SECURITY REPORT

2022

JULY

2022年7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7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。

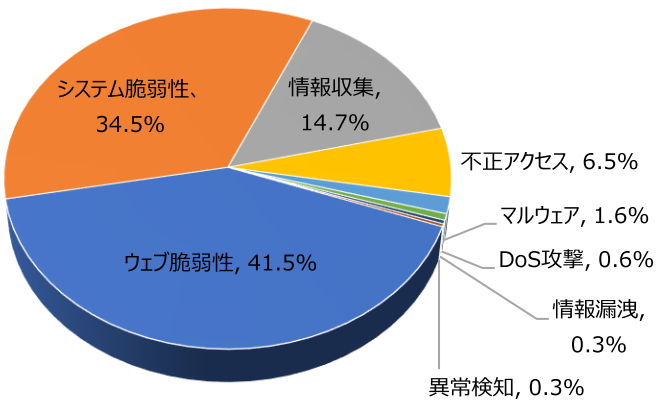
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	41.5%	-
システム脆弱性(System Vulnerability)	34.5%	-
情報収集(Information Gathering)	14.7%	-
不正アクセス(Unauthorized access)	6.5%	-
マルウェア(Malware)	1.6%	-
Dos攻撃(Denial of service attack)	0.6%	▲2
情報漏洩(Information Exposure)	0.3%	▼1
異常検知(Anomaly Detection)	0.3%	▼1

2022年7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0.85倍ぐらい減少し、それぞれの攻撃パターン件数も減少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1,100件ほど減少し、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1,100件ぐらい減少し、これはCommand Injection(NVMS-9000 DVR Vulneraility)攻撃件数増加によるものだと確認できた。



Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

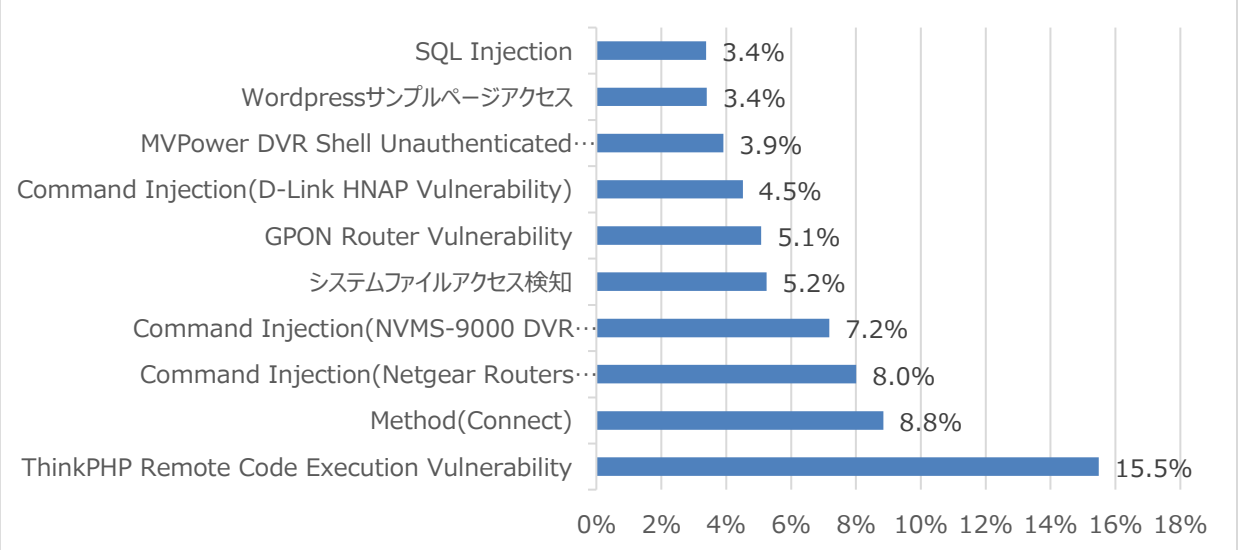
月次攻撃サービスの統計及び分析 - 2022年7月

02. 月次脆弱性攻撃TOP10

2022年7月の月次脆弱性TOP10を確認した結果、 Command Injection(D-Link HNAP Vulnerability)とSQL Injection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Method(Connect)攻撃が先月と比べて450件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	15.5%	-
2	Method(Connect)	8.8%	▲4
3	Command Injection (Netgear Routers Vulnerability)	8.0%	▲1
4	Command Injection (NVMS-9000 DVR Vulnerability)	7.2%	▼2
5	システムファイルアクセス検出	5.2%	▲2
6	GPON Router Vulnerability	5.1%	▼1
7	Command Injection (D-Link HNAP Vulnerability)	4.5%	NEW
8	MVPower DVR Shell Unauthenticated Command Execution	3.9%	▼5
9	WordPressサンプルページアクセス	3.4%	-
10	SQL Injection	3.4%	NEW

Total Threats In SOC



Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2022年7月

03. 月次ブラックリストIPアドレスTOP 10

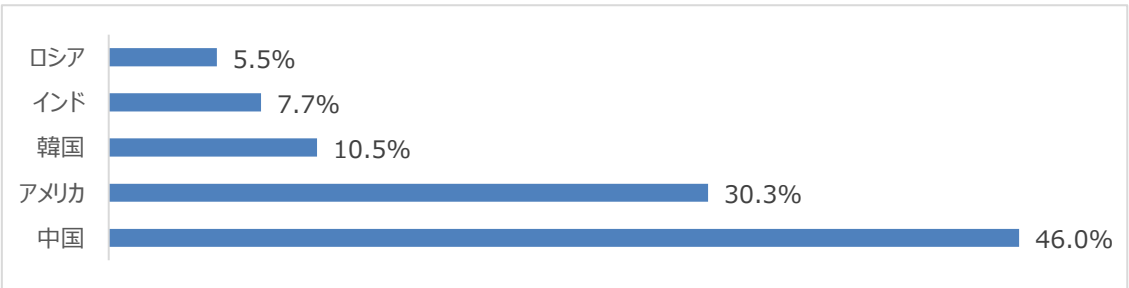
2022年7月についてTOP10を確認した結果、中国とロシアの攻撃比率が増加し、一方アメリカと韓国、インドの攻撃の比率は減少した。アメリカと中国の攻撃比率の合計は全体に比べて約50%で、半分近く増加したことが確認できた。

