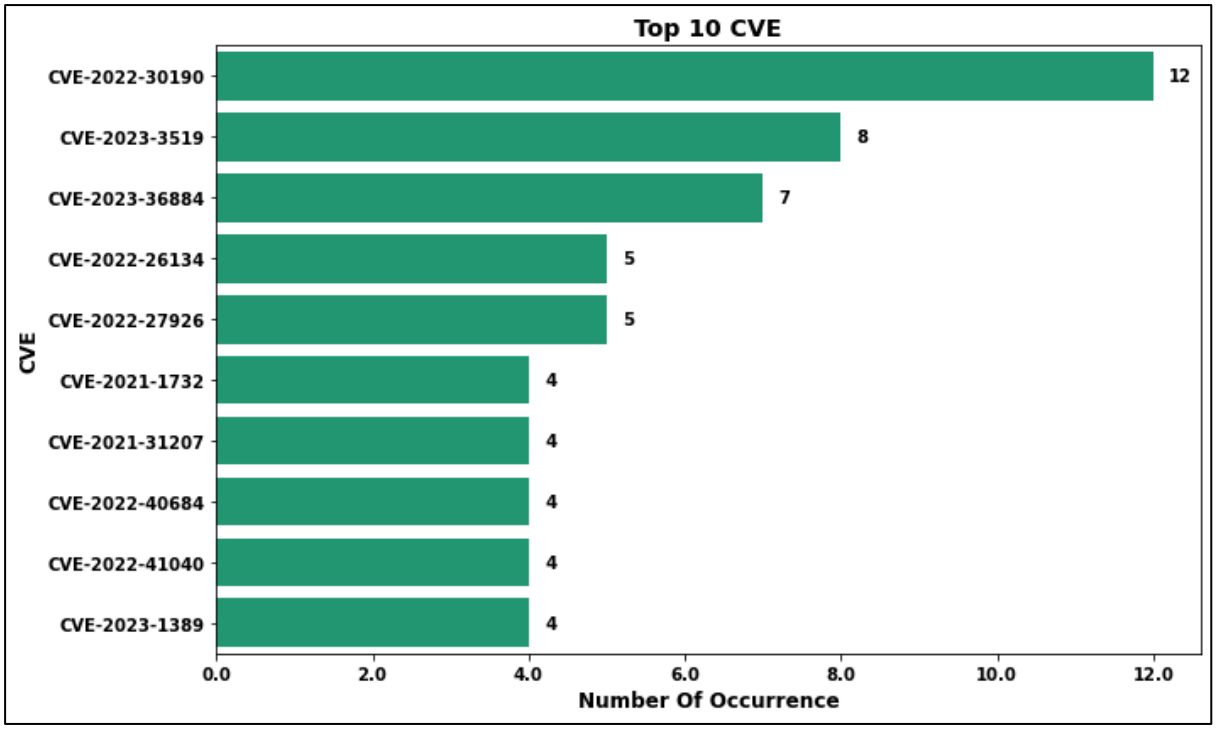
This is our monthly Threat Report for the month – August 2023. It illustrates Top 10 CVEs exploited in these months by Threat Actors. This report has been generated by enumerating threat feeds, and analysing the CVEs that are targeted by the threat actors. This report is intended to help Vulnerability Management teams to prioritize their remediation plan.

Contact info@synradar.com for queries & more information.

TOPICS

TOP TARGETED CVE LIST

Top Targeted CVEs in this period:



CVE-2022-30190

Description: Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability.

CVSS Score Version 3.x: 7.8 HIGH

CWE: CWE-610 (Externally Controlled Reference to a Resource in Another Sphere)

Patch: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
Cobalt Strike	T1566
LokiBot	T1137, T1027, T1566, T1137.001
RomCom	T1598.002
SpyNote	T1555, T1003

Targeted Countries by Threat: Ukraine, Japan, Sweden, China

Targeted Sector by Threat: Financial, Critical Infrastructure, Energy, Technology, Healthcare.

CVE-2023-3519

Description: Unauthenticated remote code execution

CVSS Score Version 3.x: 9.8 CRITICAL

CWE: CWE-94 (Improper Control of Generation of Code ('Code Injection'))

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Mitre ATT&CK Technique ID related to CVE: T1027.009, T1564.009, T1027.006

Threat	MITRE ATT&CK Technique
APT29	T1190, T1505.003, T1548.001, T1036.008, T1552.001, T1552.004

Targeted Countries by Threat: France, Bangladesh, Germany, Italy, India, Russian Federation, Japan, Switzerland, China

Targeted Sector by Threat: Foreign, Government, Critical Infrastructure

CVE-2023-36884

Description: Windows Search Remote Code Execution Vulnerability

CVSS Score Version 3.x: 7.5 HIGH

Patch: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
Industrial Spy	T1566, T1027
RomCom	T1555
Storm-0978	T1003

Targeted Countries by Threat: Belarus, United States of America, Ukraine, Viet Nam, Bulgaria, China

Targeted Sector by Threat: Education, individuals, Tactical, Healthcare, Telecommunications, Finance.

