SECURITY REPORT

2022

AUG

2022年8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 - 2022年8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。

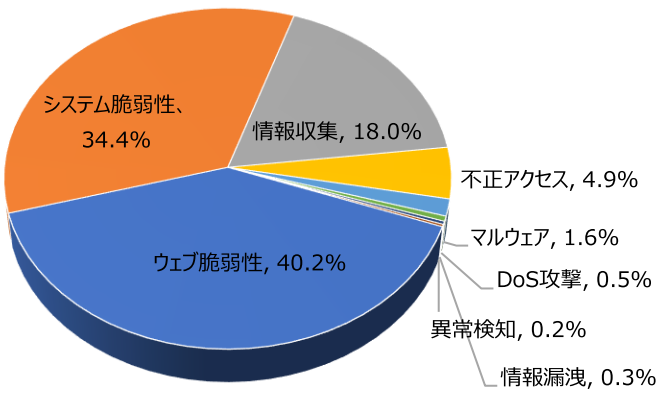
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	40.2%	-
システム脆弱性(System Vulnerability)	34.4%	-
情報収集(Information Gathering)	18.0%	-
不正アクセス(Unauthorized access)	4.9%	-
マルウェア(Malware)	1.6%	-
Dos攻撃(Denial of service attack)	0.5%	-
情報漏洩(Information Exposure)	0.3%	-
異常検知(Anomaly Detection)	0.2%	-

2022年8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1.05倍ぐらい増加し、それぞれの攻撃パターン件数も増加していることが確認できた。

このうち、ウェブ脆弱性に関する攻撃は先月比べて約100件ほど増加し、これはThinkPHP Remote Code Execution Vulnerability攻撃件数の減少によるものだと確認できた。

また、システム脆弱性に関する攻撃は先月と比べて約200件ぐらい増加し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃件数増加によるものだと確認できた。



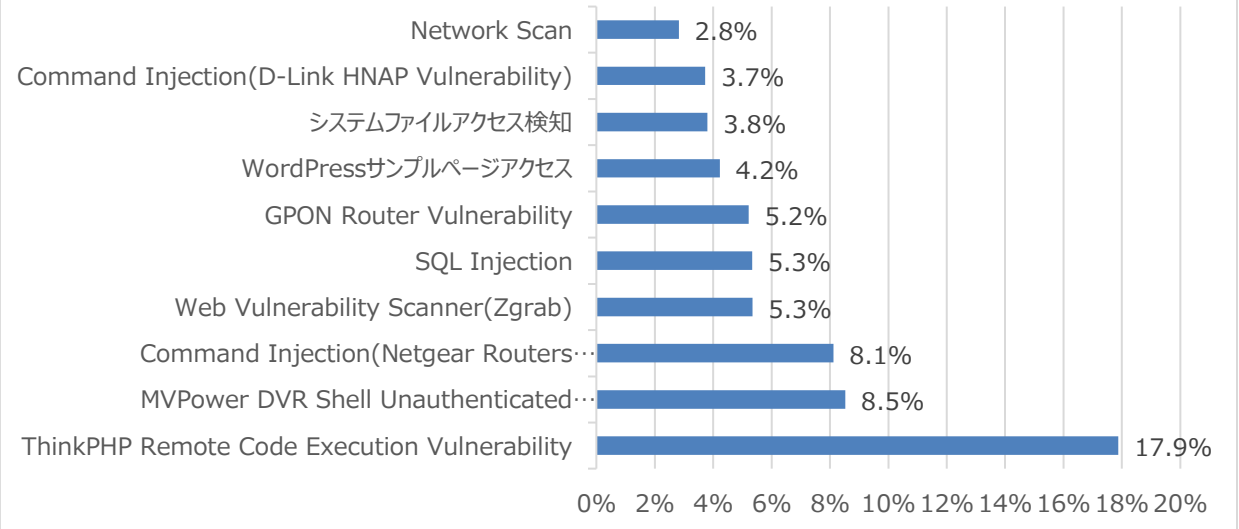
月次攻撃サービスの統計及び分析 - 2022年8月

02. 月次脆弱性攻撃TOP10

2022年8月の月次脆弱性TOP10を確認した結果、 Web Vulnerability Scanner(Zgrab)とNetwork Scan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MVPower DVR Shell Unauthenticated Command Execution攻撃が先月と比べて700ぐらい大幅に増加した。

順位	検知名	比率(%)	比較
1	ThinkPHP Remote Code Execution Vulnerability	17.9%	-
2	MVPower DVR Shell Unauthenticated Command Execution	8.5%	▲6
3	Command Injection (Netgear Routers Vulnerability)	8.1%	-
4	Web Vulnerability Scanner(Zgrab)	5.3%	NEW
5	SQL Injection	5.3%	▲5
6	GPON Router Vulnerability	5.2%	-
7	WordPressサンプルページアクセス	4.2%	▲2
8	システムファイルアクセス検出	3.8%	▼3
9	Command Injection (D-Link HNAP Vulnerability)	3.7%	▼2
10	Network Scan	2.8%	NEW

