SECURITY REPORT

2023

SEP

2023年09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09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。

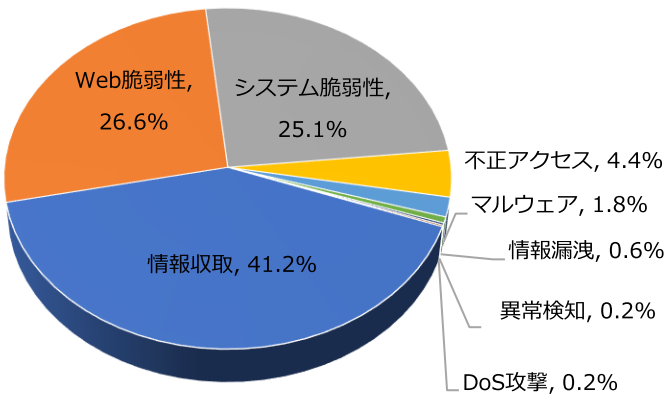
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	41.2%	▲2
Web脆弱性(Web Vulnerability)	26.6%	▼1
システム脆弱性(System Vulnerability)	25.1%	▼1
不正アクセス(Unauthorized access)	4.4%	-
マルウェア(Malware)	1.8%	-
情報漏洩(Information Exposure)	0.6%	-
異常検知(Anomaly Detection)	0.2%	▲1
DoS攻撃(Denial of service attack)	0.2%	▼1

2023年09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0.4倍ぐらい減少し、全体の攻撃件数が減少した。

