SECURITY REPORT

2023

JUL

2023年07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07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。

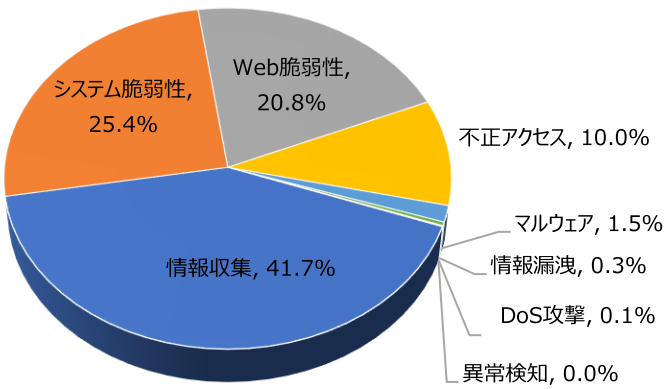
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	41.7%	-
システム脆弱性(System Vulnerability)	25.4%	-
Web脆弱性(Web Vulnerability)	20.8%	-
不正アクセス(Unauthorized access)	10.0%	-
マルウェア(Malware)	1.5%	-
情報漏洩(Information Exposure)	0.3%	-
DoS攻撃(Denial of service attack)	0.1%	-
異常検知(Anomaly Detection)	0.0%	-

2023年07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1.15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450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400件ぐらい増加し、これはThinkPHP Remote Code Execution Vulnerability攻撃件数増加によるものだと確認できた。