※ 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	49.143.32.6	KR	Command Injection(Netgear Routers Vulnerability)
2	186.233.187.21	US	Telesquare SDT-CW3B1 1.1.0 Command Injection (CVE-2021-46422)
3	62.233.50.129	RU	Apache Log4j RCE(CVE-2021-44228)
4	20.222.18.38	JP	ThinkPHP Remote Code Execution Vulnerability
5	222.186.19.205	CN	Method(Connect)
6	109.237.103.38	GB	システムファイルアクセス検出
7	109.237.103.9	GB	システムファイルアクセス検出
8	95.182.123.66	RU	Application Vulnerability(PHPUnit)
9	203.218.212.20	HK	Method(Connect)
10	13.89.48.118	US	Application Vulnerability(PHPUnit)

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	49.143.32.6	KR	6	109.237.103.38	GB
2	186.233.187.21	US	7	109.237.103.9	GB
3	62.233.50.129	RU	8	95.182.123.66	RU
4	20.222.18.38	JP	9	203.218.212.20	HK
5	222.186.19.205	CN	10	13.89.48.118	US

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

攻撃パターン毎の詳細分析結果

7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。

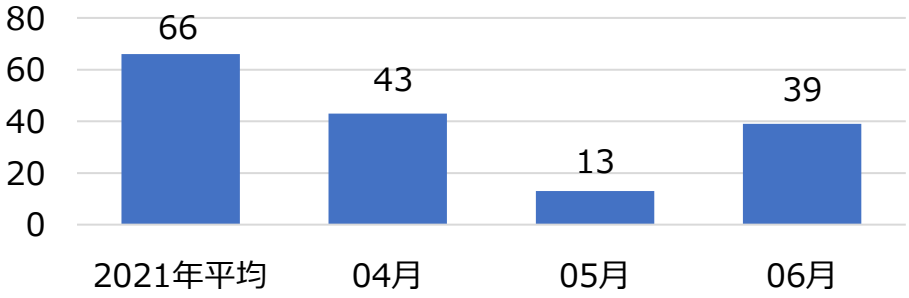
攻撃パターン	詳細分析結果
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード実行攻撃ができる脆弱性である。¥think¥*クラスを呼び出して脆弱なオブジェクトを介して攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security) トンネリングで内部アクセスを試す。これのためにConnect Methodを使用し、脆弱性が存在する場合攻撃のための中間経由地として使用される可能性がある。
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。
Command Injection (NVMS-9000 DVR Vulnerability)	Shenzhen TVT社のNVMS-9000 DVR機器の複数の脆弱性が検出された。攻撃者は該当DVR機器の基本アカウント情報をハードコードにて認証後、BOF(Buffer OverFlow)、XMLパケットを利用したRCE(Remote Code Execution)攻撃が可能となる。
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。
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。
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。
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。
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。
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。

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

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6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39件である。
6月1か月の間、Atlassian Confluence(CVE-2022-26134)脆弱性及びLinux Polkit(CVE-2021-4034)に対する検知ポリシーが配布された。



3か月間件数

5,807
全体配布量

39
今月配布量

13
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.8.05806 Webshell, JSP, Behinder. CVE-2022-26134, A Network Trojan was detected"; flow:to_server,established; content:"<%"; content:"java.util.*"; content:"extends ClassLoader"; fast_pattern:only; content:"defineClass"; content:"getInstance(|22|AES|22|)"; content:"decodeBuffer"; distance:0; sid:805806;)	Atlassian Confluenceの CVE-2022-26134脆弱性を悪用した Behinder JSP Webshellネットワーク 通信を検知するポリシー	Webshell, JSP, Behinder. CVE-2022-26134
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.1.05822 Linux, polkit, CVE-2021-4034, Attempted Administrator Privilege Gain"; flow:to_client,established; flowbits:isset,file.elf|file.macho64le|file.macholе|file.machobe; file_data; content:"pkexec"; nocase; content:"GCONV_PATH="; fast_pattern:only; content:"CHARSET="; nocase; sid:105822;)	Linux Polkitの CVE-2021-4034脆弱性を悪用したユー ザー権限を奪う試みを検出するポリシー	Linux, polkit, CVE-2021-4034
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05823 Webshell, JSP, Chopper. CVE-2022-26134, A Network Trojan was detected"; flow:to_server,established; content:"DriverManager.getConnection"; content:"ServletOutputStream"; content:"ResultSetMetaData"; content:"request.getParameter"; sid:805823;)	Atlassian Confluenceの CVE-2022-26134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	Webshell, JSP, Chopper. CVE-2022-26134
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.05834 Malware, Symbiote, A Network Trojan was detected"; flow:to_server,established; flowbits:isset,file.elf; file_data; content:"hidden_ports"; fast_pattern:only; content:"pam_set_item"; nocase; content:"pam_authenticate"; nocase; content:"pam_get_item"; nocase; content:"__gmon_start__"; nocase; sid:805834;)	Symbiote Malwareの ネットワーク通信を検知するポリシー	Malware, Symbiote

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved