SECURITY REPORT

2023

APR

2023年04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04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。

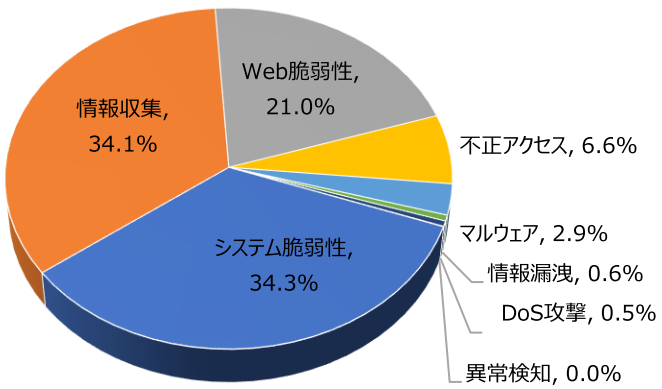
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	34.3%	-
情報収集(Information Gathering)	34.1%	▲1
Web脆弱性(Web Vulnerability)	21.0%	▼1
不正アクセス(Unauthorized access)	6.6%	-
マルウェア(Malware)	2.9%	-
情報漏洩(Information Exposure)	0.6%	-
DoS攻撃(Denial of service attack)	0.5%	-
異常検知(Anomaly Detection)	0.0%	-

2023年04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1.02倍ぐらい増加し、全体の攻撃件数が増加した。

そのうち、情報収集に関する攻撃は先月比べて約410件ほど増加し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数の増加によるものだと確認できた。