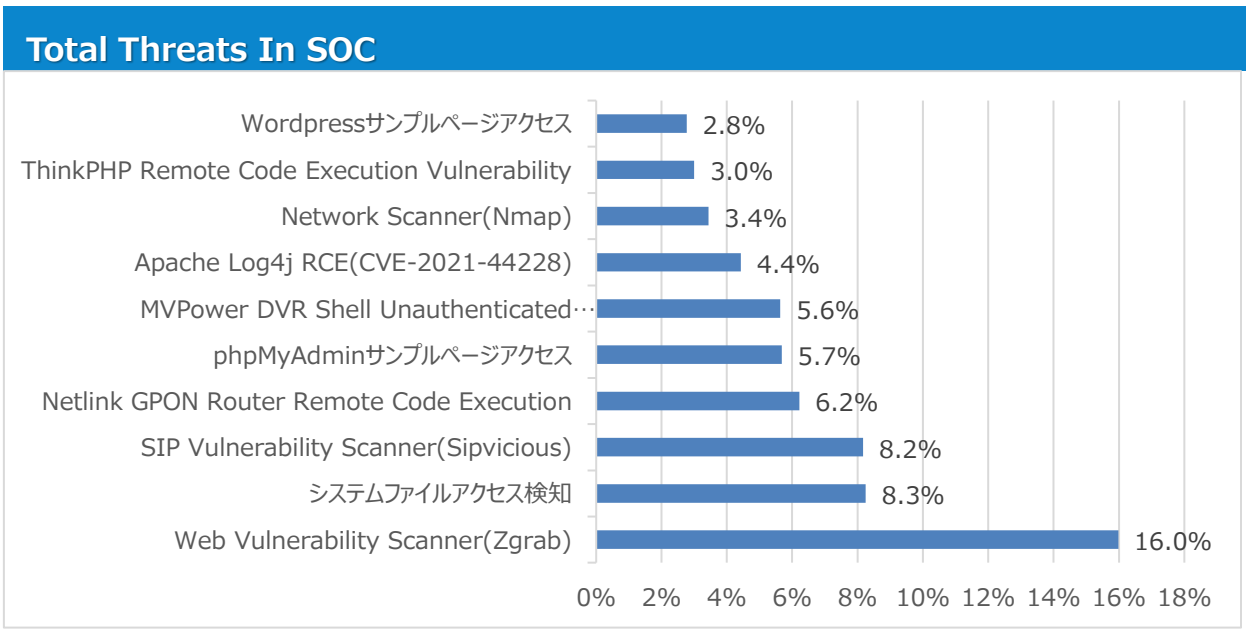


月次攻撃サービスの統計及び分析 - 2023年07月

02. 月次脆弱性攻撃TOP10

2023年07月の月次脆弱性TOP10を確認した結果、 Apache Log4j RCE(CVE-2021-44228), Network Scanner(Nmap), ThinkPHP Remote Code Execution Vulnerability, Wordpressサンプルページアクセス攻撃が新たに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、 Web Vulnerability Scanner(Zgrab)攻撃件数が210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)	16.0%	-
2	システムファイルアクセス検知	8.3%	▲3
3	SIP Vulnerability Scanner(Sipvicious)	8.2%	▲1
4	Netlink GPON Router Remote Code Execution	6.2%	▼1
5	phpMyAdminサンプルページアクセス	5.7%	▲1
6	MVPower DVR Shell Unauthenticated Command Execution	5.6%	▼4
7	Apache Log4j RCE(CVE-2021-44228)	4.4%	NEW
8	Network Scanner(Nmap)	3.4%	NEW
9	ThinkPHP Remote Code Execution Vulnerability	3.0%	NEW
10	Wordpressサンプルページアクセス	2.8%	NEW



月次攻撃サービスの統計及び分析 - 2023年07月

03. 月次ブラックリストIPアドレスTOP 10

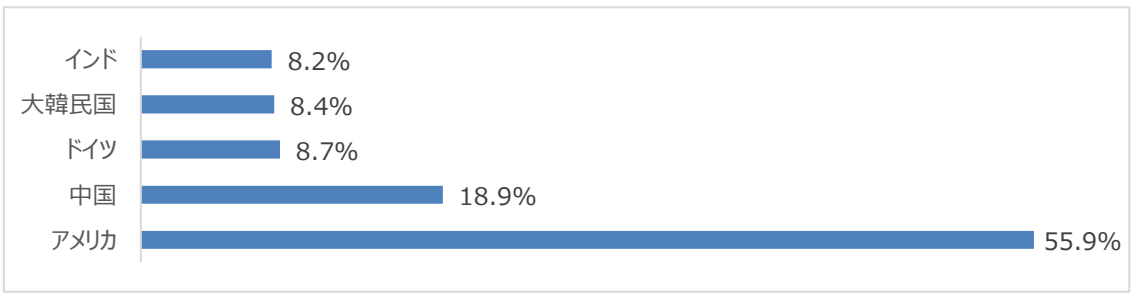
2023年07月についてTOP10を確認した結果、ドイツと大韓民国の攻撃比率が増加し、一方アメリカと中国、インドの攻撃の比率は減少した。特にアメリカと中国の攻撃比率が合わせて約46.1%ぐらいで攻撃のほぼ半分ぐらいを占めていることが確認できた。

※ 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	45.134.144.57	US	SIP Vulnerability Scanner(Sipvicious)
2	83.97.73.89	DE	Synacor Zimbra Collaboration Suite autodiscover XXE(CVE-2019-9670)
3	109.237.97.180	GB	システムファイルアクセス検知
4	95.214.27.51	NL	システムファイルアクセス検知
5	193.35.18.177	NL	Application Vulnerability(PHPUnit)
6	192.227.196.131	US	SIP Vulnerability Scanner(Sipvicious)
7	109.237.98.226	GB	システムファイルアクセス検知
8	195.90.116.158	FR	Command Injection
9	45.134.144.113	US	SIP Vulnerability Scanner(Sipvicious)
10	45.155.91.84	PL	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
1	45.134.144.57	US
2	83.97.73.89	DE
3	109.237.97.180	GB
4	95.214.27.51	NL
5	193.35.18.177	NL

Rank	Source IP	Country
6	192.227.196.131	US
7	109.237.98.226	GB
8	195.90.116.158	FR
9	45.134.144.113	US
10	45.155.91.84	PL

