SECURITY REPORT

2023

OCT

2023年10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10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。

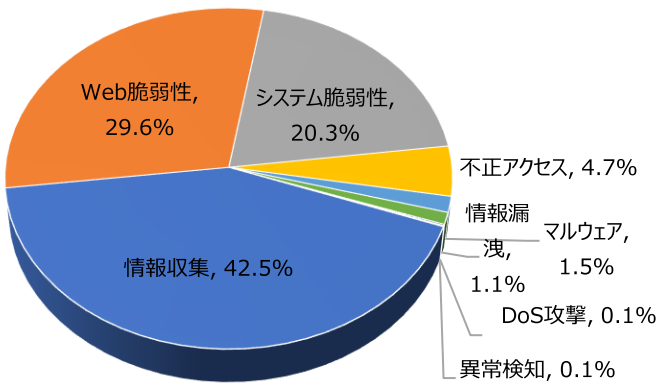
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	42.5%	-
Web脆弱性(Web Vulnerability)	29.6%	-
システム脆弱性(System Vulnerability)	20.3%	-
不正アクセス(Unauthorized access)	4.7%	-
マルウェア(Malware)	1.5%	-
情報漏洩(Information Exposure)	1.1%	-
DoS攻撃(Denial of service attack)	0.1%	▲1
異常検知(Anomaly Detection)	0.1%	▼1

2023年10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1.07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400件ほど増加し、これはNetwork Scanner(Nmap)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470件ぐらい増加し、これはphpMyAdminサンプルページアクセス攻撃件数増加によるものだと確認できた。

