SECURITY REPORT

2023

JUN

2023年06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06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。

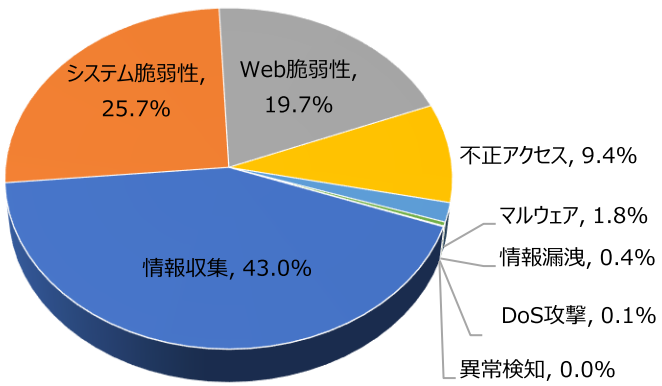
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	43.0%	-
システム脆弱性(System Vulnerability)	25.7%	-
Web脆弱性(Web Vulnerability)	19.7%	-
不正アクセス(Unauthorized access)	9.4%	-
マルウェア(Malware)	1.8%	-
情報漏洩(Information Exposure)	0.4%	-
DoS攻撃(Denial of service attack)	0.1%	-
異常検知(Anomaly Detection)	0.0%	-

2023年06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1.28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900件ほど増加し、これはSIP Vulnerability Scanner(Sipvicious)攻撃件数の増加によるものだと確認できた。

一方、システム脆弱性に関する攻撃は先月と比べて約450件ぐらい増加し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃件数増加によるものだと確認できた。



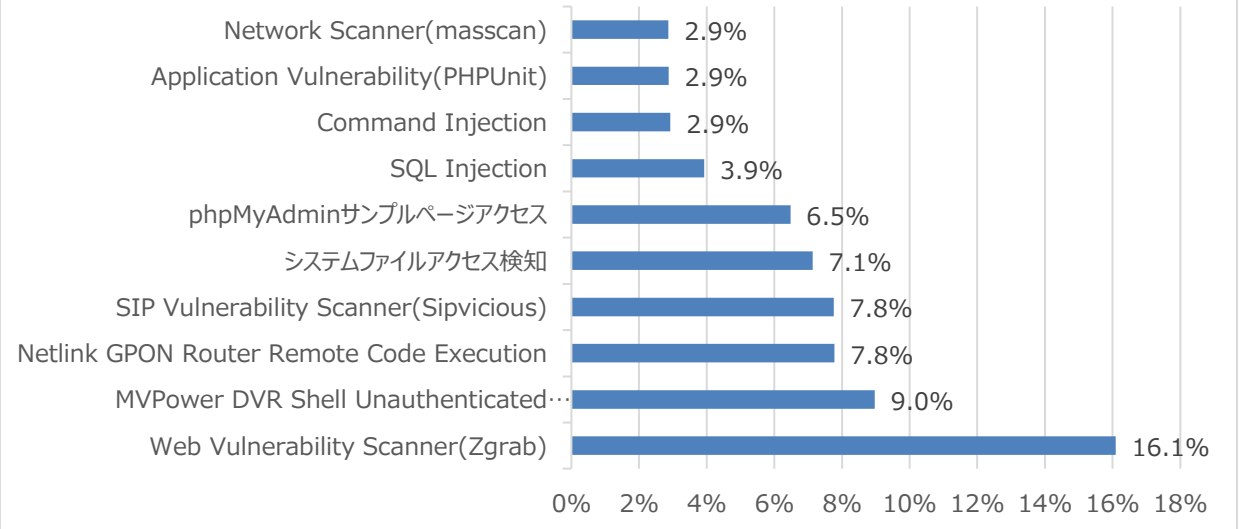
月次攻撃サービスの統計及び分析 - 2023年06月

02. 月次脆弱性攻撃TOP10

2023年06月の月次脆弱性TOP10を確認した結果、 Command Injection, Application Vulnerability (PHPUnit)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。特に、Netlink GPON Router Remote Code Execution攻撃件数が400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	Web Vulnerability Scanner(Zgrab)	16.1%	-
2	MVPower DVR Shell Unauthenticated Command Execution	9.0%	-
3	Netlink GPON Router Remote Code Execution	7.8%	▲3
4	SIP Vulnerability Scanner(Sipvicious)	7.8%	▲1
5	システムファイルアクセス検知	7.1%	▼2
6	phpMyAdminサンプルページアクセス	6.5%	▲3
7	SQL Injection	3.9%	▼3
8	Command Injection	2.9%	NEW
9	Application Vulnerability(PHPUnit)	2.9%	NEW
10	Network Scanner(masscan)	2.9%	▼2

