CyberFortress Report

2021
JULY

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。

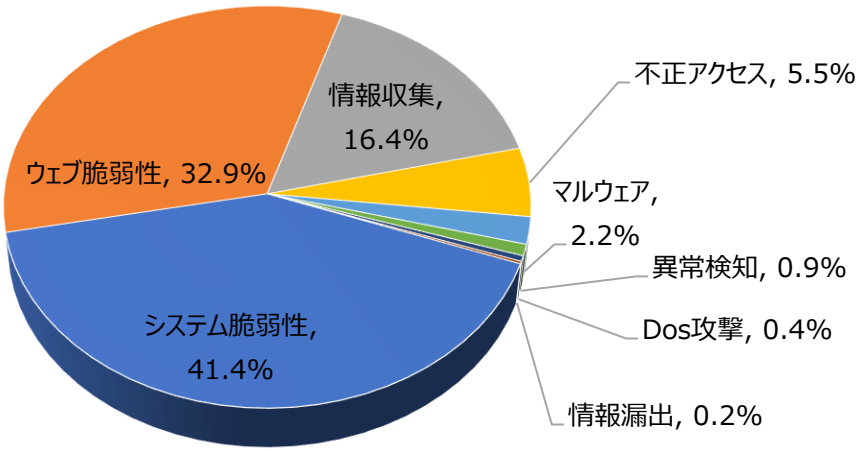
月次攻撃サービスの統計及び分析 - 2021年07月

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
いただければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	41.4%	-
ウェブ脆弱性(Web Vulnerability)	32.9%	-
情報収集(Information Gathering)	16.4%	-
不正アクセス(Unauthorized access)	5.5%	-
マルウェア(Malware)	2.2%	-
異常検知(Anomaly Detection)	0.9%	-
Dos攻撃(Denial of service attack)	0.4%	-
情報漏洩(Information Exposure)	0.2%	-

2021年07月の月次攻撃の類型を確認した結果、先月と同じであることが確認できた。
月次脆弱性TOP10のウェブ脆弱性攻撃(ThinkPHP)が幅広く増加したが、攻撃の類型の比率は先月ほぼ同じである。
また、件数自体は先月と比べて減っているがシステム及びウェブ脆弱性の比率は少し増加した。