CVE-2022-26134

Description: In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.

CVSS Score Version 3.x: 9.8 CRITICAL

CWE: CWE-917 (Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection'))

Exploit: http://packetstormsecurity.com/files/167430/Confluence-OGNL-Injection-Remote-Code-Execution.html, http://packetstormsecurity.com/files/167449/Atlassian-Confluence-Namespace-OGNL-Injection.html

Patch: https://jira.atlassian.com/browse/CONFSERVER-79016

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
Cobalt Strike	T1210, T1203, T1505
TAC-040	T1055, T1555.003, T1560, T1426

Targeted Countries by Threat: Japan, United States of America

Targeted Sector by Threat: Critical Infrastructure, Technology, Financial, Energy, individuals, environmental and agriculture

CVE-2022-27926

Description: A reflected cross-site scripting (XSS) vulnerability in the /public/launchNewWindow.jsp component of Zimbra Collaboration (aka ZCS) 9.0 allows unauthenticated attackers to execute arbitrary web script or HTML via request parameters.

CVSS Score Version 3.x: 6.1 MEDIUM

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
Winter Vivern	T1566, T1055, T1199

Targeted Countries by Threat: Belarus, Italy, Türkiye, Ecuador, Poland, India, Slovakia

Targeted Sector by Threat: Foreign, Government, Diplomatic, Embassy, Military

CVE-2021-1732

Description: Windows Win32k Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1698.

CVSS Score Version 3.x: 7.8 HIGH

CWE: CWE-787 (Out-of-bounds Write)

Exploit: http://packetstormsecurity.com/files/161880/Win32k-ConsoleControl-Offset-Confusion.html, http://packetstormsecurity.com/files/166169/Win32k-ConsoleControl-Offset-Confusion-Privilege-Escalation.html

Patch: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1732

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
Winter Vivern	T1189, T1204.002, T1068, T1565.002
Turla	T1189, T1204.002, T1068, T1565.002

Targeted Countries by Threat: Türkiye, Belarus, Egypt

Targeted Sector by Threat: Foreign, Embassy

CVE-2021-31207

Description: Microsoft Exchange Server Security Feature Bypass Vulnerability

CVSS Score Version 3.x: 6.6 MEDIUM

CWE: CWE-434 (Unrestricted Upload of File with Dangerous Type)

Exploit: http://packetstormsecurity.com/files/163895/Microsoft-Exchange-ProxyShell-Remote-Code-Execution.html

Patch: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
BlackByte	T1190, T1505.003, T1595.002, T1055, T1003, T1105, T1021.002
Cobalt Strike	T1190, T1505.003, T1595.002, T1055, T1003, T1105, T1021.002
MimiKatz	T1003

Targeted Countries by Threat: U.S., Europe, and Australia

Targeted Sector by Threat: Government

CVE-2022-40684

Description: An authentication bypass using an alternate path or channel [CWE-288] in Fortinet FortiOS version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.6, FortiProxy version 7.2.0 and version 7.0.0 through 7.0.6 and FortiSwitchManager version 7.2.0 and 7.0.0 allows an unauthenticated atttacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS requests.

CVSS Score Version 3.x: 9.8 CRITICAL

CWE: CWE-287 (Improper Authentication)

Exploit: http://packetstormsecurity.com/files/169431/Fortinet-FortiOS-FortiProxy-FortiSwitchManager-Authentication-Bypass.html

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Mitre ATT&CK Technique ID related to CVE: T1134, T1185, T1505.003, T1563, T1548, T1550.001, T1557, T1040

Threat	MITRE ATT&CK Technique
Volt Typhoon	T1566

Targeted Countries by Threat: United States of America, Europe, Ukraine

Targeted Sector by Threat: Individuals, Government

CVE-2022-41040

Description: Microsoft Exchange Server Elevation of Privilege Vulnerability.

