SECURITY REPORT

2023

NOV

2023年11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11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。

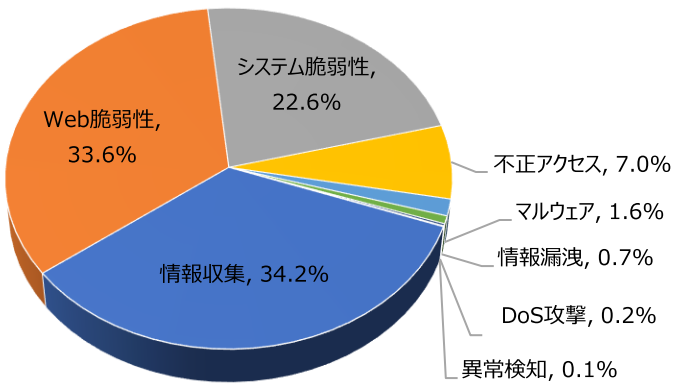
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	34.2%	-
Web脆弱性(Web Vulnerability)	33.6%	-
システム脆弱性(System Vulnerability)	22.6%	-
不正アクセス(Unauthorized access)	7.0%	-
マルウェア(Malware)	1.6%	-
情報漏洩(Information Exposure)	0.7%	-
DoS攻撃(Denial of service attack)	0.2%	-
異常検知(Anomaly Detection)	0.1%	-

2023年11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0.88倍ぐらい減少し、全体の攻撃件数が減少した。

そのうち、情報収集に関する攻撃は先月比べて約1,200件ほど減少し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数の減少によるものだと確認できた。