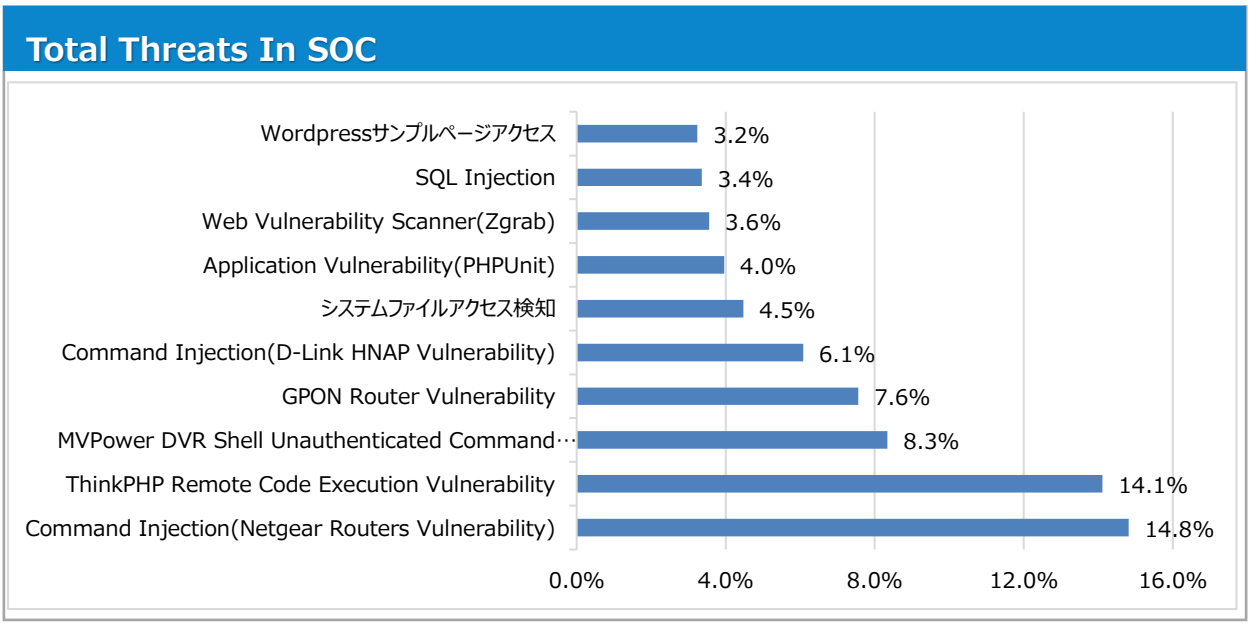


月次攻撃サービスの統計及び分析 - 2021年07月

02. 月次脆弱性攻撃TOP10

2021年07月の月次脆弱性TOP10を確認した結果、Wordpressサンプルページアクセスの脆弱性が新たにTOP10に登場し、先月と比べてThinkPHP Remote Code Execution Vulnerabilityが幅広く増加した。また、先月と同じくCommand Injectionに関する攻撃は上位を占めていることが確認できる。

順位	検知名	比率(%)	比較
1	Command Injection(Netgear Routers Vulnerability)	14.8%	-
2	ThinkPHP Remote Code Execution Vulnerability	14.1%	▲4
3	MVPower DVR Shell Unauthenticated Command Execution	8.3%	▲2
4	GPON Router Vulnerability	7.6%	▼2
5	Command Injection(D-Link HNAP Vulnerability)	6.1%	▼1
6	システムファイルアクセス検知	4.5%	▲1
7	Application Vulnerability(PHPUnit)	4.0%	▼2
8	Web Vulnerability Scanner(Zgrab)	3.6%	▲2
9	SQL Injection	3.4%	▼1
10	Wordpressサンプルページアクセス	3.2%	NEW



月次攻撃サービスの統計及び分析 - 2021年07月

03. 月次ブラックリストIPアドレスTOP 10

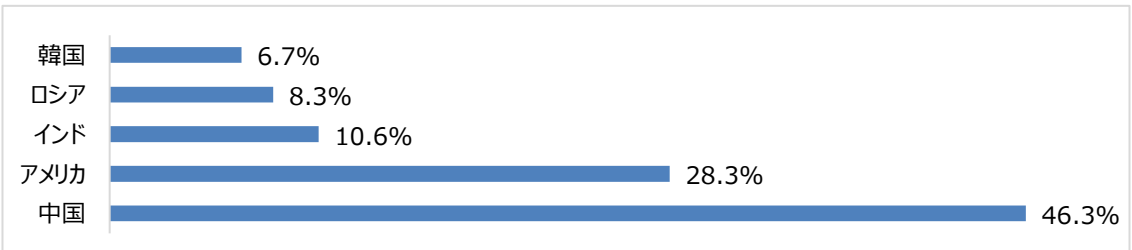
2021年07月は中国と韓国からの攻撃の比率が少し上昇し、アメリカとインド、ロシアの比率は少し下落した。先月比べて全体的に似たような様子である。

下記の表を参考にしてファイウォールやセキュリティ機器からの遮断を推奨する。

順位	ブックリストIP	国	攻撃情報
1	45.146.165.123	RU	ThinkPHP Remote Code Execution Vulnerability
2	31.210.20.100	NL	Cisco HyperFlex HX Command Injection (CVE-2021-1497)
3	5.188.210.4	RU	URL拡張子アクセス制御
4	212.192.241.87	CZ	SonicWall SSL-VPN 8.0.0.0 Remote Code Execution(shellshock/visualdoor)
5	45.146.166.253	RU	Pulse Secure SSL VPN File Disclosure
6	45.146.164.125	RU	ThinkPHP Remote Code Execution Vulnerability
7	211.231.20.14	KR	Directory Traversal
8	45.61.184.166	US	Web Scanner(ZmEu)
9	45.61.186.43	US	Web Scanner(ZmEu)
10	179.43.175.9	CH	zyxel remote code execution(CVE-2020-9054)

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	45.146.165.123	RU
2	31.210.20.100	NL
3	5.188.210.4	RU
4	212.192.241.87	CZ
5	45.146.166.253	RU