攻撃パターン毎の詳細分析結果

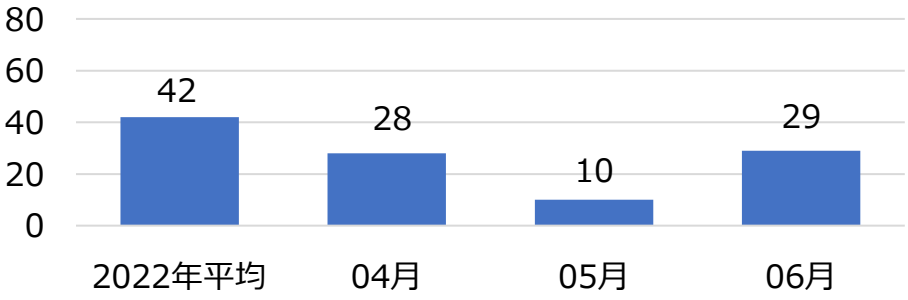
07月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。.
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。
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。
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。
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。
Network Scanner(Nmap)	代表的なNetwork Scanツールで、IP ScanとPort Scanの機能がある。ネットワーク脆弱性診断ツールとして活用されるが攻撃者から悪用されて攻撃ツールとして使用される。
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード 実行攻撃ができる脆弱性である。¥think¥*クラスを呼び出して脆弱なオブジェクトを介して攻撃 者は任意のPHPコード及びシステムコマンドが実行できる。
Wordpress サンプルページ アクセス	Wordpressのログインページである「wp-login.php, wp-admin.php, wp-config.php」やサ ンプルページにアクセスするイベントで主にページの有無を確認するためのアクセスである。

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06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29件である。
06月1か月の間、VeeamBackup資格証明盗用スクリプト、MS SharePoint(CVE-2023-29357)、
MOVEit Transfer(CVE-2023-34362)などに対する検知ポリシーが配布された。



3か月間件数

6,188
全体配布量

29
今月配布量

10
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 $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.28.06202 Veeam Backup, Misc activity"; flow:to_client,established; file_data; content:"Veeam Backup and Replication"; fast_pattern:only; content:".SqlServerName"; nocase; content:"SELECT"; nocase; content:"FROM"; nocase; content:".[dbo].[Credentials]"; nocase; sid:2806202;)	Veeam Backup Server資格証明盗用スクリプトダウンロード試みを検知するポリシー	Veeam Backup
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06205 SERVER-WEBAPP, Microsoft, SharePoint, CVE-2023-29357, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"Authorization|3A|"; nocase; http_header; content:"Bearer"; within:500; http_header; base64_decode:bytes 100,offset 1,relative; base64_data; content:"|22|alg|22|"; nocase; content:"|22|none|22|"; within:50; nocase; content:"/_vti_bin/"; fast_pattern:only; http_uri; sid:106205;)	Microsoft SharePointの脆弱性であるCVE-2023-29357を悪用したOAuth認証迂回試みを検知するポリシー	SERVER-WEBAPP, Microsoft, SharePoint, CVE-2023-29357
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.06206 SERVER-WEBAPP, MOVEit, Transfer, CVE-2023-34362, Web Application Attack"; flow:to_server,established; content:"moveitisapi.dll"; fast_pattern:only; http_uri; content:"action=m2"; nocase; http_uri; content:"x-silock-transaction"; nocase; http_header; content:"X-siLock-Transaction"; distance:0; nocase; http_header; content:"folder_add_by_path"; nocase; http_header; content:"session_setvars"; nocase; http_header; sid:1006206;)	MOVEit Transferの脆弱性であるCVE-2023-34362を悪用したサーバ側のリクエストなりすまし試みを検知するポリシー	SERVER-WEBAPP, MOVEit, Transfer, CVE-2023-34362
alert tcp any $HTTP_PORTS -> any any (msg:"IGRSS.8.06221 Malware, Backdoor, MovelTShell, A Network Trojan was detected"; flow:to_client,established; content:"X-siLock-Comment"; fast_pattern:only; http_header; sid:806221;)	MovelTShellのネットワーク通信を検知するポリシー	Malware, Backdoor, MovelTShell