CyberFortress Report

2021
AUG

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
いただければと思います。

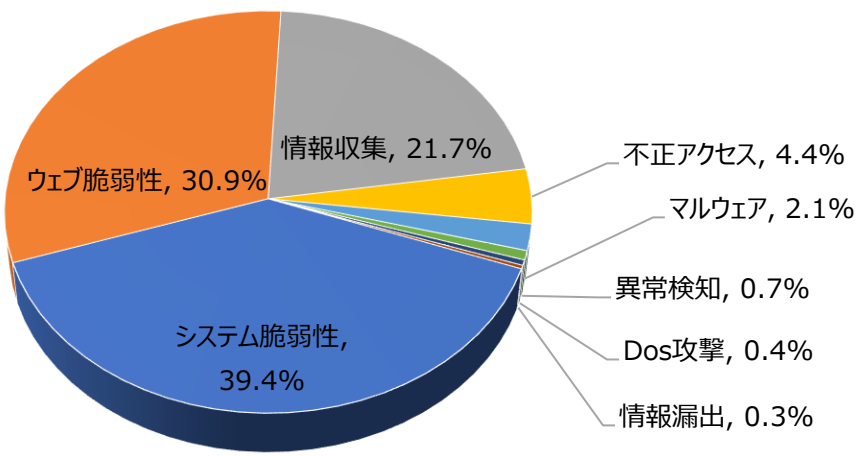
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	39.4%	-
ウェブ脆弱性(Web Vulnerability)	30.9%	-
情報収集(Information Gathering)	21.7%	-
不正アクセス(Unauthorized access)	4.4%	-
マルウェア(Malware)	2.1%	-
異常検知(Anomaly Detection)	0.7%	-
情報漏洩(Information Exposure)	0.4%	-
Dos攻撃(Denial of service attack)	0.3%	-

2021年08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。

システム脆弱性とウェブ脆弱性に関する攻撃はまだ高い比率を占めており、先月と比較し当該攻撃の件数は増加したが攻撃の比率は少し減少した。

一方、情報収取に関する攻撃は先月と比べて増加し、件数も増加したことが確認できた。

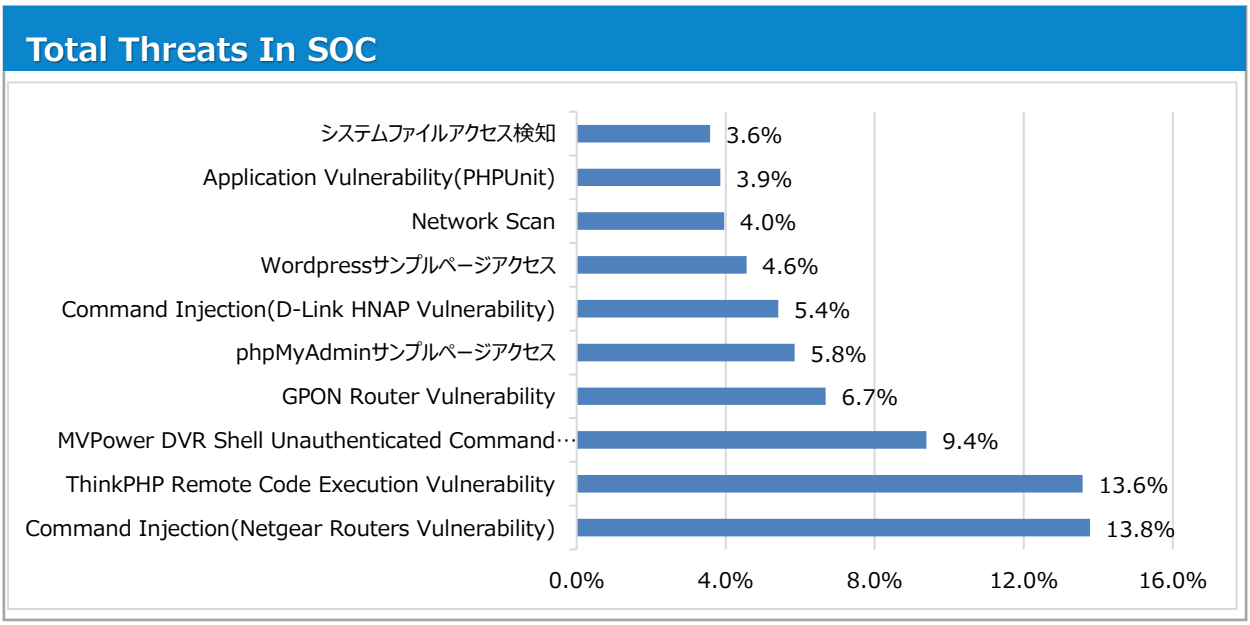


月次攻撃サービスの統計及び分析 - 2021年08月

02. 月次脆弱性攻撃TOP10

2021年08月の月次脆弱性TOP10を確認した結果、 phpMyAdminサンプルページアクセスとNetwork Scanが新たにTOP10に登場し、当該の攻撃の件数も先月と比べて2倍以上上昇した。また、先月と比べてWordpressサンプルページアクセスが幅広く増加したことがかくにんできる。そして先月似たようにCommand Injectionに関する攻撃が上位になっ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)	13.8%	-
2	ThinkPHP Remote Code Execution Vulnerability	13.6%	-
3	MVPower DVR Shell Unauthenticated Command Execution	9.4%	-
4	GPON Router Vulnerability	6.7%	-
5	phpMyAdminサンプルページアクセス	5.8%	NEW
6	Command Injection(D-Link HNAP Vulnerability)	5.4%	▼1
7	Wordpressサンプルページアクセス	4.6%	▲3
8	Network Scan	4.0%	NEW
9	Application Vulnerability(PHPUnit)	3.9%	▼2
10	システムファイルアクセス検知	3.6%	▼4



月次攻撃サービスの統計及び分析 - 2021年08月

03. 月次ブラックリストIPアドレスTOP 10

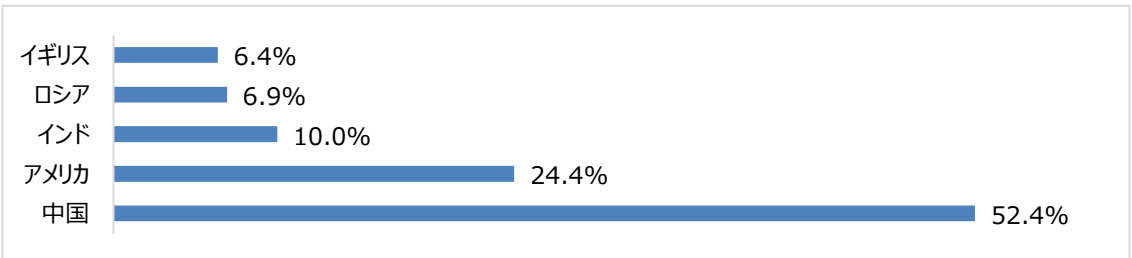
2021年08月は中国とイギリスからの攻撃の比率が少し高まった。またアメリカやインド、ロシアの比率は少し下落し、先月と比べると似たような比率である。

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	45.146.164.110	RU	ThinkPHP Remote Code Execution Vulnerability
2	106.55.150.83	CH	phpMyAdminサンプルページアクセス
3	210.108.70.119	KR	Apache Struts2 Jakarta RCE (CVE-2017-5638)
4	159.75.25.179	CH	phpMyAdminサンプルページアクセス
5	106.55.250.60	CH	phpMyAdminサンプルページアクセス
6	80.82.65.202	NL	Network Scan
7	159.75.9.197	CH	phpMyAdminサンプルページアクセス
8	35.75.4.158	US	Wordpressサンプルページアクセス
9	209.141.45.210	US	Wordpressサンプルページアクセス
10	20.199.105.48	FR	phpinfo()ページ露出

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	45.146.164.110	RU
2	106.55.150.83	CH
3	210.108.70.119	KR
4	159.75.25.179	CH
5	106.55.250.60	CH

