SECURITY REPORT

2023

MAR

2023年03月
攻撃統計情報

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

月次攻撃サービスの統計及び分析 - 2023年03月

株式会社サイバーフォートレスでは攻撃情報を収集し、分析しています。
分析内容から、月次攻撃類型、脆弱性攻撃、ブラックリストのTOP10を確認し、過去データと比較し、
攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てて頂ければと思います。

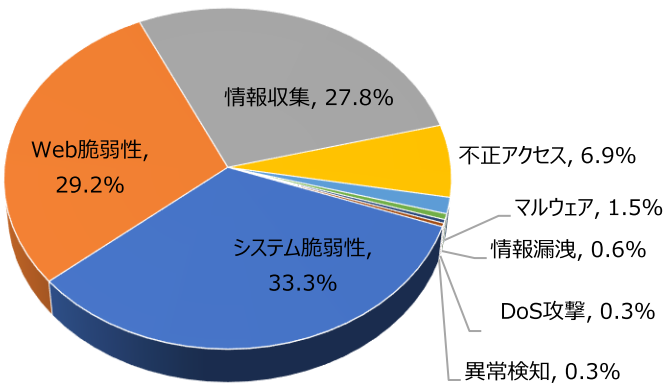
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	33.3%	-
Web脆弱性(Web Vulnerability)	29.2%	▲1
情報収集(Information Gathering)	27.8%	▼1
不正アクセス(Unauthorized access)	6.9%	-
マルウェア(Malware)	1.5%	-
情報漏洩(Information Exposure)	0.6%	▲2
異常検知(Anomaly Detection)	0.3%	-
DoS攻撃(Denial of service attack)	0.3%	▼2

2023年03月の攻撃類型を確認した結果、全体の攻撃合計が先月と比べて約0.82倍ぐらい減少し、全体の攻撃件数が減少した。

そのうち、システム脆弱性に関する攻撃は先月比べて約410件ほど減少し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃件数の減少によるものだと確認できた。

また、情報収集に関する攻撃は先月と比べて約480件ぐらい増加し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数増加によるものだと確認できた。