そのうち、Web脆弱性に関する攻撃は先月比べて約12,000件ほど減少し、これはPUT method Detection攻撃件数の減少によるものだと確認できた。

一方、情報収集に関する攻撃は先月と比べて約350件ぐらい増加し、これはNetwork Scanner(Nmap)攻撃件数増加によるものだと確認できた。

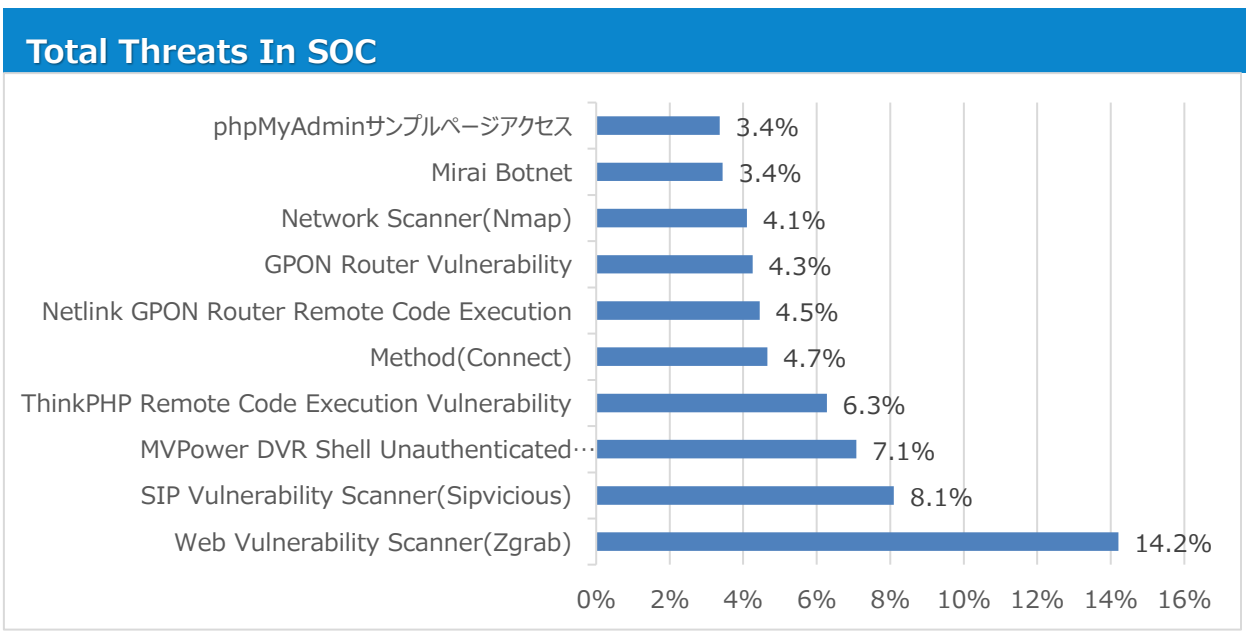


月次攻撃サービスの統計及び分析 - 2023年09月

02. 月次脆弱性攻撃TOP10

2023年09月の月次脆弱性TOP10を確認した結果、 Mirai Botnet, phpMyAdmin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10,000件ぐらい減少したことが確認できた。

順位	検知名	比率(%)	比較
1	Web Vulnerability Scanner(Zgrab)	14.2%	▲3
2	SIP Vulnerability Scanner(Sipvicious)	8.1%	▲3
3	MVPower DVR Shell Unauthenticated Command Execution	7.1%	▼1
4	ThinkPHP Remote Code Execution Vulnerability	6.3%	▲2
5	Method(Connect)	4.7%	▲3
6	Netlink GPON Router Remote Code Execution	4.5%	▲1
7	GPON Router Vulnerability	4.3%	▼4
8	Network Scanner(Nmap)	4.1%	▲1
9	Mirai Botnet	3.4%	NEW
10	phpMyAdminサンプルページアクセス	3.4%	NEW



月次攻撃サービスの統計及び分析 - 2023年09月

03. 月次ブラックリストIPアドレスTOP 10

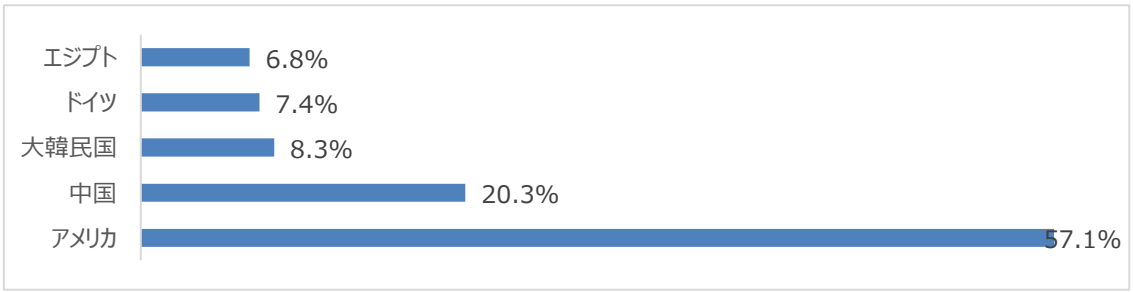
2023年09月についてTOP10を確認した結果、アメリカと中国、大韓民国、ドイツの攻撃比率が増加し、一方エジプトの攻撃の比率は減少した。特にアメリカと中国のの攻撃比率が合わせて約50%ぐらいあることが確認できた。

※ 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	83.97.73.87	RU	Application Vulnerability(PHPUnit)
2	84.54.51.12	NL	Method(Connect)
3	92.204.145.83	US	SIP Vulnerability Scanner(Sipvicious)
4	45.134.144.113	US	SIP Vulnerability Scanner(Sipvicious)
5	151.106.41.111	NL	SIP Vulnerability Scanner(Sipvicious)
6	92.204.136.167	US	SIP Vulnerability Scanner(Sipvicious)
7	2.59.254.9	NL	Web Vulnerability Scanner(Zgrab)
8	45.93.16.153	US	SIP Vulnerability Scanner(Sipvicious)
9	137.74.19.133	NL	SIP Vulnerability Scanner(Sipvicious)
10	45.88.90.113	NL	Netlink GPON Router Remote Code Execution