また、Web脆弱性に関する攻撃は先月と比べて約450件ぐらい減少し、これはetcpasswd Detect攻撃件数減少によるものだと確認できた。

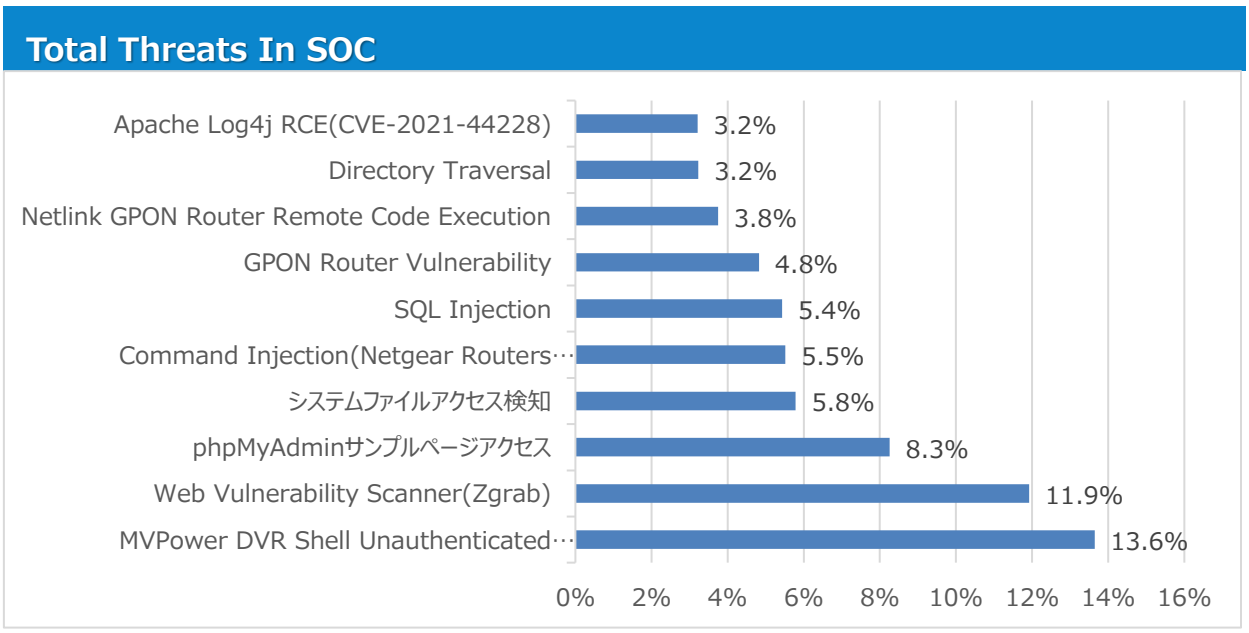


月次攻撃サービスの統計及び分析 - 2023年04月

02. 月次脆弱性攻撃TOP10

2023年04月の月次脆弱性TOP10を確認した結果、 Netlink GPON Router Remote Code Execution, Directory Traversal 攻撃が新たにTOP10に登場し、全体的な攻撃件数が増加したことが確認できた。一方 MVPower DVR Shell Unauthenticated Command Execution攻撃件数が150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	13.6%	-
2	Web Vulnerability Scanner(Zgrab)	11.9%	-
3	phpMyAdminサンプルページアクセス	8.3%	▲1
4	システムファイルアクセス検知	5.8%	▲2
5	Command Injection(Netgear Routers Vulnerability)	5.5%	▼2
6	SQL Injection	5.4%	▼1
7	GPON Router Vulnerability	4.8%	▲1
8	Netlink GPON Router Remote Code Execution	3.8%	NEW
9	Directory Traversal	3.2%	NEW
10	Apache Log4j RCE(CVE-2021-44228)	3.2%	▼1



月次攻撃サービスの統計及び分析 - 2023年04月

03. 月次ブラックリストIPアドレスTOP 10

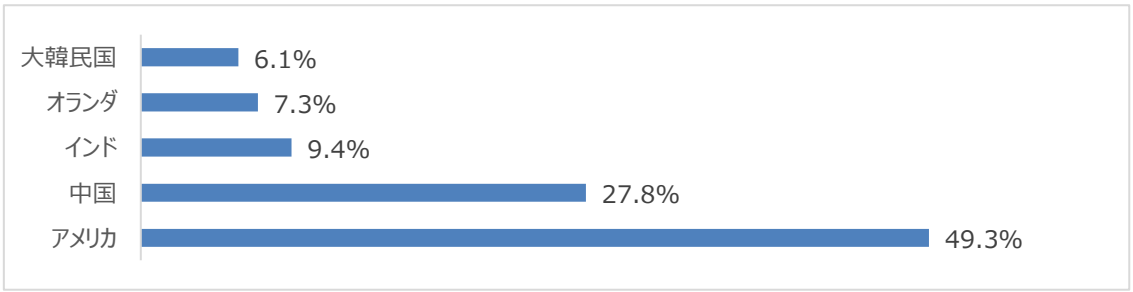
2023年04月についてTOP10を確認した結果、インドとオランダの攻撃比率が増加し、一方アメリカと中国、大韓民国の攻撃の比率は減少した。特にアメリカと中国の攻撃比率が合わせて約52%ぐらいで攻撃の半分以上を占めていることが確認できた。

※ 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	94.102.51.9	NL	Network Scanner(masscan)
2	152.89.196.54	GB	Application Vulnerability(PHPUnit)
3	5.255.102.98	NL	Apache Log4j RCE(CVE-2021-44228)
4	13.233.112.105	IN	Apache Log4j RCE(CVE-2021-44228)
5	45.145.248.50	BR	Drupalgeddon2 Remote Code Execution(CVE-2018-7600)
6	208.67.226.200	US	Apache Log4j RCE(CVE-2021-44228)
7	194.55.224.203	US	Directory Traversal
8	79.124.58.130	BG	SQL Injection
9	45.81.243.34	SK	Command Injection(D-Link HNAP Vulnerability)
10	52.56.247.64	GB	Apache Log4j RCE(CVE-2021-44228)

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
1	94.102.51.9	NL
2	152.89.196.54	GB
3	5.255.102.98	NL
4	13.233.112.105	IN
5	45.145.248.50	BR

Rank	Source IP	Country
6	208.67.226.200	US
7	194.55.224.203	US
8	79.124.58.130	BG
9	45.81.243.34	SK
10	52.56.247.64	GB

攻撃パターン毎の詳細分析結果

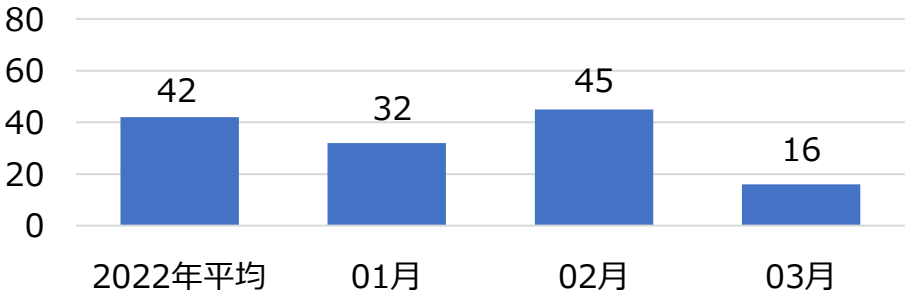
04月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
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。
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。
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。
Netlink GPON Router Remote Code Execution	Netlink GPONルータで発見された脆弱性として、ターゲットアドレスの後に/boaform/admin/formPing文字列を入力して認証手順を通過する可能性がある。この脆弱性を悪用し、認証されていない攻撃者が端末からリモートでコマンドを実行、悪意のあるファイルをアップロードする などが可能になる。
Directory Traversal	ホームページの表示もしくはダウンロードページのURLを使用せず、Webサーバ上のhomeディレクトリ外の任意のディレクトリ上のファイル(/etc/passwdファイルなど)を参照またはダウンロードすることが出来る。内部情報については、システム情報を含む/etc/pass/shadow、/etc/hosts/hostsなどの主要ファイルをダウンロードすることが可能であり、システム侵入や内部データ漏洩などの二次的な攻撃 に悪用される可能性がある。
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。

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03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16件である。
03月1か月の間、IBM Aspera Faspex(CVE-2022-47986), MS Outlook (CVE-2023-3397)などに対する検知ポリシーが配布された。



3か月間件数

6,121
全体配布量

16
今月配布量

45
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 -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06142 SERVER-WEBAPP, IBM, Aspera Faspex, CVE-2022-47986, Attempted User Privilege Gain"; flow:to_server,established; content:"/aspera/faspex/package_relay/relay_package"; fast_pattern:only; http_uri; content:"|22|external_emails|22|"; nocase; http_client_body; pcre:"/¥x22external_emails¥x22¥s*¥x3a¥s*¥x22((?!(?<!¥x5c)¥x22).)*?ruby¥x2fobject¥x3aPrettyPrint/Pi"; sid:206142;)	IBM Aspera FaspexのCVE-2022-47986脆弱性を悪用したコマンドインジェクション攻撃を検知するポリシー	Malware, WinPWN
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.2.06151 FILE-OFFICE, MS, Outlook, CVE-2023-23397, Attempted User Privilege Gain"; flow:to_client,established; flowbits:isset,file.ole; file_data; content:"|1F 85 00 00|"; content:"|1C 85 00 00|"; content:"_|00|_|00|s|00|u|00|b|00|s|00|t|00|g|00|1|00|.|00|0|00|_|00|"; content:"I|00|P|00|M|00|.|00|"; content:"|00 00 00 00 5C 00 5C 00|"; pcre:"/¥x00¥x00¥x00¥x00¥x5c¥x00¥x5c¥x00(¥d¥x00){1,3}¥x2e¥x00(¥d¥x00){1,3}¥x2e¥x00(¥d¥x00){1,3}¥x2e¥x00(¥d¥x00){1,3}/"; sid:206151;)	Microsoft OutlookのCVE-2023-23397脆弱性を悪用した権限上昇攻撃を検知するポリシー	SERVER-WEBAPP, Microsoft, Exchange Server, CVE-2023-21706
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.2.06154 FILE-OFFICE, MS, Outlook, CVE-2023-23397, Attempted User Privilege Gain"; flow:to_server,established; flowbits:isset,file.tnef; file_data; content:"|1C 85 00 00 01 00 00 00|"; content:"|1F 85 00 00 01 00 00 00|"; fast_pattern; content:"|5C 5C|"; within:2; distance:4; pcre:"/¥x1f¥x85¥x00¥x00¥x01¥x00¥x00¥x00.{4}¥x5c¥x5c¥d{1,3}¥x2e¥d{1,3}¥x2e¥d{1,3}¥x2e¥d{1,3}/s"; sid:206154;)	Microsoft OutlookのCVE-2023-23397脆弱性を悪用した権限上昇攻撃を検知するポリシー	SERVER-WEBAPP, Microsoft, Exchange Server, CVE-2023-21529
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.2.06156 FILE-OFFICE, MS, Outlook, CVE-2023-23397, Attempted User Privilege Gain"; flow:to_client,established; flowbits:isset,file.tnef; file_data; content:"|1C 85 00 00 01 00 00 00|"; content:"|1F 85 00 00 01 00 00 00|"; fast_pattern; content:"|5C 5C|"; within:2; distance:4; pcre:"/¥x1f¥x85¥x00¥x00¥x01¥x00¥x00¥x00.{4}¥x5c¥x5c¥d{1,3}¥x2e¥d{1,3}¥x2e¥d{1,3}¥x2e¥d{1,3}/s"; sid:206156;)	Microsoft OutlookのCVE-2023-23397脆弱性を悪用した権限上昇攻撃を検知するポリシー	SERVER-OTHER, Fortinet, Fortinac, CVE-2022-39952