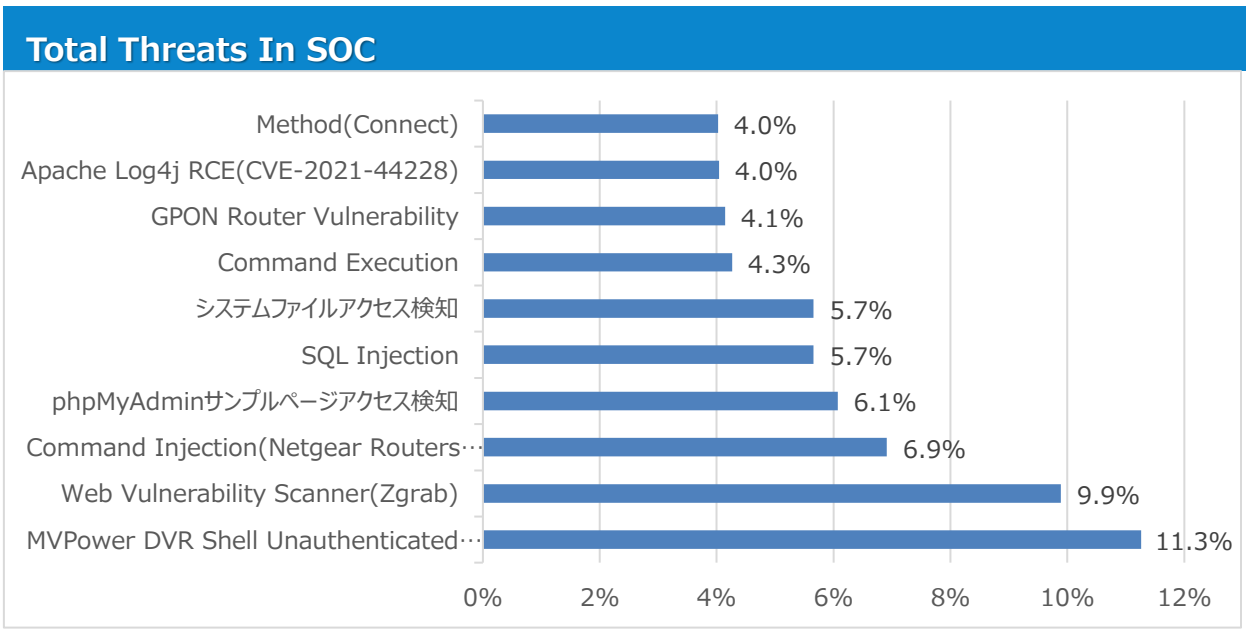


月次攻撃サービスの統計及び分析 - 2023年03月

02. 月次脆弱性攻撃TOP10

2023年03月の月次脆弱性TOP10を確認した結果、 Apache Log4j RCE(CVE-2021-44228)攻撃が新たにTOP10に登場し、全体的な攻撃件数が減少したことが確認できた。一方MVPower DVR Shell Unauthenticated Command Execution攻撃件数が370件ぐらい増加したことが確認できた。

順位	検知名	比率(%)	比較
1	MVPower DVR Shell Unauthenticated Command Execution	11.3%	-
2	Web Vulnerability Scanner(Zgrab)	9.9%	-
3	Command Injection(Netgear Routers Vulnerability)	6.9%	▲1
4	phpMyAdminサンプルページアクセス	6.1%	▼1
5	SQL Injection	5.7%	-
6	システムファイルアクセス検知	5.7%	-
7	Command Execution	4.3%	▲3
8	GPON Router Vulnerability	4.1%	▼1
9	Apache Log4j RCE(CVE-2021-44228)	4.0%	NEW
10	Method(Connect)	4.0%	▼1



月次攻撃サービスの統計及び分析 - 2023年03月

03. 月次ブラックリストIPアドレスTOP 10

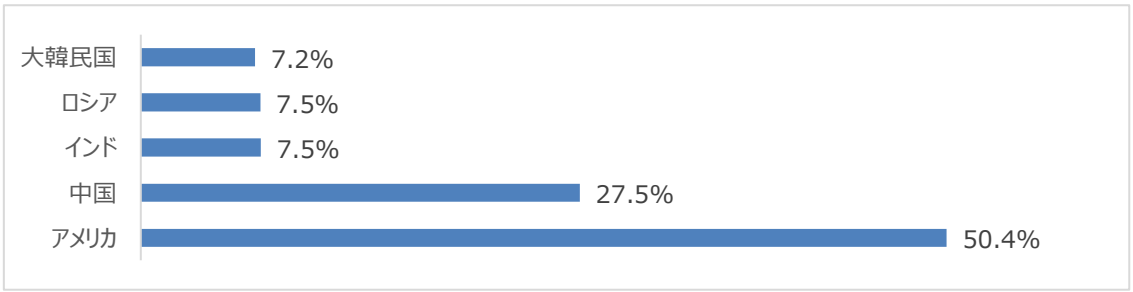
2023年03月についてTOP10を確認した結果、アメリカとロシア、大韓民国の攻撃比率が増加し、一方中国とインドの攻撃の比率は減少した。特にアメリカと中国の攻撃比率が合わせて約55%ぐらいで攻撃の半分以上を占めていることが確認できた。

※ 下記の表を参考にしたファイウォールやセキュリティ機器からの遮断を推奨します。

順位	ブックリストIP	国	攻撃情報
1	5.255.109.233	NL	Apache Log4j RCE(CVE-2021-44228)
2	198.23.227.34	US	SQL Injection
3	5.255.109.219	NL	Apache Log4j RCE(CVE-2021-44228)
4	34.171.198.211	US	Apache Log4j RCE(CVE-2021-44228)
5	95.181.161.66	NL	Network Scan
6	172.93.110.238	US	Apache Log4j RCE(CVE-2021-44228)
7	152.89.196.211	GB	Application Vulnerability(PHPUnit)
8	89.248.163.239	NL	Network Scan
9	209.141.36.87	US	Command Execution
10	112.47.34.246	CN	phpMyAdminサンプルページアクセス