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2023年06月

03. 月次ブラックリストIPアドレスTOP 10

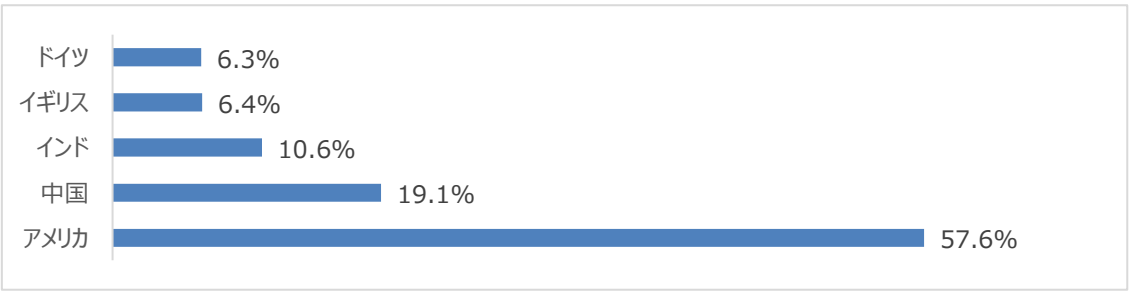
2023年06月についてTOP10を確認した結果、アメリカとインド、イギリス、ドイツの攻撃比率が増加し、一方中国の攻撃の比率は減少した。特にアメリカと中国の攻撃比率が合わせて約47.5%ぐらいで攻撃のほぼ半分ぐらいを占めていることが確認できた。

※ 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	74.84.150.2	US	SIP Vulnerability Scanner(Sipvicious)
2	109.237.98.226	GB	システムファイルアクセス検知
3	211.43.13.222	KR	Apache Log4j RCE(CVE-2021-44228)
4	109.237.97.180	GB	システムファイルアクセス検知
5	152.89.196.144	RU	Application Vulnerability(PHPUnit)
6	45.155.91.59	PL	SIP Vulnerability Scanner(Sipvicious)
7	74.84.150.62	US	SIP Vulnerability Scanner(Sipvicious)
8	45.134.144.6	US	SIP Vulnerability Scanner(Sipvicious)
9	83.97.73.89	RU	MobileIron RCE(CVE-2020-15505)
10	185.224.128.29	NL	SIP Vulnerability Scanner(Sipvicious)

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	152.89.196.54	NL	6	51.159.93.171	FR
2	95.214.55.244	PL	7	80.66.77.239	TF
3	109.237.97.180	GB	8	192.142.226.5	TH
4	109.237.98.226	GB	9	152.89.196.222	NL
5	79.124.59.170	BG	10	69.174.102.18	US