一方、不正アクセスに関する攻撃は先月と比べて約140件ぐらい増加し、これはシステムファイルアクセス検知攻撃件数増加によるものだと確認できた。

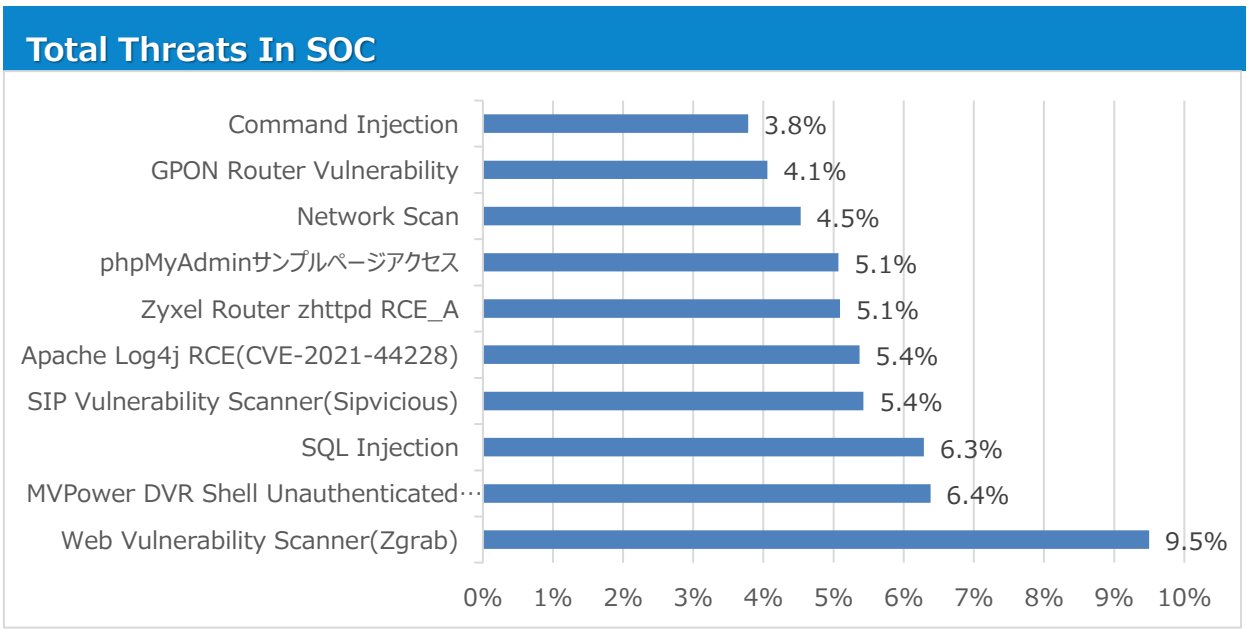


月次攻撃サービスの統計及び分析 - 2023年11月

02. 月次脆弱性攻撃TOP10

2023年11月の月次脆弱性TOP10を確認した結果、Apache Log4j RCE(CVE-2021-44228), GPON Router Vulnerability攻撃が新たにTOP10に登場し、全体的な攻撃件数が減少したことが確認できた。特にWeb Vulnerability Scanner(Zgrab)攻撃件数は先月と比べて約300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)	9.5%	-
2	MVPower DVR Shell Unauthenticated Command Execution	6.4%	▲2
3	SQL Injection	6.3%	▲7
4	SIP Vulnerability Scanner(Sipvicious)	5.4%	▼2
5	Apache Log4j RCE(CVE-2021-44228)	5.4%	NEW
6	Zyxel Router zhttpd RCE_A	5.1%	-
7	phpMyAdminサンプルページアクセス	5.1%	▼2
8	Network Scan	4.5%	▼5
9	GPON Router Vulnerability	4.1%	NEW
10	Command Injection	3.8%	▼1



月次攻撃サービスの統計及び分析 - 2023年11月

03. 月次ブラックリストIPアドレスTOP 10

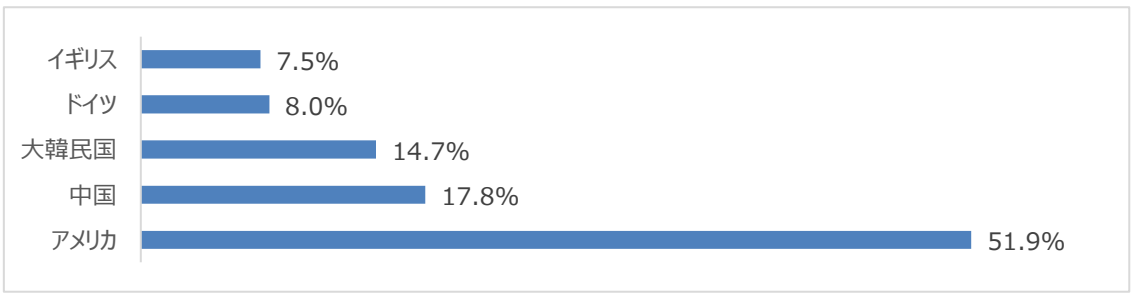
2023年11月についてTOP10を確認した結果、アメリカ、中国、イギリス攻撃比率が増加し、一方大韓民国とドイツの攻撃の比率は減少した。特にアメリカの攻撃比率が合わせて約50%ぐらいを超えることが確認できた。

※ 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	193.35.18.187	DE	Method(Connect)
2	72.251.232.180	US	SIP Vulnerability Scanner(Sipvicious)
3	45.95.147.236	NL	Application Vulnerability(PHPUnit)
4	45.155.91.237	PL	SIP Vulnerability Scanner(Sipvicious)
5	120.63.180.123	IN	TP-Link Router Remote Code Execution(CVE-2023-1389)
6	83.97.73.87	RU	Synacor Zimbra Collaboration Suite autodiscover XXE (CVE-2019-9670)
7	80.76.51.191	NL	Command Injection
8	67.215.234.42	US	SIP Vulnerability Scanner(Sipvicious)
9	23.226.138.26	US	SIP Vulnerability Scanner(Sipvicious)
10	185.91.127.166	NL	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	193.35.18.187	DE	6	83.97.73.87	RU
2	72.251.232.180	US	7	80.76.51.191	NL
3	45.95.147.236	NL	8	67.215.234.42	US
4	45.155.91.237	PL	9	23.226.138.26	US
5	120.63.180.123	IN	10	185.91.127.166	NL