Total Countries

今月攻撃IP, 国家順位の詳細TOP10の表及び比率



Rank	Source IP	Country	Rank	Source IP	Country
1	5.255.109.233	NL	6	172.93.110.238	US
2	198.23.227.34	US	7	152.89.196.211	GB
3	5.255.109.219	NL	8	89.248.163.239	NL
4	34.171.198.211	US	9	209.141.36.87	US
5	95.181.161.66	NL	10	112.47.34.246	CN

攻撃パターン毎の詳細分析結果

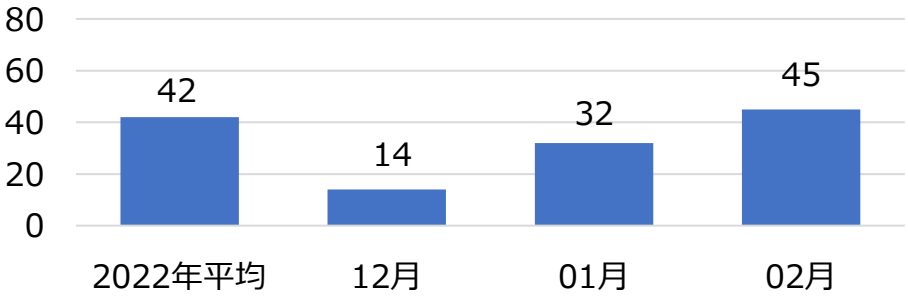
03月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥'shell¥'」ファイルを利用することでクエリの文字列の中から任意のシステムコマンドが実行できるようになる。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)は、Webサーバの設定ページや許可方法、許可されていないWebページ、ライセンスのないポートなど、脆弱性部分の存在を判断するために使用される。
CommandInjection (Netgear Routers Vulnerability)	NetGear DGNシリーズのルータ内のウェブサーバが一部のURLに対して認証をせず、「setup.cgi」スクリプトの「syscmd」機能を活用して任意のコマンドを実行することができる。
phpMyAdmin サンプルページ アクセス	phpMyAdminはMySQLをWebサーバで管理する目的にてPHPで作成されたオープンソースツールである。MySQLサーバを対象に脆弱性を見つけ、データベースの作成/削除、テーブルの作成/削除、フィールドの生成/削除、SQL文の実行など、権限を利用した管理機能実行による攻撃が可能となる。 その脆弱性が存在する場合、phpMyAdminのscript/setup.phpファイルに `?` 引数を使用して任意の関数を挿入し、システム命令を実行できる。
SQL Injection	SQL Injection攻撃はウェブページから記号やUnion, Selectなどクエリで使用される文字列をフィルタリ ングせずに入力された値がクエリに使用される場合発生しうる。攻撃者はDBに繋がっているアカウントが 持っている権限内で様々なクエリを使用して保存された情報の取得、修正、削除及びシステムアクセスな どが可能である。
システムファイル アクセス検出	Directory Traversalの脆弱性などを利用し、「/etc/passwd」や「*.conf /.env」などの構成情報を含む主要なシステム ファイルにアクセスを計る。
Command Execution	適切な認証が行われていない使用者の入力値がOSコマンドの一部、もしくはその他のコマンドで構成され実行される場合、意図しないシステムコマンドが実行され、不正に権限が変更されたり、システム動作及び運用に悪影響を及ぼす可能性がある。一般的なコマンドラインのパラメータやストリーム入力など、外部入力を使用しシステムコマンドを生成するプログラムはたくさん存在するが、この場合、外部の入力文字列は信頼できないため、適切な処理（チェック処理）をしないと攻撃者が望むコマンドが実行可能になる。
GPON Router Vulnerability	Dasan GPON家庭用のルータから発見された脆弱性で「?images」の文字列を機器アクセス用URLに入力することで認証をスルー出来る脆弱性である。 当該の脆弱性を利用して認証されていない攻撃者が機器へリモートでコマンドを実行し、DNS設定修正などの様々な攻撃が可能である。 この脆弱性は家庭用ルータにて発見された。
Apache Log4j RCE (CVE-2021-44228)	幅広く使用されているJava logging libraryのApache Log4jを利用して攻撃者は認証なく、サーバに対してリモートコード実行ができる。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security) トンネリングで内部アクセスを試す。これのためにConnect Methodを使用し、脆弱性が存在する場合攻撃のための中間経由地として使用される可能性がある。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

