SECURITY REPORT

2021 SEP

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09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。

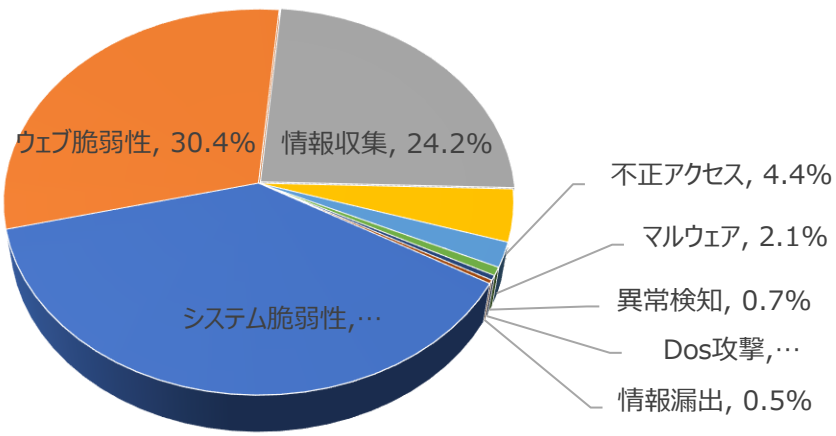
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	38.1%	-
ウェブ脆弱性(Web Vulnerability)	30.4%	-
情報収集(Information Gathering)	24.2%	-
不正アクセス(Unauthorized access)	3.3%	-
マルウェア(Malware)	2.5%	-
異常検知(Anomaly Detection)	0.7%	-
情報漏洩(Information Exposure)	0.5%	▲1
Dos攻撃(Denial of service attack)	0.3%	▼1

2021年09月の月次攻撃の類型を確認した結果、ランキング上位3項目とDos攻撃、情報漏洩を除く残りの項目は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今年上半期から着実に増加しており、情報収集に関する攻撃も前年から大幅に増加した。

情報漏洩については前月より若干の増加が見られ、ランキングも上がっている状況が分かる。

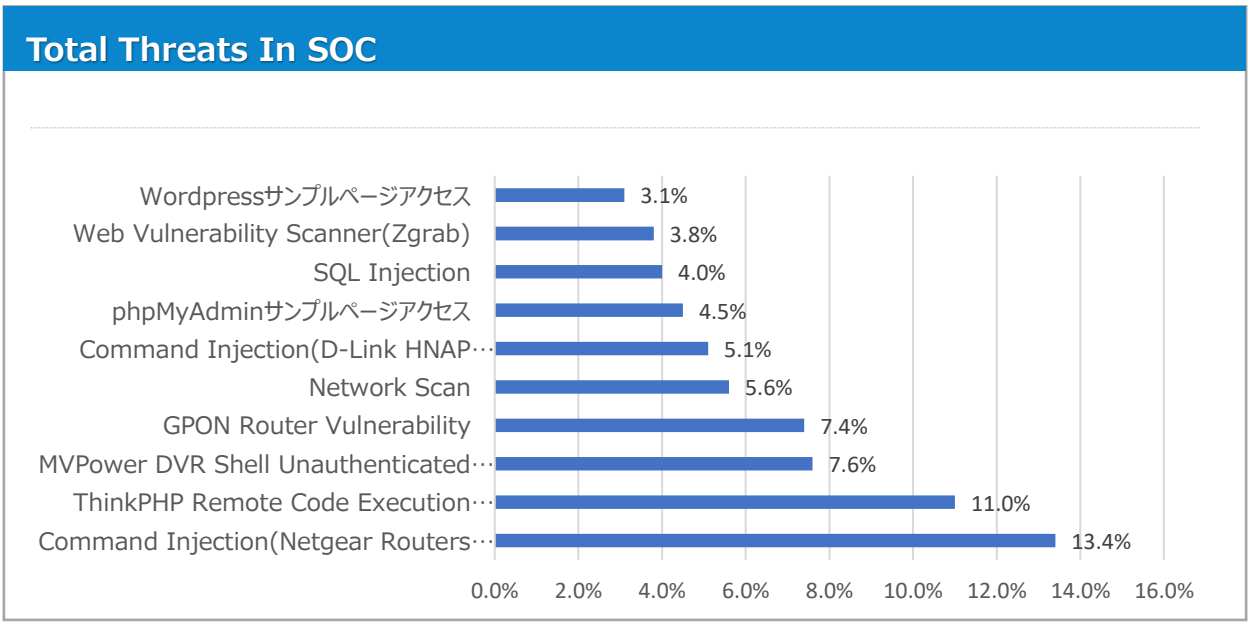


月次攻撃サービスの統計及び分析 - 2021年09月

02. 月次脆弱性攻撃TOP10

2021年09月の月次脆弱性TOP10を確認した結果、SQLインジェクションとWeb Vulnerability Scanner(Zgrab)がトップ10入りし、前月から比べて攻撃数は2倍に増加しました。
Network Scan件数も前月から更に増加が続いています。
前月同様にCommand Injectionがランキング上位を維持していることも分かります。

順位	検知名	比率(%)	比較
1	Command Injection (Netgear Routers Vulnerability)	13.4%	-
2	ThinkPHP Remote Code Execution Vulnerability	11.0%	-
3	MVPower DVR Shell Unauthenticated Command Execution	7.6%	-
4	GPON Router Vulnerability	7.4%	-
5	Network Scan	5.6%	▲3
6	Command Injection (D-Link HNAP Vulnerability)	5.1%	-
7	phpMyAdmin サンプルページアクセス	4.5%	▼2
8	SQL インジェクション	4.0%	NEW
9	Web Vulnerability Scanner(Zgrab)	3.8%	NEW
10	Wordpressサンプルページアクセス	3.1%	▼3