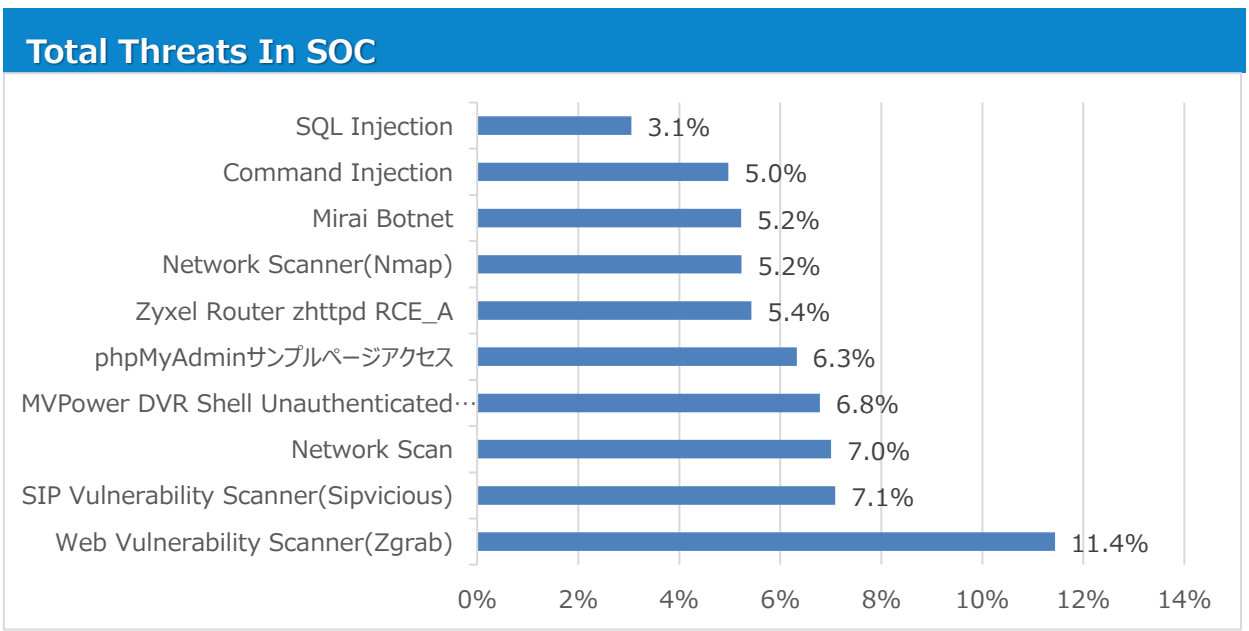


月次攻撃サービスの統計及び分析 - 2023年10月

02. 月次脆弱性攻撃TOP10

2023年10月の月次脆弱性TOP10を確認した結果、Network Scan, Zyxel Router zhttpd RCE_A, Command Injection, SQL Injection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。しかし、Web Vulnerability Scanner(Zgrab)攻撃件数は先月と比べて約200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)	11.4%	-
2	SIP Vulnerability Scanner(Sipvicious)	7.1%	-
3	Network Scan	7.0%	NEW
4	MVPower DVR Shell Unauthenticated Command Execution	6.8%	▼1
5	phpMyAdminサンプルページアクセス	6.3%	▲5
6	Zyxel Router zhttpd RCE_A	5.4%	NEW
7	Network Scanner(Nmap)	5.2%	▲1
8	Mirai Botnet	5.2%	▲1
9	Command Injection	5.0%	NEW
10	SQL Injection	3.1%	NEW



月次攻撃サービスの統計及び分析 - 2023年10月

03. 月次ブラックリストIPアドレスTOP 10

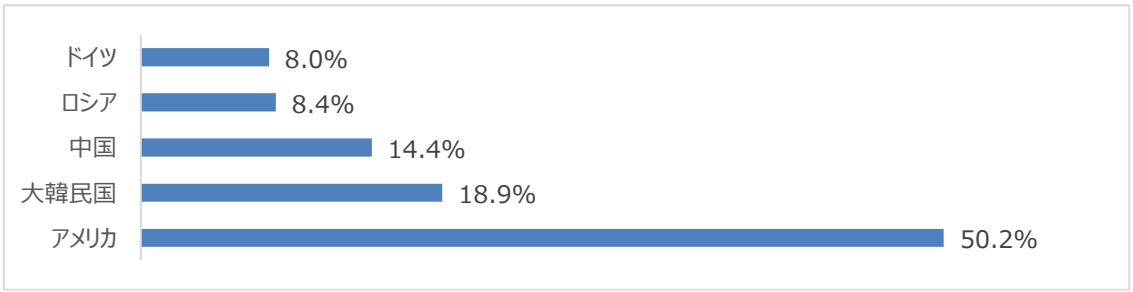
2023年10月についてTOP10を確認した結果、大韓民国、ロシア、ドイツ攻撃比率が増加し、一方アメリカと中国の攻撃の比率は減少した。特にアメリカの攻撃比率が合わせて約50%ぐらいを超えることが確認できた。

※ 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	80.76.51.163	NL	Command Injection
2	92.63.196.30	RU	Network Scan
3	45.134.144.113	HK	SIP Vulnerability Scanner(Sipvicious)
4	61.77.39.173	KR	Zyxel Router zhttpd RCE_A
5	92.63.196.28	RU	Network Scan
6	83.97.73.87	RU	Synacor Zimbra Collaboration Suite autodiscover XXE (CVE-2019-9670)
7	45.93.16.86	US	SIP Vulnerability Scanner(Sipvicious)
8	92.63.196.29	RU	Network Scan
9	92.63.196.92	RU	Network Scan
10	103.127.78.55	IN	Command Injection

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	80.76.51.163	NL	6	83.97.73.87	RU
2	92.63.196.30	RU	7	45.93.16.86	US
3	45.134.144.113	HK	8	92.63.196.29	RU
4	61.77.39.173	KR	9	92.63.196.92	RU
5	92.63.196.28	RU	10	103.127.78.55	IN

攻撃パターン毎の詳細分析結果

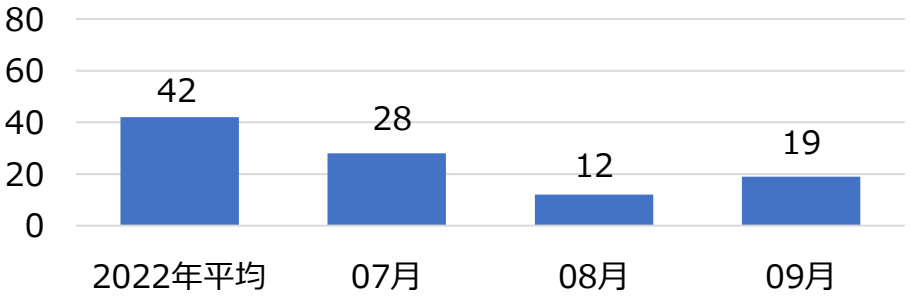
10月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。.
Network Scan	ネットワーク脆弱性スキャン攻撃は送信先の多数のシステムに対してシステムそのもののバグ、構成上の問題点などハッキング可能なシステムのセキュリティ脆弱性を調べるための攻撃で、一番頻繁に行われる攻撃である。
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。
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。
Zyxel Router zhttpd RCE_A	Zyel RouterにREC(Remote Code Execution)脆弱性が存在する。当該の脆弱性は/bin/zhttpd/パスにユーザーの入力値の不適切な有効性の検証で発生する。リモート攻撃者は悪意的に操作されたリクエストを送信して攻撃できる。攻撃成功時、任意のコードが実行できる。
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。
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。
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。
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。

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09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19件である。09月1か月の間、Adobe ColdFusion(CVE-2023-26359, CVE-2023-26360), Ivanti MobileIron Sentry(CVE-2023-38035), PhoenixMiner 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

6,247
全体配布量

19
今月配布量

12
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,8500] (msg:"IGRSS.2.06266 SERVER-WEBAPP, Adobe, ColdFusion, CVE-2023-26359, Attempted User Privilege Gain"; flow:to_server,established; content:".cfc"; fast_pattern:only; http_uri; content:"_variables"; nocase; http_client_body; content:"_metadata"; nocase; http_client_body; content:"classname"; nocase; http_client_body; pcre:"/(^|&)_variables=[^&]*?(¥x22|%(25)?22)_metadata(¥x22|%(25)?22)¥s*?(:|%(25)?3A)¥s*?(¥x7B|%(25)?7B)¥s*?(¥x22|%(25)?22)classname(¥x22|%(25)?22)/Pi"; sid:206266;)	Adobe ColdFusionのCVE-2023-26359脆弱性を悪用したコード実行攻撃を検知するポリシー	SERVER-WEBAPP, Adobe, ColdFusion, CVE-2023-26359
alert tcp $EXTERNAL_NET any -> $HOME_NET [$HTTP_PORTS,8500] (msg:"IGRSS.2.06267 SERVER-WEBAPP, Adobe, ColdFusion, CVE-2023-26360, Attempted User Privilege Gain"; flow:to_server,established; content:".cfc"; fast_pattern:only; http_uri; content:"Content-Disposition"; nocase; http_client_body; content:"|22|_metadata|22|"; nocase; http_client_body; content:"|22|classname|22|"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?(_variables|argumentCollection)((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?¥x22_metadata¥x22¥s*?:¥s*?¥x7B¥s*?¥x22classname¥x22/Pims"; sid:206267;)	Adobe ColdFusionのCVE-2023-2636脆弱性を悪用したコード実行攻撃を検知するポリシー	SERVER-WEBAPP, Adobe, ColdFusion, CVE-2023-26360
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06280 SERVER-WEBAPP, Ivanti, Sentry, CVE-2023-38035, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/mics/services/MICSLogService"; fast_pattern:only; http_uri; content:"uploadFileUsingFileInput"; nocase; http_client_body; content:"command"; nocase; http_client_body; sid:106280;)	Ivanti MobileIron Sentry의 CVE-2023-38035 脆弱性を悪用したコマンド実行攻撃を検知するポリシー	SERVER-WEBAPP, Ivanti, Sentry, CVE-2023-38035
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06281 Malware, Dropper, PhoenixMiner, A Network Trojan was detected"; flow:to_server,established; content:"/?smd_process_download=1&download_id=90"; fast_pattern:only; http_uri; sid:806281;)	PhoenixMiner Malwareのネットワーク通信を検知するポリシー	Malware, Dropper, PhoenixMiner