攻撃パターン毎の詳細分析結果

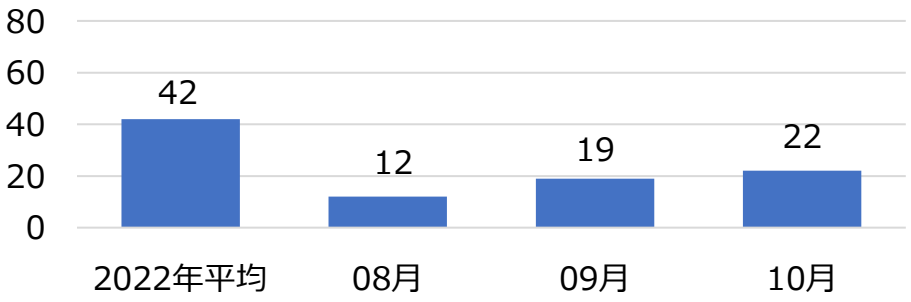
11月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。.
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。
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。
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。
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。
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。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2023年10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22件である。
10月1か月の間、Microsoft SharePoint (CVE-2023-29357), MOVEit (CVE-2023-36934), Ivanti Avalanche (CVE-2023-32563), Atlassian Confluence (CVE-2023-22515)などに対する検知ポリシーが配布された。



3か月間件数

6,269
全体配布量

22
今月配布量

19
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.1.06287 SERVER-WEBAPP, Microsoft, SharePoint, CVE-2023-29357, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"access_token="; nocase; http_client_body; base64_decode:bytes 100,relative; base64_data; content:"|22|alg|22|"; nocase; content:"|22|none|22|"; within:50; nocase; content:"/_layouts/15/"; fast_pattern:only; http_uri; sid:106287;)	Microsoft SharePointの脆弱性であるCVE-2023-29357を悪用したOAuth認証バイパス試みを検知するポリシー	SERVER-WEBAPP, Microsoft, SharePoint, CVE-2023-29357
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06302 SERVER-WEBAPP, MOVEit, CVE-2023-36934, Web Application Attack"; flow:to_server,established; content:"/human.aspx"; fast_pattern:only; http_uri; content:"username"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?username((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?([¥x27¥x22¥x3b¥x23¥x28]|¥x2f¥x2a|(?<!^)¥x2d{2})/Psim"; sid:1006302;)	MOVEitの脆弱性であるCVE-2023-36934を悪用したSQL Injection攻撃を検知するポリシー	SERVER-WEBAPP, MOVEit, CVE-2023-36934
alert tcp $EXTERNAL_NET any -> $HOME_NET [$HTTP_PORTS,1900] (msg:"IGRSS.10.06298 SERVER-WEBAPP, Ivanti, Avalanche, CVE-2023-32563, Web Application Attack"; flow:to_server,established; content:"/Servlet/Skins"; fast_pattern:only; content:"guid"; nocase; content:"Content-Disposition"; nocase; pcre:"/name¥s*=¥s*[¥x22¥x27]?guid((?!^--).)*?¥x2e¥x2e[¥x2f¥x5c]/sim"; sid:1006298;)	Ivanti Avalancheの脆弱性であるCVE-2023-32563を悪用したDirectory Traversal攻撃を検知するポリシー	SERVER-WEBAPP, Ivanti, Avalanche, CVE-2023-32563
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.2.06295 SERVER-WEBAPP, Atlassian, Confluence, CVE-2023-22515, Attempted User Privilege Gain"; flow:to_server,established; content:"bootstrapStatusProvider"; fast_pattern; nocase; http_client_body; content:"applicationConfig"; within:22; nocase; http_client_body; content:"setupComplete"; within:18; nocase; http_client_body; content:"false"; distance:0; nocase; http_client_body; sid:206295;)	Atlassian Confluenceの脆弱性であるCVE-2023-22515を悪用したリモートコマンド実行攻撃を検知するポリシー	SERVER-WEBAPP, Atlassian, Confluence, CVE-2023-22515