Rank	Source IP	Country
6	45.146.164.125	RU
7	211.231.20.14	KR
8	45.61.184.166	US
9	45.61.186.43	US
10	179.43.175.9	CH

攻撃パターン毎の詳細分析結果

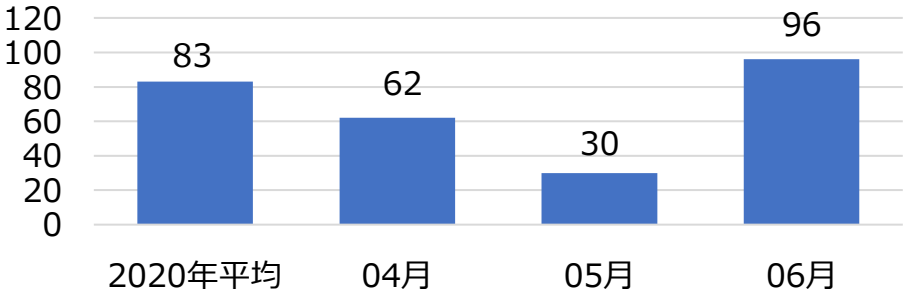
07月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

攻撃パターン	詳細分析結果
Command Injection(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。
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。
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。
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。 攻撃者は「Domain/HNAP1/GetDeviceSettings/」パスの後ろにコマンドを挿入し、「SOAPAction」フィールドを利用して実行を試みる。
システムファイルアクセス検知	攻撃者はシステムの情報の獲得のためにDirectory Traversal脆弱性を利用して/etc/passwdや*.conf /.envのようなアカウント、環境変数など、設定ファイルにアクセスを試す。
Application Vulnerability(PHPUnit)	PHPUnitはユニットテストフレームワークで/phpunit/src/Util/PHP/eval-stdin.phpファイルに存在する脆弱性を利用してリモートで任意のコードが実行できる。攻撃者は<?phpの文字列から始まるHTTP POSTデータで任意のPHPコードが実行できる。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)はウェブサーバの設定ページもしくは、許可メソッド、非認可ウェブページ、非許可ポートなど、脆弱なところの存在有無を確認するために使用する。
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。
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。

検知ポリシー

▶. 月間サイバー脅威検知ポリシー統計

SPIDER TM のポリシーで、2021年06月の1か月間共有されたサイバー脅威検知ポリシーは96件である。
MS Edge(CVE-2021-31959), ASPXSpy Webshell検知ポリシー及びLazarus, Kimsuky Groupに関する検知ポリシー62件が追加に配布された。



3か月間件数

5,093
全体配布量

96
今月配布量

30
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"IGRSS.8.05035 Malware, NecroBot, A Network Trojan was detected"; flow:to_server,established; content:"p2l44qilgm433bad5gbszb4mluxuejwkjaaon767m5dzuuc7mjqhcead.onion"; fast_pattern:only; sid:805035;)	NecroBot Malwareのネットワーク通信を検知するポリシー	Malware, NecroBot
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.2.05061 MS, Edge, CVE-2021-31959, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"|28|Date.now|28 29| - start < 200"; fast_pattern:only; content:".postMessage"; content:".terminate"; sid:205061;)	MS EdgeのCVE-2021-31959脆弱性を悪用したユーザー権限を奪取試しを検知するポリシー	MS, Edge, CVE-2021-31959
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05127 Webshell, ASPXSpy, A Network Trojan was detected"; flow:to_server,established; content:"&HRJ="; fast_pattern:only; http_client_body; content:"&ZSnXu=Login"; http_client_body; sid:805127;)	ASPXSpy Webshellのネットワーク通信を検知するポリシー	Webshell, ASPXSpy
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05130 WebApp, HP, CVE-2019-5386, Attempted User Privilege Gain"; flow:to_server,established; content:"/imc/icc/taskmng/viewBatchTaskResultDetailFact.xhtml"; fast_pattern:only; http_uri; content:"beanName="; nocase; http_uri; content:"ScriptEngineManager"; within:150; nocase; http_uri; content:"exec"; within:150; nocase; http_uri; sid:205130;)	HP機器のCVE-2019-5386脆弱性を悪用したユーザー権限を奪取試しを検知するポリシー	WebApp, HP, CVE-2019-5386