SECURITY REPORT

2023

AUG

2023年08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08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。

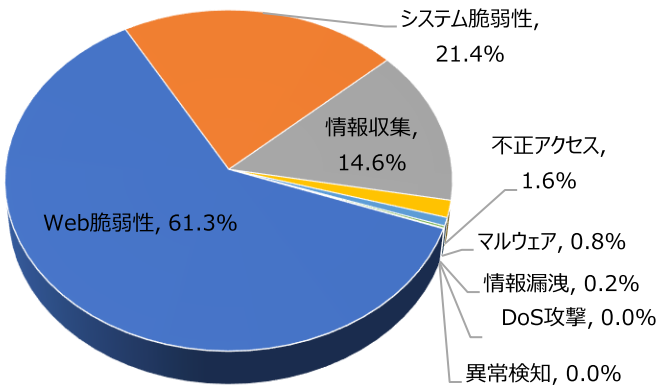
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	61.3%	▲2
システム脆弱性(System Vulnerability)	21.4%	-
情報収集(Information Gathering)	14.6%	▼2
不正アクセス(Unauthorized access)	1.6%	-
マルウェア(Malware)	0.8%	-
情報漏洩(Information Exposure)	0.2%	-
DoS攻撃(Denial of service attack)	0.0%	-
異常検知(Anomaly Detection)	0.0%	-

2023年08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2.17倍ぐらい増加し、全体の攻撃件数が増加した。

そのうち、Web脆弱性に関する攻撃は先月比べて約12,200件ほど増加し、これはPUT method Detection攻撃件数の増加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1,100件ぐらい減少し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数減少によるものだと確認できた。