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2022年8月

03. 月次ブラックリストIPアドレスTOP 10

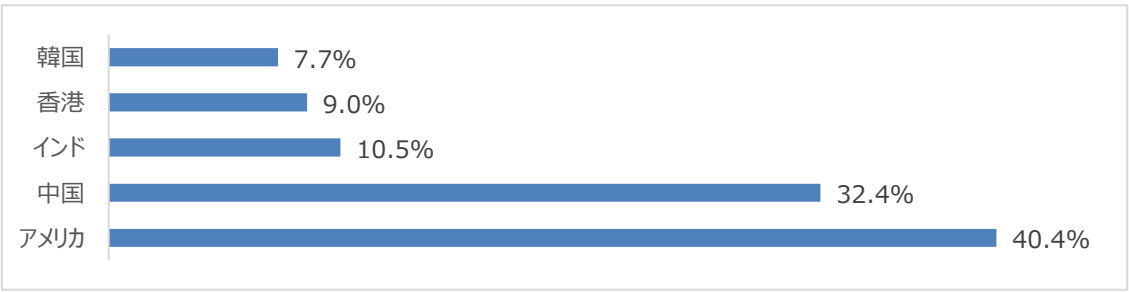
2022年8月についてTOP10を確認した結果、アメリカ、インド、香港、韓国の攻撃比率が増加し、一方中国の攻撃の比率は減少した。アメリカと中国の攻撃比率の合計は全体に比べて約45%で、半分に少し足りないぐらい減少したことが確認できた。

※ 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	141.255.162.201	CH	Apache Log4j RCE(CVE-2021-44228)
2	49.143.32.6	KR	Command Injection(Netgear Routers Vulnerability)
3	92.255.85.38	RU	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
4	95.161.131.235	RU	Web Vulnerability Scanner(Zgrab)
5	13.89.48.118	US	Application Vulnerability(PHPUnit)
6	45.134.144.140	US	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
7	185.53.90.45	NL	Network Scan
8	65.49.27.190	US	Apache Log4j RCE(CVE-2021-44228)
9	103.145.13.58	NL	SIP Vulnerability Scanner(Sipvicious)
10	52.18.4.40	IE	Network Scan

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	141.255.162.201	CH
2	49.143.32.6	KR
3	92.255.85.38	RU
4	95.161.131.235	RU
5	13.89.48.118	US

Rank	Source IP	Country
6	45.134.144.140	US
7	185.53.90.45	NL
8	65.49.27.190	US
9	103.145.13.58	NL
10	52.18.4.40	IE

攻撃パターン毎の詳細分析結果

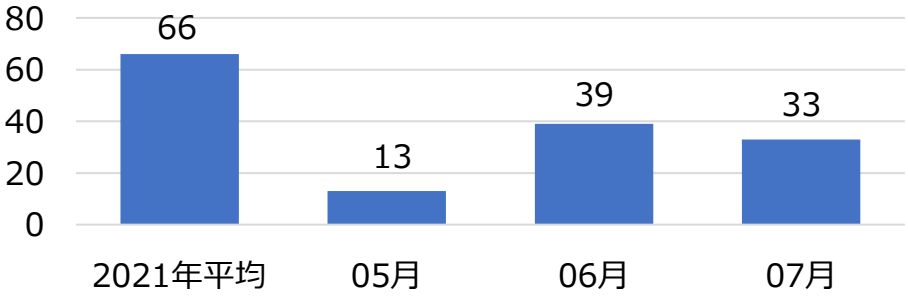
8月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
CommandInjection (Netgear Routers Vulnerability)	NetGear DGNシリーズのルータ内のウェブサーバが一部のURLに対して認証をせず、「setup.cgi」スクリプトの「syscmd」機能を活用して任意のコマンドを実行することができる。
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。
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。
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。 当該の脆弱性を利用して認証されていない攻撃者が機器へリモートでコマンドを実行し、DNS設定修正などの様々な攻撃が可能である。 この脆弱性は家庭用ルータにて発見された。
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。
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。
Command Injection (D-Link HNAP Vulnerability)	D-Link製品を設置する際に使用されるHNAP(Home Network Administration Protocol)に関 するスクリプトに存在する脆弱性で認証を迂回してサービス中止、バックドアインストールなどのコマンドの実 行が可能になる。
Network Scan	ネットワーク脆弱性スキャン攻撃はリモートからシステムのバグ、構成上の問題などハッキングできるセキュリティ脆弱性を確認するための攻撃であり、一番頻繁に発生する攻撃である。

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、2022年7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33件である。
7月1か月の間、Atlassian Confluence(CVE-2022-26138)脆弱性及びL Apple Safari(CVE-2022-22620), CrimsonRATに対する検知ポリシーが配布された。



3か月間件数

5,840
全体配布量

33
今月配布量

39
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.2.05845 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:205845;)	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 $HOME_NET any -> $EXTERNAL_NET any (msg:"IGRSS.8.05852 Malware, CrimsonRAT, A Network Trojan was detected"; flow:to_server,established; content:"|00 00 00 00|Chairtabkjh-"; fast_pattern:only; sid:805852;)	CrimsonRAT Malwareの ネットワーク通信を検知するポリシー	Malware, CrimsonRAT
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.05869 Atlassian, Confluence, CVE-2022-26138, Web Application Attack"; flow:to_server,established; content:"disabled1system1user6708"; fast_pattern:only; http_uri; content:"disabledsystemuser"; nocase; http_uri; sid:1005869;)	Atlassian Confluenceの CVE-2022-26138脆弱性を悪用した Chopper JSP Webshellネットワーク通信 を検知するポリシー	Atlassian, Confluence, CVE-2022-26138
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05874 Webshell, php, Cybershell, A Network Trojan was detected"; flow:to_server,established; content:".php?downloadfile="; fast_pattern:only; http_uri; sid:805874;)	Cybershell PHP Webshellの ネットワーク通信を検知するポリシー	Webshell, php, Cybershell