CVSS Score Version 3.x: 8.8 HIGH

CWE: CWE-918 (Server-Side Request Forgery (SSRF))

Exploit: http://packetstormsecurity.com/files/170066/Microsoft-Exchange-ProxyNotShell-Remote-Code-Execution.html

Patch: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
PLAY	T1190, T1068, T1562
SystemBC	T1059, T1203
MimiKatz	T1552, T1003

Targeted Countries by Threat: France, Australia, Germany, United States of America, Italy, UK

Targeted Sector by Threat: Government, Logistics, Shipping, Healthcare, Media, Construction, Legal, individuals, Finance

CVE-2023-1389

Description: TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 contained a command injection vulnerability in the country form of the /cgi-bin/luci;stok=/locale endpoint on the web management interface. Specifically, the country parameter of the write operation was not sanitized before being used in a call to popen(), allowing an unauthenticated attacker to inject commands, which would be run as root, with a simple POST request.

CVSS Score Version 3.x: 8.8 HIGH

CWE: CWE-77 (Improper Neutralization of Special Elements used in a Command ('Command Injection'))

Found in CISA Known Exploited Vulnerabilities: Yes

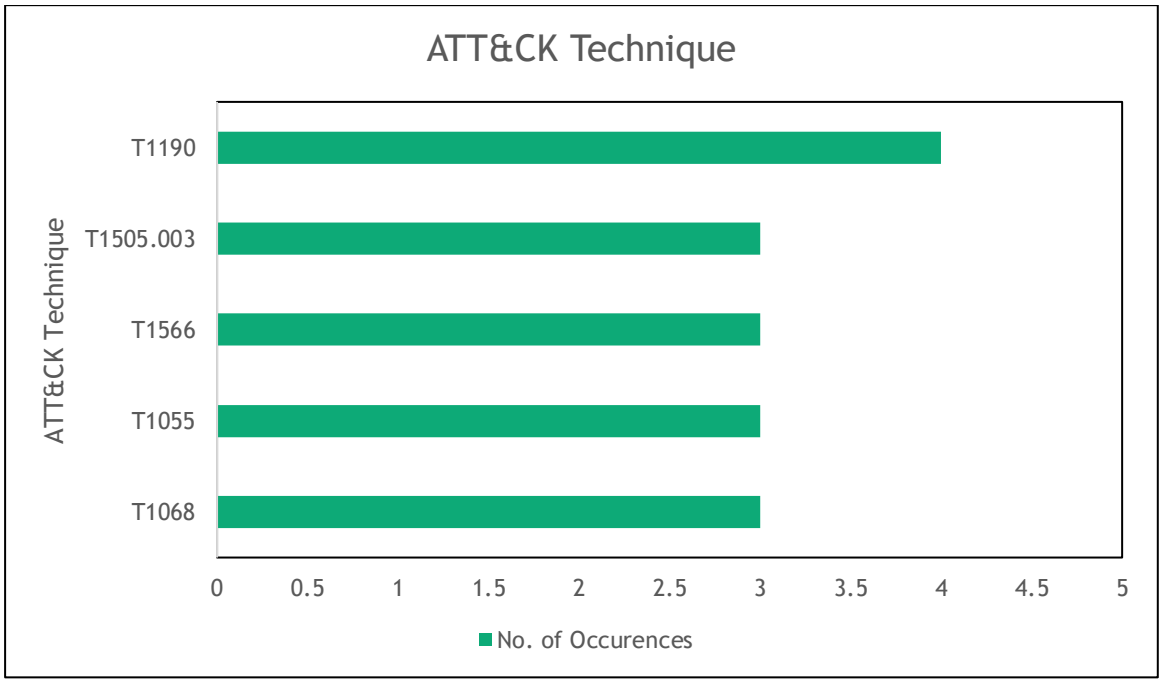
Vulnerability-Threat Information:

Threat	MITRE ATT&CK Technique
Mirai	T1498, T0814, T1202

Targeted Countries by Threat: Japan, Eastern Europe

Targeted Sector by Threat: Financial, Critical Infrastructure, Energy

Top ATT&CK Technique Based on Top Targeted CVEs



TARGETED CVE LIST AS PER INDIA REGION

CVE-2023-3519

Description: Unauthenticated remote code execution

CVSS Score Version 3.x: 9.8 CRITICAL

CWE: CWE-94 (Improper Control of Generation of Code ('Code Injection'))

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

Mitre ATT&CK Technique ID related to CVE: 'T1027.009', 'T1564.009', 'T1027.006'

Threat	MITRE ATT&CK Technique
APT29	T1190, T1505.003, T1548.001, T1036.008, T1552.001, T1552.004

Targeted Countries by Threat: France, Bangladesh, Germany, Italy, India, Russian Federation, Japan, Switzerland, China

Targeted Sector by Threat: Foreign, Government, Critical Infrastructure

CVE-2022-27926

Description: A reflected cross-site scripting (XSS) vulnerability in the /public/launchNewWindow.jsp component of Zimbra Collaboration (aka ZCS) 9.0 allows unauthenticated attackers to execute arbitrary web script or HTML via request parameters.