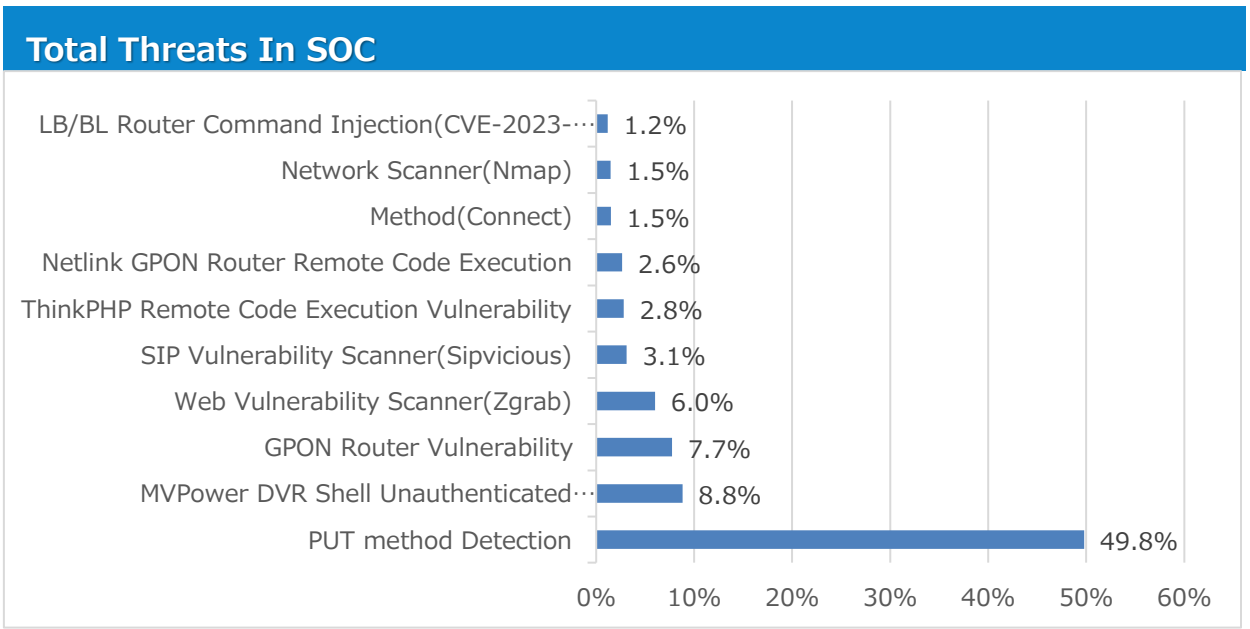


月次攻撃サービスの統計及び分析 - 2023年08月

02. 月次脆弱性攻撃TOP10

2023年08月の月次脆弱性TOP10を確認した結果、 A PUT method Detection, GPON Router Vulnerability, Method(Connect), LB/BL Router Command Injection(CVE-2023-26801)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、PUT method Detection攻撃件数が10,000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	PUT method Detection	49.8%	NEW
2	MVPower DVR Shell Unauthenticated Command Execution	8.8%	▲4
3	GPON Router Vulnerability	7.7%	NEW
4	Web Vulnerability Scanner(Zgrab)	6.0%	▼3
5	SIP Vulnerability Scanner(Sipvicious)	3.1%	▲2
6	ThinkPHP Remote Code Execution Vulnerability	2.8%	▲3
7	Netlink GPON Router Remote Code Execution	2.6%	▼3
8	Method(Connect)	1.5%	NEW
9	Network Scanner(Nmap)	1.5%	▼1
10	LB/BL Router Command Injection(CVE-2023-26801)	1.2%	NEW



月次攻撃サービスの統計及び分析 - 2023年08月

03. 月次ブラックリストIPアドレスTOP 10

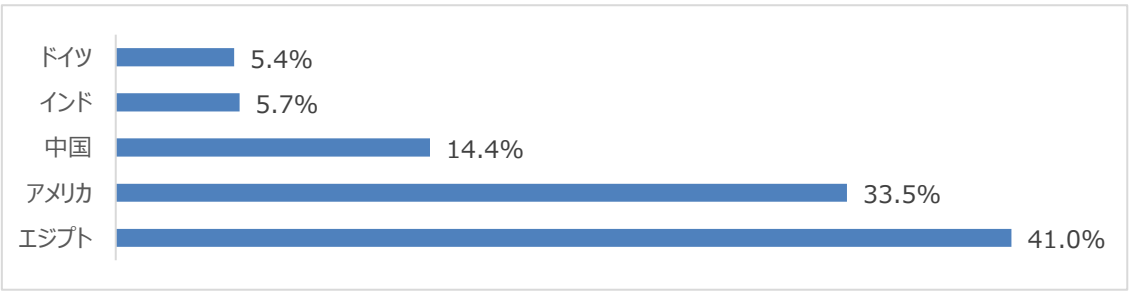
2023年08月についてTOP10を確認した結果、エジプトの攻撃比率が増加し、一方アメリカと中国、インドの攻撃の比率は減少した。特にエジプトの攻撃比率が合わせて約29%ぐらいで約3,300件ぐらい増加したことが確認できた。

※ 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	137.74.19.132	NL	SIP Vulnerability Scanner(Sipvicious)
2	45.93.16.217	US	SIP Vulnerability Scanner(Sipvicious)
3	45.134.144.113	US	SIP Vulnerability Scanner(Sipvicious)
4	84.54.51.12	NL	Method(Connect)
5	137.74.19.133	NL	SIP Vulnerability Scanner(Sipvicious)
6	213.109.202.66	RU	Synacor Zimbra Collaboration Suite autodiscover XXE (CVE-2019-9670)
7	45.155.91.249	PL	SIP Vulnerability Scanner(Sipvicious)
8	45.128.232.176	NL	Method(Connect)
9	195.90.116.158	FR	Command Injection
10	109.206.242.25	US	PHP-CGI Vulnerability (CVE-2012-1823)

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	137.74.19.132	NL
2	45.93.16.217	US
3	45.134.144.113	US
4	84.54.51.12	NL
5	137.74.19.133	NL

Rank	Source IP	Country
6	213.109.202.66	RU
7	45.155.91.249	PL
8	45.128.232.176	NL
9	195.90.116.158	FR
10	109.206.242.25	US

攻撃パターン毎の詳細分析結果

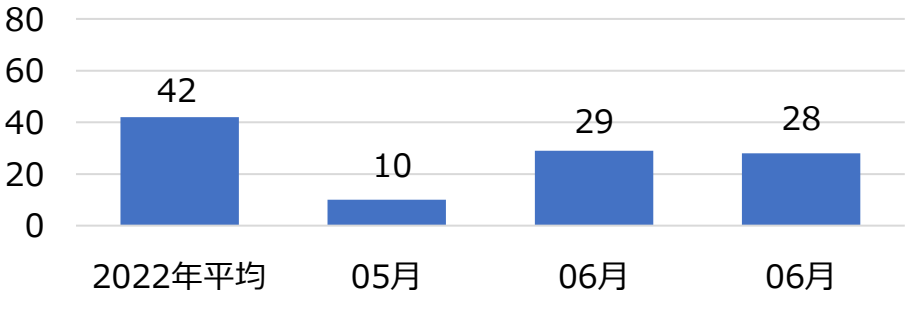
08月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
PUT method Detection	Methodはウェブアプリケーションからデフォルトで提供するクライアントと通信をするためのツールでGET, POST, PUT, MOVE, DELETEなど様々なMethodがある。Methodに対する制限がない場合ファイル生成 (PUT)、削除(DELETE)、トンネリングアクセス(CONNECT)などの動作ができる。
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。
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。
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。.
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。
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。
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。
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。
LB/BL Router Command Injection(CVE-2023-26801)	LB-LINK BL-AC1900_2.0 V1.0.1, BL-WR9000 V2.4.9, BL-X26 V1.2.5 and BL-LTE300 V1.0.8 Wireless RoutersはCommand injection脆弱性が含まれていることが確認できた。この脆弱性はmacパラメータの緩い検査によって発生する。この脆弱性を悪用して権限がない攻撃者が /goform/set_LimitClient_cfgを要請時、リモートで任意のコマンドを実行して送信することができる。

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07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28件である。06月1か月の間、Safari (CVE-2022-22620), Zoho(CVE-2022-28219), MS Exchange(CVE-2021-26858), SolarView(CVE-2022-29303)などに対する検知ポリシーが配布された。



3か月間件数

6,216
全体配布量

28
今月配布量

29
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 -> $SMTP_SERVERS 25 (msg:"IGRSS.2.06225 Apple, Safari, CVE-2022-22620, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"history.pushState"; fast_pattern; content:"location"; within:50; content:"|23|"; within:50; content:"|2E|focus"; distance:0; content:"|2E|onblur"; distance:0; content:"history.replaceState"; within:100; content:"setTimeout"; distance:0; content:"history.back"; within:100; sid:206225;)	SafariブラウザのCVE-2022-22620脆弱性を悪用したUAF攻撃を検知するポリシー	Apple, Safari, CVE-2022-22620
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06228 SERVER-WEBAPP, Zoho, ManageEngine, CVE-2022-28219, Web Application Attack"; flow:to_server,established; content:"/cewolf"; fast_pattern:only; http_uri; content:"img"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?img((?!^--).)*?¥x2e¥x2e[¥x2f¥x5c]/Pims"; sid:1006228;)	Zoho ManageEngineの脆弱性であるCVE-2022-28219を悪用したリモートコード実行攻撃を検知するポリシー	SERVER-WEBAPP, Zoho, ManageEngine, CVE-2022-28219
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06236 MS, Exchange, CVE-2021-26858, Web Application Attack"; flow:to_server,established; content:"/mapi/emsmdb"; fast_pattern:only; http_uri; content:"X-RequestType: Execute"; nocase; http_header; content:"|00 00 04 00|"; depth:4; offset:8; http_client_body; content:"|2D|"; within:1; distance:6; http_client_body; content:"JScript"; distance:0; nocase; http_client_body; content:"eval(Request["; distance:0; nocase; http_client_body; sid:1006236;)	MS ExchangeのCVE-2021-26858脆弱性を悪用したリモートコード実行攻撃を検知するポリシー	MS, Exchange, CVE-2021-26858
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06238 SERVER-WEBAPP, SolarView, CVE-2022-29303, Attempted User Privilege Gain"; flow:to_server,established; content:"/conf_mail.php"; fast_pattern:only; http_uri; content:"address"; nocase; http_cookie; pcre:"/mail(¥x5f|%(25)?5f)address=[^¥x3b¥r¥n]*?([¥x60¥x7c¥x23]|%(25)?(60|3b|7c|23|26|0a)|([¥x3c¥x3e¥x24]|%(25)?(3c|3e|24))(¥x28|%(25)?28))/Ci"; sid:206238;)	SolarViewのCVE-2022-29303脆弱性を悪用したリモートコード実行攻撃を検知するポリシー	SERVER-WEBAPP, SolarView, CVE-2022-29303