Rank	Source IP	Country
6	80.82.65.202	NL
7	159.75.9.197	CH
8	35.75.4.158	US
9	209.141.45.210	US
10	20.199.105.48	FR

攻撃パターン毎の詳細分析結果

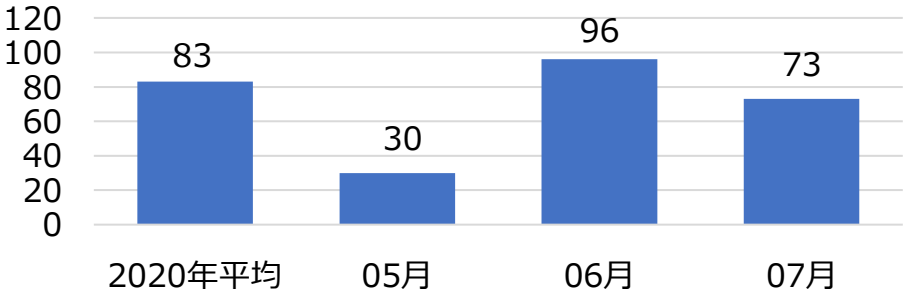
08月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
phpMyAdmin サンプルページアクセス	phpMyAdminはウェブサーバーからMySQLを管理する目的でPHPで作成されているオープンソースツー ルで、この攻撃はMy-SQLサーバを対象に脆弱性を探してデータベースの作成/削除、テーブルの作成/ 削除、フィールドの作成/削除、SQL問い合わせ実行、実行権限管理機能などが実行できる脆弱性が 存在している場合、phpMyAdminの「script/setup.php」ファイルに「?」因子を利用して任意の関数 を挿入することでシステムコマンドが実行できる。
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。
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。
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。
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。
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。

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07月の1か月間共有されたサイバー脅威検知ポリシーは73件である。
Netfilter, ASPXWebshell及びMS Exchange(CVE-2021-34473)脆弱性に関する検知ポリシーが配布された。



3か月間件数

5,166
全体配布量

73
今月配布量

96
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.8.05134 Malware, Netfilter, A Network Trojan was detected"; flow:to_server,established; content:"GET "; depth:4; content:"/v?v="; fast_pattern; content:"&m="; within:4; distance:1; content:" HTTP/1.1|0D 0A|"; within:11; distance:32; content:"|0D 0A|Accept: text/html,application/xhtml+xml,application/xml|3B|q=0.9,image/webp,image/apng,*/*|3B|q=0.8,application/signed-exchange|3B|v=b3|3B|q=0.9|0D 0A|"; content:"|0D 0A 0D 0A 00|"; sid:805134;)	Netfilter Malwareの ネットワーク通信を検知するポリシー	Malware, Netfilter
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.05158 MS, Exchange, CVE-2021-34473, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/autodiscover/"; fast_pattern:only; http_uri; content:"<EMailAddress"; nocase; http_client_body; pcre:"/<EMailAddress(¥s[^>]*?)?>[^<]*?¥x2fautodiscover/Pi"; sid:105158;)	MS ExchangeのCVE-2021-34473脆弱性を悪用して管理者権限奪取試しを検知するポリシー	MS, Exchange, CVE-2021-34473
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.05162 MS, Exchange, CVE-2021-34473, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/autodiscover/"; fast_pattern:only; http_uri; content:"Email"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?Email((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?¥x2fautodiscover/Psim"; sid:105162;)	MS Exchangeの CVE-2021-34473脆弱性を悪用して管理者権限奪取試しを検知するポリシー	MS, Exchange, CVE-2021-34473
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05178 Malware, ASPXSpy, Webshell, A Network Trojan was detected"; flow:to_server,established; content:"Content-Disposition: form-data|3B| name=|22|MainButton|22 0D 0A 0D 0A|Sysinfo|0D 0A|"; fast_pattern:only; http_client_body; sid:805178;)	ASPXSpy Webshellの ネットワーク通信を検知するポリシー	Malware, ASPXSpy, Webshell