CVSS Score Version 3.x: 6.1 MEDIUM

Found in CISA Known Exploited Vulnerabilities: Yes

Vulnerability-Threat Information:

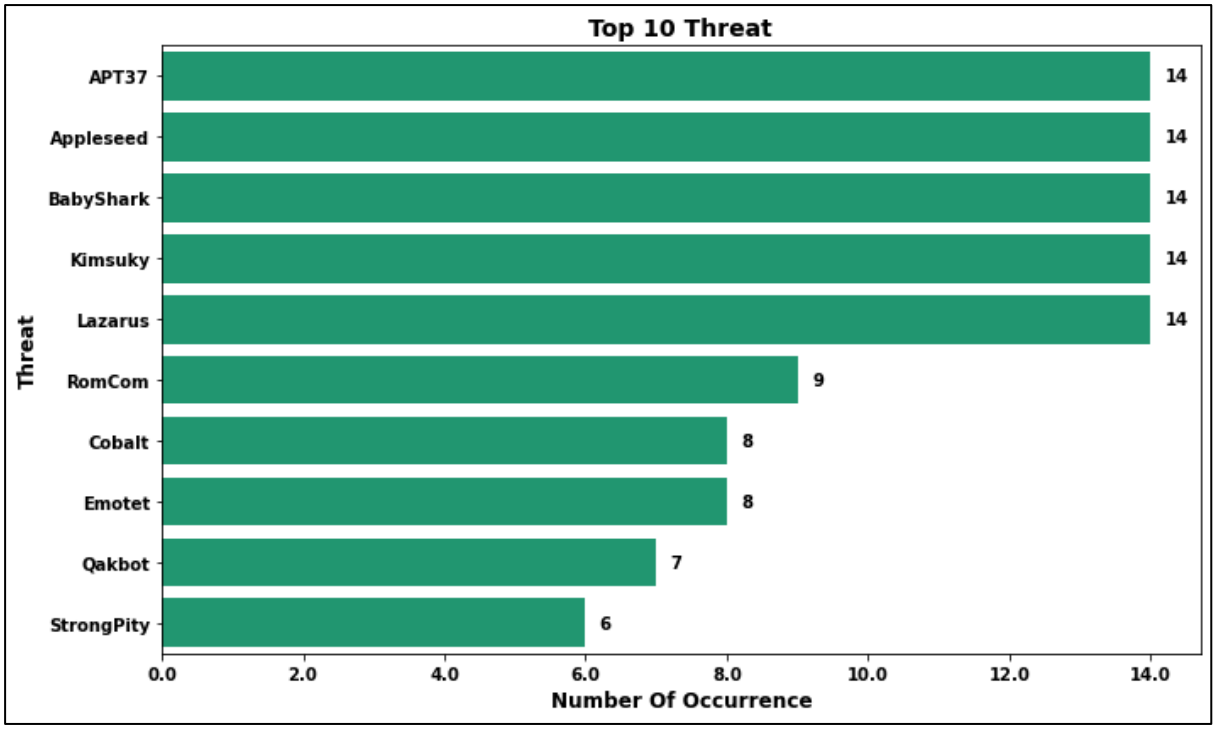
Threat	MITRE ATT&CK Technique
Winter Vivern	T1566, T1055, T1199

Targeted Countries by Threat: Belarus, Italy, Türkiye, Ecuador, Poland, India, Slovakia

Targeted Sector by Threat: Foreign, Government, Diplomatic, Embassy, Military

TOP THREATS [APT / MALWARES]