攻撃パターン毎の詳細分析結果

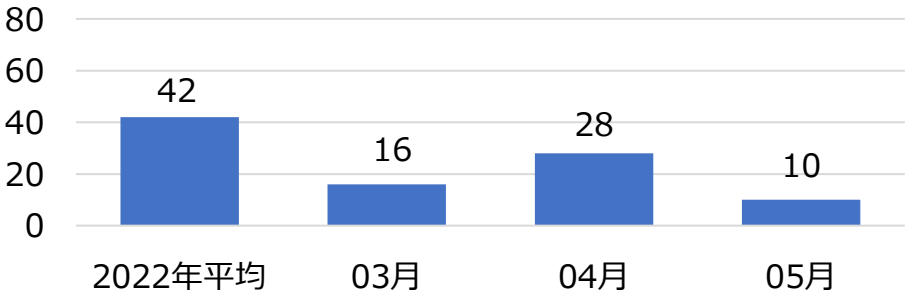
06月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。
SIP Vulnerability Scanner(Sipvicious)	SIPViciousはSIP(インターネット電話プロトコル)基盤のVoIP監査ツールであるが、攻撃者によって悪用されている。インターネットに繋がっているVoIP, PBX(電話交換システム)を探した後、Brute Force攻撃でアカウント奪取及び国際電話番号やプレミアム電話番号に電話をかけて課金を誘導する。主にUser-Agent methodにFriendly-ScannerやSIPViciousの文字列が使用されて、攻撃対象がVoIP, PBXシステムではない場合、攻撃に対する有効性はない。.
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。
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。
Command Injection	システムコマンドが含まれている入力値が適切な検証プロセスを通らない場合、入力されたコマンドが実行しうる。この脆弱性が存在する場合、攻撃者がシステムに直接コマンド送信できるため、ファイルの閲覧、ダウンロード、実行などで追加被害が発生する可能性がある。
Application Vulnerability(PHPUnit)	PHPUnitはユニットテストフレームワークで/phpunit/src/Util/PHP/eval-stdin.phpファイルに存在する脆弱性を利用してリモートで任意のコードが実行できる。攻撃者は<?phpの文字列から始まるHTTP POSTデータで任意のPHPコードが実行できる。
Network Scanner(masscan)	ネットワーク帯域スキャン攻撃ができるmasscanである。NMAPと似たようだがカスタムしたTCP/IP Stackを使用して速度的に効率的である。

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05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10件である。
05月1か月の間、CryptoLocker, Zoho(CVE-2021-43319), CommonsCollection(CVE-2018-15381)などに対する検知ポリシーが配布された。



3か月間件数

6,159
全体配布量

10
今月配布量

28
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06186 Malware, Ransomware, CryptoLocker, A Network Trojan was detected"; flow:to_server,established; urilen:5,norm; content:"/home"; depth:5; nocase; http_uri; content:"|F4 B0 B0 08 D1 8B BE 1F 03 FB EC 16 CE B0 08 70 B4 61 CA 8D 50 37|"; fast_pattern:only; http_client_body; sid:806186;)	CryptoLocker Malwareのネットワーク通信を検知するポリシー	Malware, Ransomware, CryptoLocker
alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"IGRSS.10.06187 SERVER-WEBAPP, Zoho, ManageEngine, CVE-2021-43319, Web Application Attack"; flow:to_server,established; content:"/client/api/json/ncmsettings/pingCheck"; fast_pattern:only; nocase; content:"IPADDRESS"; nocase; content:"Content-Disposition"; nocase; pcre:"/name¥s*=¥s*[¥x22¥x27]?IPADDRESS((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/sim"; sid:1006187;)	Zoho ManageEngineの脆弱性であるCVE-2021-43319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	SERVER-WEBAPP, Zoho, ManageEngine, CVE-2021-43319
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.06194 Malware, Downloader, Agent, A Network Trojan was detected"; flow:to_client,established; file_data; content:"powershell"; depth:10; nocase; content:"$update=|27|windows|27|"; nocase; content:"$command=\|27\|run\|27\|"; nocase; content:"$url=$scheme+$command+|27|.mocky.io/|27|"; fast_pattern:only; sid:806194;)	Powershellを使用するDownloader Agentのネットワーク通信を検知するポリシー	Malware, Downloader, Agent
alert tcp $EXTERNAL_NET any -> $HOME_NET [1099,6099,7001,$HTTP_PORTS] (msg:"IGRSS.2.06195 SERVER-OTHER, JAVA, CommonsCollection, CVE-2018-15381, Attempted User Privilege Gain"; flow:to_server,established; content:"|AC ED 00 05|"; content:"getRuntime"; distance:0; content:"java.lang.Class"; within:50; content:"invoke"; distance:90; sid:206195;)	JAVA CommonsCollectionライブラリの脆弱性であるCVE-2018-15381を悪用したデータ逆直列化攻撃を検知するポリシー	SERVER-OTHER, JAVA, CommonsCollection, CVE-2018-15381