月次攻撃サービスの統計及び分析 - 2021年09月

03. 月次ブラックリストIPアドレスTOP 10

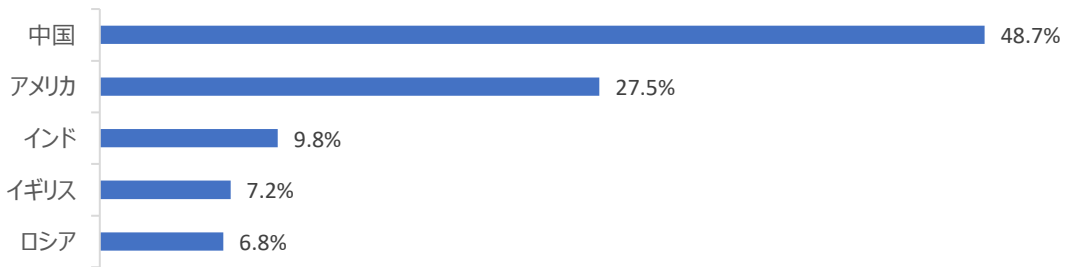
2021年09月はアメリカ、インド、イギリスの中でも、特にアメリカからの攻撃の比率が前月から約3.5%増加している。中国とロシア間での攻撃率はわずかに低下している。前月同様に全体的な攻撃数では増加している。

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	Application Vulnerability(PHPUnit)
2	20.102.74.72	US	phpinfo()ページ露出
3	20.150.209.191	US	Method(Connect)
4	80.82.65.201	NL	Network Scan
5	1.234.41.218	KR	Apache Struts2 Jakarta RCE (CVE-2017-5638)
6	80.82.65.202	NL	Network Scan
7	185.216.140.185	NL	Network Scan
8	89.248.168.222	NL	Network Scan
9	34.87.200.179	AU	SIP Vulnerability Scanner(Sipvicious)
10	89.248.165.13	GB	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	45.146.164.110	RU
2	20.102.74.72	US
3	20.150.209.191	US
4	80.82.65.201	GB
5	1.234.41.218	KR

Rank	Source IP	Country
6	80.82.65.202	GB
7	185.216.140.185	GB
8	89.248.168.222	GB
9	34.87.200.179	US
10	89.248.165.13	GB

攻撃パターン毎の詳細分析結果

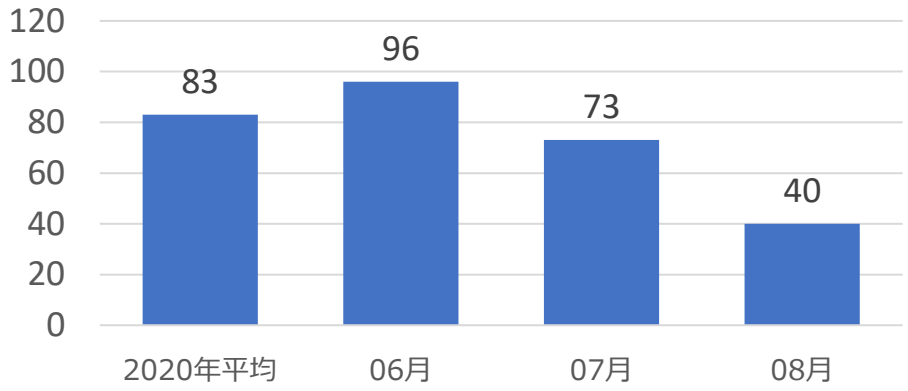
09月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
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。
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。
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。
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。
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。
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08月の1か月間共有されたサイバー脅威検知ポリシーは40件である。
DNS, RDP Tunneling, JspFileBrowser Webshell及びfortinet WebUI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

5,206
全体配布量

40
今月配布量

73
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert udp $EXTERNAL_NET 53 -> any any (msg:"IGRSS.28.05205 DNS tunneling, Misc activity"; flow:to_client; byte_test:1,!&,0x01,2; content:"|03|s"; nocase; content:"|03|1yf|02|de|00|"; distance:2; nocase; sid:2805205;)	DNSトンネリングの検知ポリシー	DNS tunneling
alert tcp $EXTERNAL_NET any -> $HOME_NET !3389 (msg:"IGRSS.2.05210 RDP tunneling, Attempted User Privilege Gain"; flow:to_server,established; content:"|03 00 00|"; depth:3; content:"|E0 00 00 00 00 00|"; depth:6; offset:5; content:"Cookie: mstshash="; within:17; fast_pattern; sid:205210;)	RDPトンネリングの検知ポリシー	RDP tunneling
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05221 Webshell, JspFileBrowser, A Network Trojan was detected"; flow:to_server,established; content:"&dir="; fast_pattern:only; http_client_body; content:"&sort="; nocase; http_client_body; content:"&"; within:2; distance:1; http_client_body; content:"&Submit"; nocase; http_client_body; content:"="; within:2; http_client_body; sid:805221;)	jspFile Browser Webshellのネットワーク通信を検知するポリシー	Webshell, JspFileBrowser
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.05234 Fortinet, FortiWeb, Vul, Web Application Attack"; flow:to_server,established; content:"/api/v2.0/user/remoteserver.saml"; fast_pattern:only; http_uri; content:"name="; nocase; http_uri; content:"26"; http_raw_uri; pcre:"/[?&]name=[^&]*?%(25)?26/Ii"; sid:1005234;)	Fortinet FortiWebのコマンドインジェクション脆弱性を検知するポリシー	Fortinet, FortiWeb, Vul