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	137.74.19.132	NL	6	213.109.202.66	RU
2	45.93.16.217	US	7	45.155.91.249	PL
3	45.134.144.113	US	8	45.128.232.176	NL
4	84.54.51.12	NL	9	195.90.116.158	FR
5	137.74.19.133	NL	10	109.206.242.25	US

攻撃パターン毎の詳細分析結果

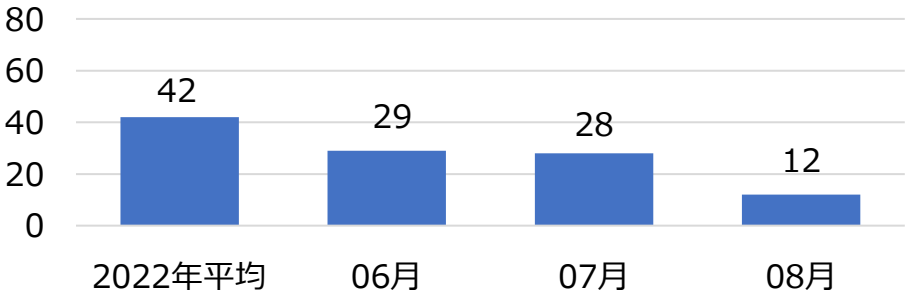
09月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。.
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。
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。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security)トンネリングは内部にアクセ スをする。このため、Connect Methodを使用していて、脆弱性が存在する場合、中間経由地として使 用される可能性がある。
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。
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。
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。
Mirai Botnet	Mirai botnetはモノのインターネット(IoT)機器をゾンビ化させてネットワークからハッカーが自由に操作できるようにするボットネット(Botnet)の一つである。
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。

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08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12件である。
08月1か月の間、MOVEit(CVE-2023-34362), htmlunit(CVE-2023-26119), QuiteRAT, Lazarus 変種Malwareなどに対する検知ポリシーが配布された。



3か月間件数

6,228
全体配布量

12
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 $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06255 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-SessVar"; nocase; http_header; pcre:"/^X-siLock-SessVar[^¥r¥n]*?([¥x27¥x22¥x3b¥x23¥x28]|%(25)?(27|22|3b|23|28)|(¥x2f|%(25)?2f)(¥x2a|%(25)?2a)|(¥x2d|%(25)?2d){2})/Him"; sid:1006255;)	MOVEit Transferの脆弱性であるCVE-2023-34362を悪用したSQL Injection攻撃を検知するポリシー	SERVER-WEBAPP, MOVEit, Transfer, CVE-2023-34362
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06257 Malware, CNC, QuiteRAT, A Network Trojan was detected"; flow:to_server,established; content:"/resource/main/rawmail.php"; fast_pattern:only; http_uri; content:"mailid"; nocase; http_uri; content:"action"; nocase; http_uri; content:"param"; nocase; http_uri; content:"session"; nocase; http_uri; sid:806257;)	QuiteRAT変種Malwareのネットワーク通信を検知するポリシー	Malware, CNC, QuiteRAT
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06260 Malware, CNC, Lazarus, A Network Trojan was detected"; flow:to_server,established; content:"/boards/boardindex.php"; fast_pattern:only; http_uri; content:"plan="; nocase; http_uri; content:"page="; nocase; http_uri; sid:806260;)	Lazarus変種Malwareのネットワーク通信を検知するポリシー	Malware, CNC, Lazarus
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.2.06264 FILE-OTHER, htmlunit, CVE-2023-26119, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"<xsl:stylesheet"; fast_pattern:only; content:"java.lang.Runtime"; nocase; content:":exec("; nocase; content:":getRuntime()"; nocase; content:"<xsl:value-of"; nocase; sid:206264;)	htmlunit脆弱性でくあるCVE-2023-26119を悪用したユーザー権限上昇を検知するポリシー	FILE-OTHER, htmlunit, CVE-2023-26119