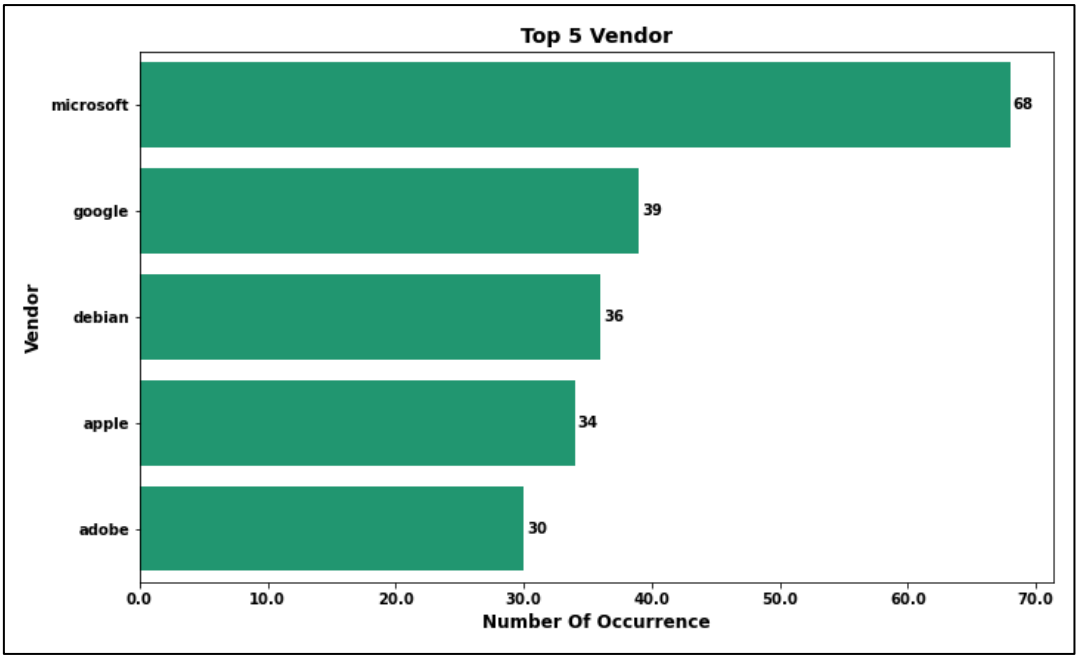
Top Threats [APT / Malwares] targeting CVEs in this period:



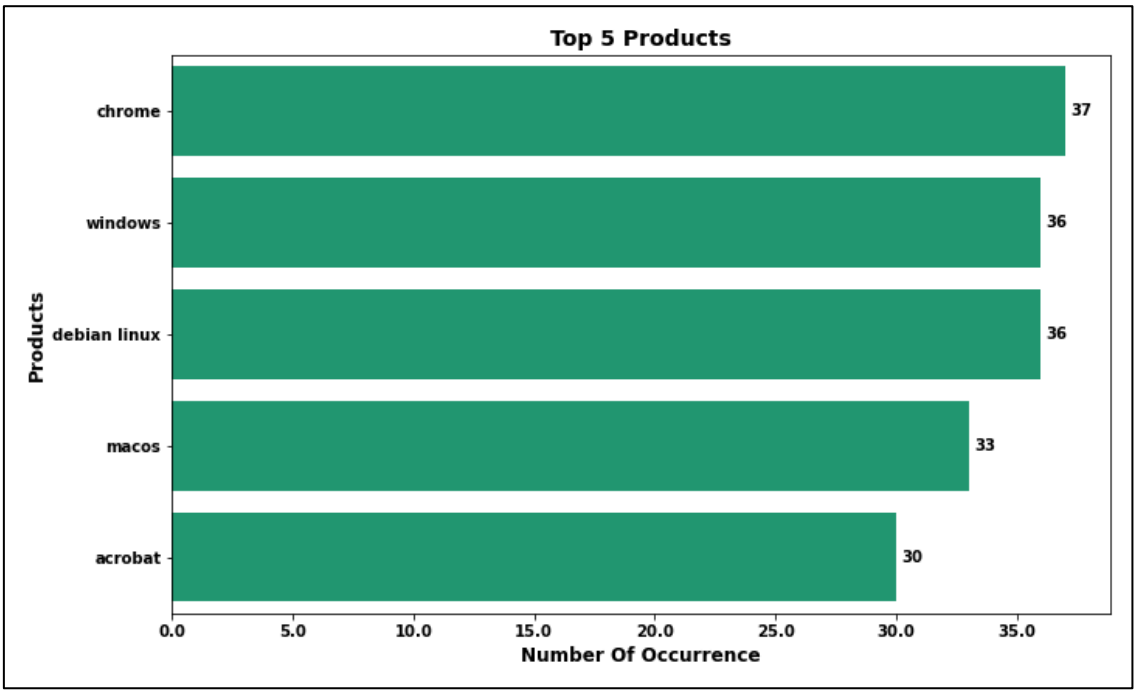
Threat	Threat Types	ATT&CK Technique & Tactics
APT37	APT	T1071, T1059, T1204.002, TA0043
Appleseed	Malware	TA0011,T1105, T1056.001, T1113, TA0010
BabyShark	Malware	T1547, T1059, T1566, T1204.002, T1137, TA0010
Kimsuky	APT_Malware	T1566, T1204.002, T1137
Lazarus	APT	T1082, T1087.002, T1210, T1203, T1091, T1025
RomCom	APT	T1566, T1083, T1027, T1547, T1036, T1140, T1106, T1573
Cobalt	APT	TA0011,T1055.001, T1574.001
Emotet	Malware	T1140, T1059, T1055, TA0002
Qakbot	Malware	T1041, T1210, T1566
StrongPity	APT	T1020, T1041, T1105

TOP TARGETED VENDORS & PRODUCT

Top Vendor reported as per Targeted CVEs in this period:

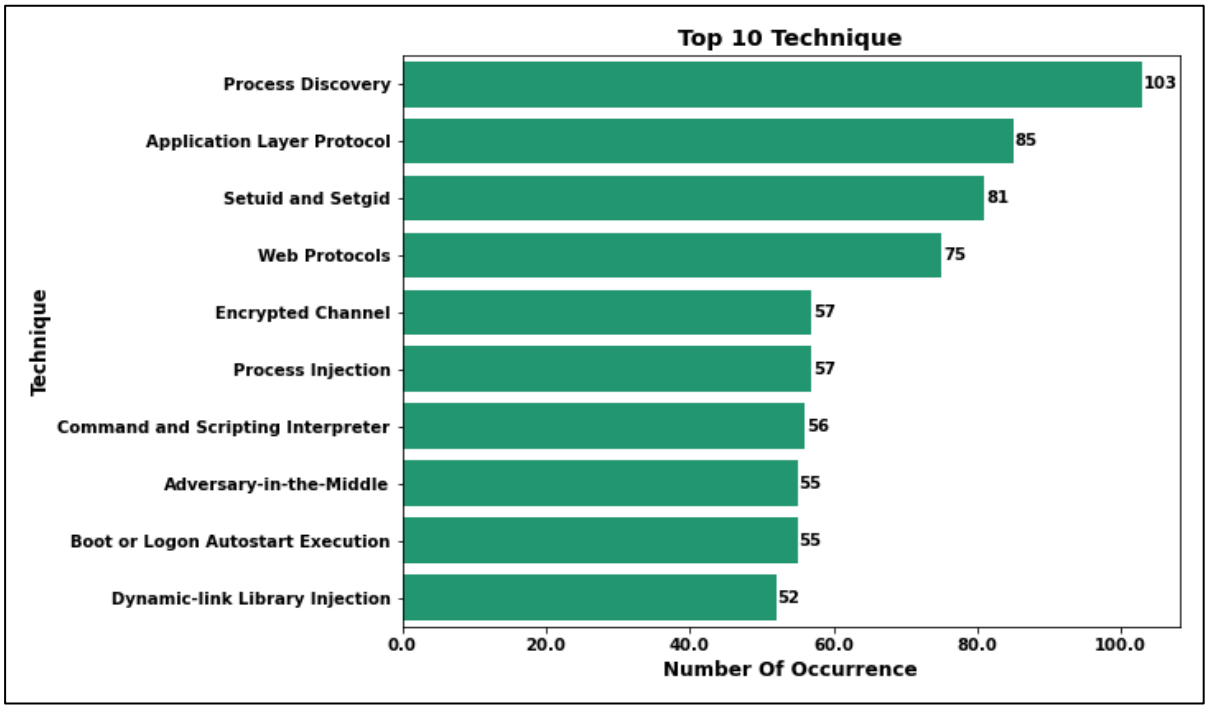


Top Product reported as per Targeted CVEs in this period:

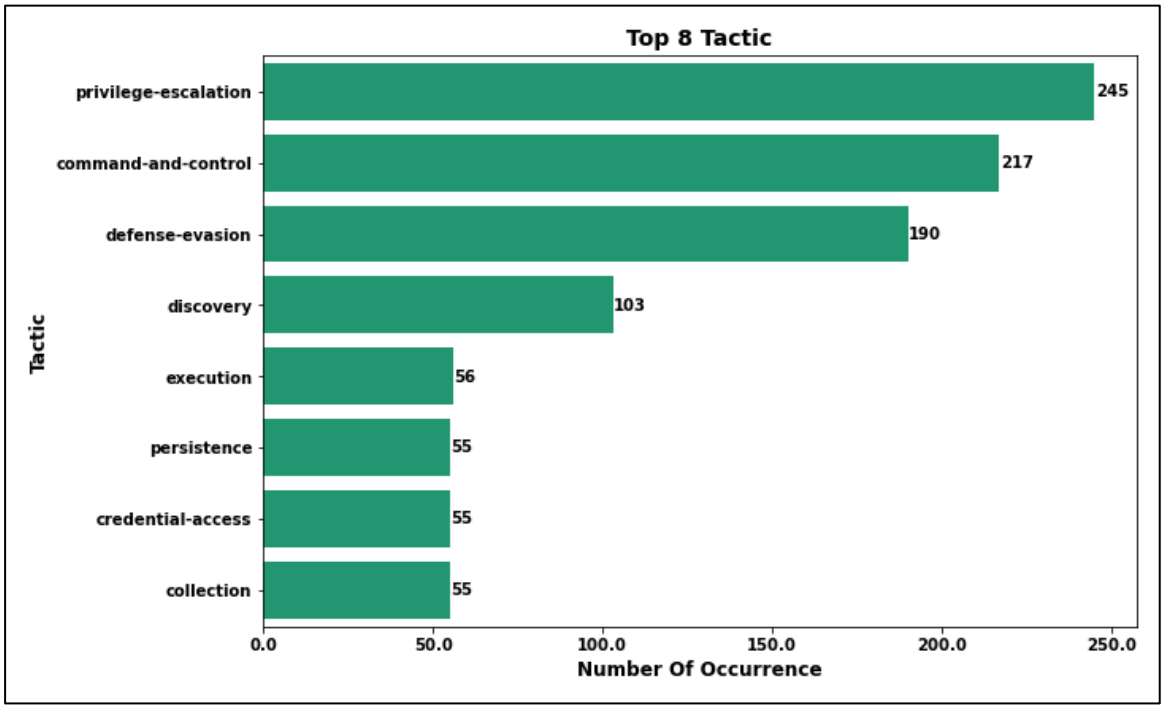


TOP TARGETED TECHNIQUE & TACTICS

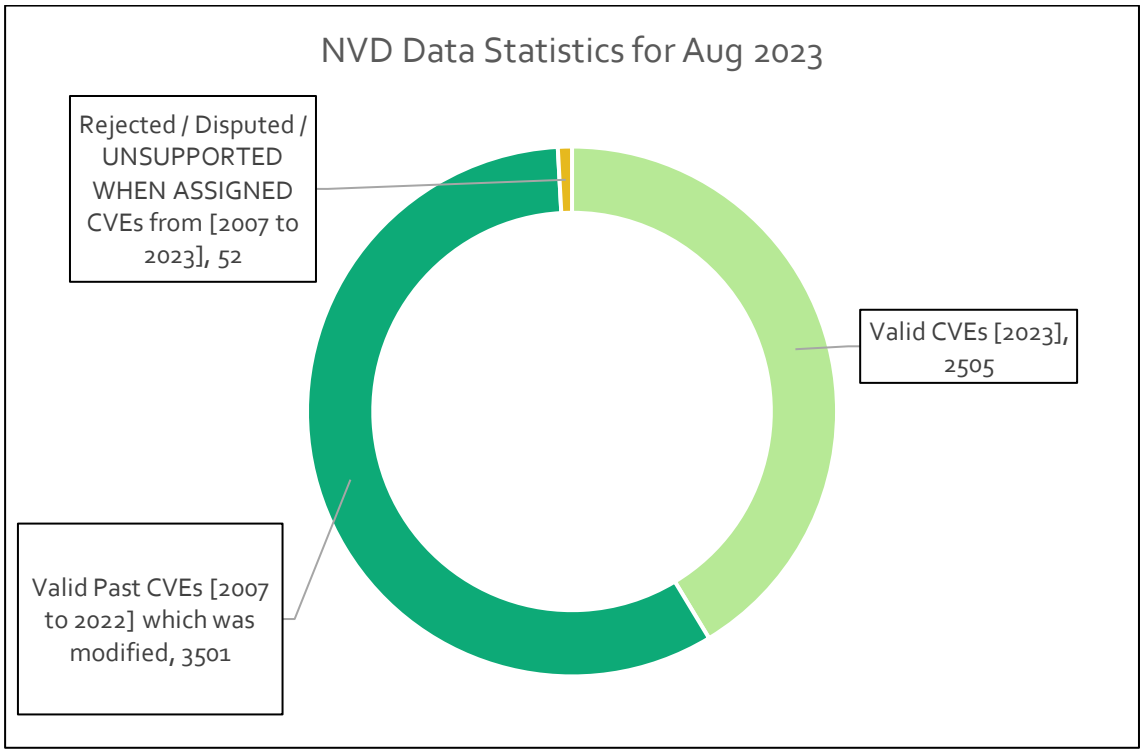
Top ATT&CK Technique as per CVEs in this period:

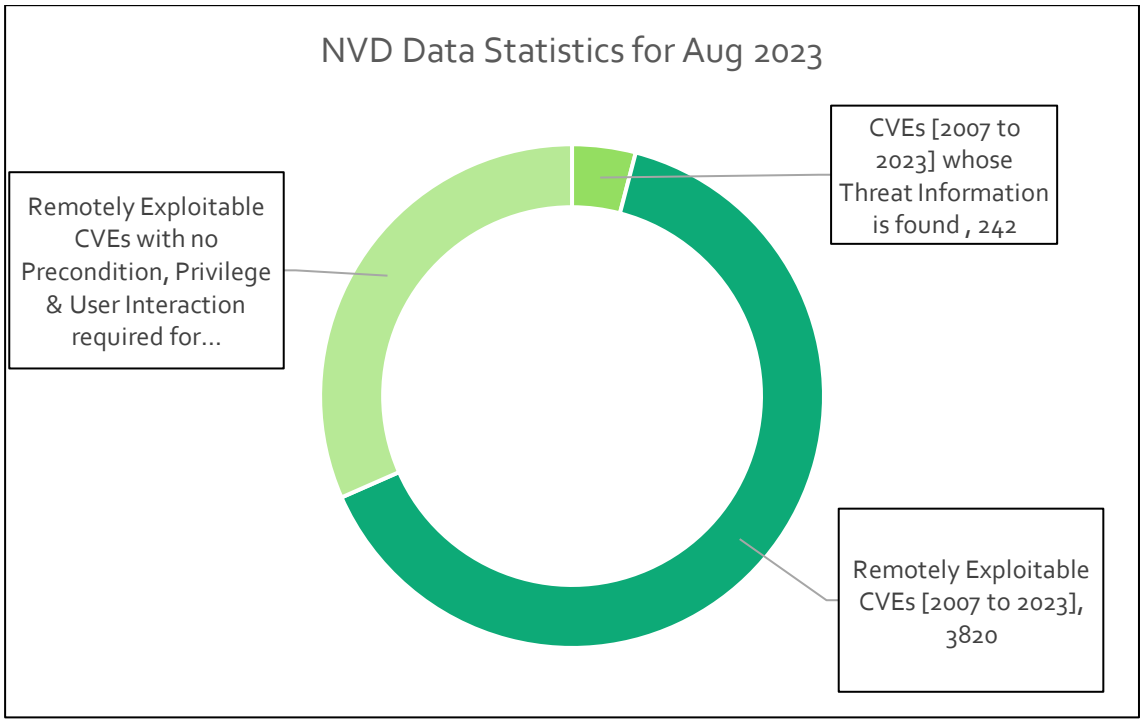


ATT&CK Tactics based on Top Technique:

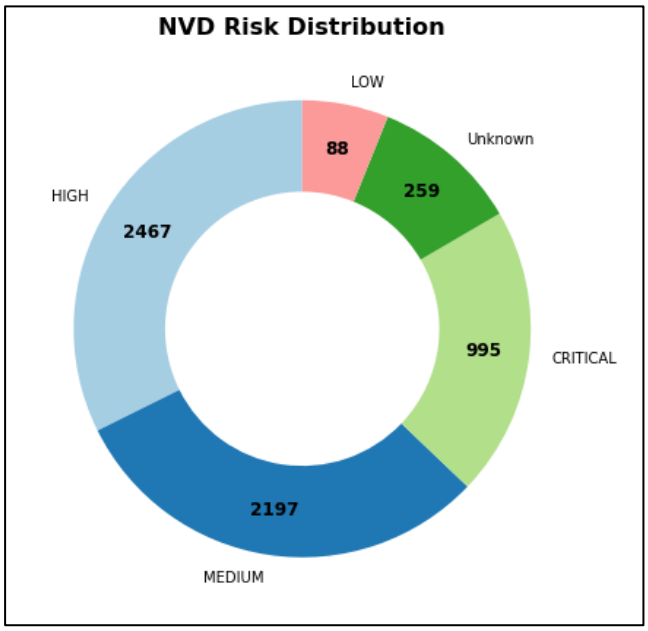


NVD DATA STATISTICS





Valid CVEs [2007 – 2023] Risk Distribution



CVEs [2007 – 2023] whose Threat Information Found Targeted Risk Distribution