SPIDER TMのポリシーにて、2023年02月の1か月間で共有されたサイバー脅威検知ポリシーは45件である。
02月1か月の間、WinPWN, MS Exchange Server(CVE-2023-21706, CVE-2023-21529), Fortinet Fortinac(CVE-2022-39952)などに対する検知ポリシーが配布された。



3か月間件数

6,105
全体配布量

45
今月配布量

32
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.06111 Malware, WinPWN, A Network Trojan was detected"; flow:to_server,established; file_data; content:"|28 24 5F 2D 62 58 6F 52 20 20 30 78 30 38 20 29 20 7D 29 20 2D 6A 4F 69 4E 20 27 27 7C 20 26 20 28 20 24 45 4E 56 3A 63 4F 4D 53 50 45 63 5B 34 2C 32 34 2C 32 35 5D|"; fast_pattern:only; sid:806111;)	WinPWN Malwareのネットワーク通信を検知するポリシー	Malware, WinPWN
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06131 SERVER-WEBAPP, Microsoft, Exchange Server, CVE-2023-21706, Attempted User Privilege Gain"; flow:to_server,established; content:"System.Diagnostics"; fast_pattern; nocase; http_client_body; content:"Process"; distance:0; nocase; http_client_body; content:"<BA N=|22|SerializationData|22|>"; nocase; http_client_body; base64_decode:bytes 1000,relative; base64_data; content:"UnitySerializationHolder"; nocase; content:"/Powershell"; nocase; http_uri; sid:206131;)	Microsoft Exchange ServerのCVE-2023-21706の脆弱性を悪用したリモートコードを実行する攻撃を検知するポリシー	SERVER-WEBAPP, Microsoft, Exchange Server, CVE-2023-21706
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06136 SERVER-WEBAPP, Microsoft, Exchange Server, CVE-2023-21529, Attempted User Privilege Gain"; flow:to_server,established; content:"System.Diagnostics"; fast_pattern; nocase; http_client_body; content:"Process"; distance:0; nocase; http_client_body; content:"<BA N=|22|SerializationData|22|>"; nocase; http_client_body; base64_decode:bytes 1000,relative; base64_data; content:"MultiValuedProperty"; nocase; content:"/Powershell"; nocase; http_uri; sid:206136;)	Microsoft Exchange ServerのCVE-2023-21529の脆弱性を悪用したリモートコードを実行する攻撃を検知するポリシー	SERVER-WEBAPP, Microsoft, Exchange Server, CVE-2023-21529
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.1.06137 SERVER-OTHER, Fortinet, Fortinac, CVE-2022-39952, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/configWizard/keyUpload.jsp"; fast_pattern:only; http_uri; content:"name=|22|key|22|"; nocase; http_client_body; content:"filename="; nocase; http_client_body; sid:106137;)	Fortinet FortinacのCVE-2022-39952の脆弱性を悪用したリモートコードを実行する攻撃を検知するポリシー	SERVER-OTHER, Fortinet, Fortinac, CVE-2022-39952