SECURITY REPORT

2021 NOV

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11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。

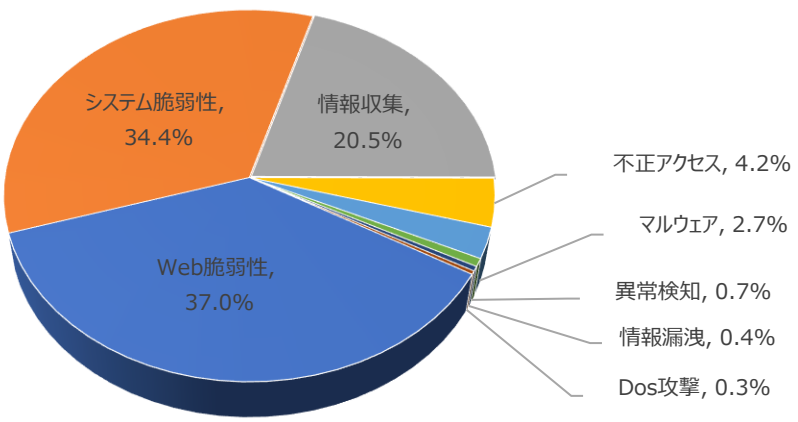
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	37.0%	▲2
システム脆弱性(System Vulnerability)	34.3%	▼1
情報収集(Information Gathering)	20.5%	▼1
不正アクセス(Unauthorized access)	4.2%	-
マルウェア(Malware)	2.7%	-
異常検知(Anomaly Detection)	0.7%	-
情報漏洩(Information Exposure)	0.4%	▲1
Dos攻撃(Denial of service attack)	0.3%	▼1

2021年11月の攻撃類型を確認した結果、攻撃の総数は前月と比較して増加しています。

特に Web脆弱性に関連するものは約 1.5 倍に増加し、上位3項目の合計比率は92%となり、前月より更に高まっていることが分かります。

一方、情報漏洩に関連する攻撃やDos攻撃は、前月より若干減少していることも確認できます。



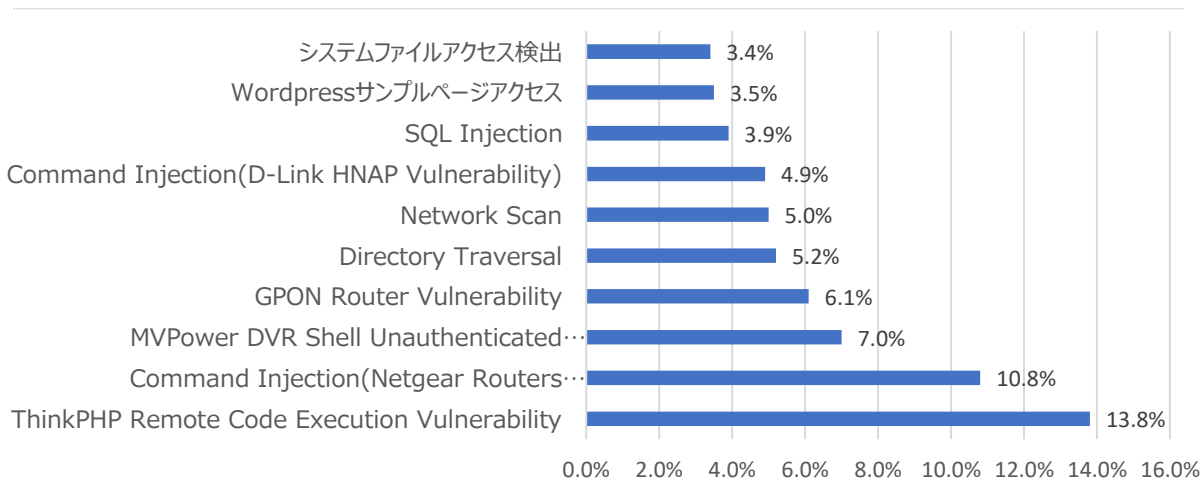
月次攻撃サービスの統計及び分析 - 2021年11月

02. 月次脆弱性攻撃TOP10

2021年11月の月次脆弱性TOP10を確認した結果、ディレクトリ トラバーサル攻撃とSQL インジェクション攻撃が新たにトップ10入りしました。
その中でもディレクトリ トラバーサル攻撃は前月から7倍に増加し、SQL インジェクション攻撃は1.5倍に増加しています。また、ThinkPHP Remote Code Execution 脆弱性攻撃の数は前月に比べて約2.5倍に増加し、ランキング1位となりました。

順位	検知名	比率(%)	比較
1	ThinkPHP Remote Code Execution Vulnerability	13.8%	▲4
2	Command Injection (Netgear Routers Vulnerability)	10.8%	▼1
3	MVPower DVR Shell Unauthenticated Command Execution	7.0%	-
4	GPON Router Vulnerability	6.1%	-
5	Directory Traversal	5.2%	NEW
6	Network Scan	5.0%	▼4
7	Command Injection (D-Link HNAP Vulnerability)	4.9%	▼1
8	SQL Injection	3.9%	NEW
9	Wordpressサンプルページアクセス	3.5%	▼1
10	システムファイルアクセス検出	3.4%	▼3

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2021年11月

03. 月次ブラックリストIPアドレスTOP 10

2021年11月は、中国、アメリカ、ロシアでの攻撃が増加し、上位の中国とアメリカだけで攻撃は約80%近くになっています。

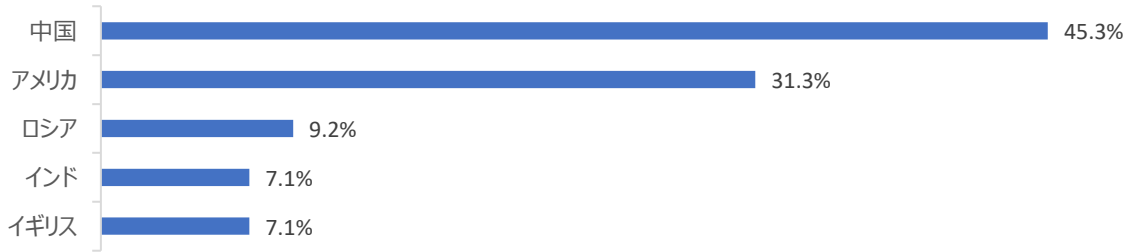
一方、インドとイギリスでの攻撃はわずかに低下が見られました。

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しています。

順位	ブックリストIP	国	攻撃情報
1	45.146.164.110	RU	Directory Traversal
2	91.132.58.79	AU	Directory Traversal
3	145.220.25.28	NL	etcpasswd Detect
4	209.141.56.100	US	Web Scanner(ZmEu)
5	109.237.103.118	RU	システムファイルアクセス検出
6	185.170.144.50	EE	Directory Traversal
7	178.239.21.101	CN	Fortinet FortiOS Directory Traversal (CVE-2018-13379)
8	209.141.62.185	US	D-LINK DCS-2530L,DCS-2670L Getuser Password Information Disclosure(CVE-2020-25078)
9	167.99.133.28	DE	Directory Traversal
10	161.35.188.242	US	Directory Traversal

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	91.132.58.79	AU
3	145.220.25.28	NL
4	209.141.56.100	US
5	109.237.103.118	RU

Rank	Source IP	Country
6	185.170.144.50	EE
7	178.239.21.101	CN
8	209.141.62.185	US
9	167.99.133.28	DE
10	161.35.188.242	US

攻撃パターン毎の詳細分析結果

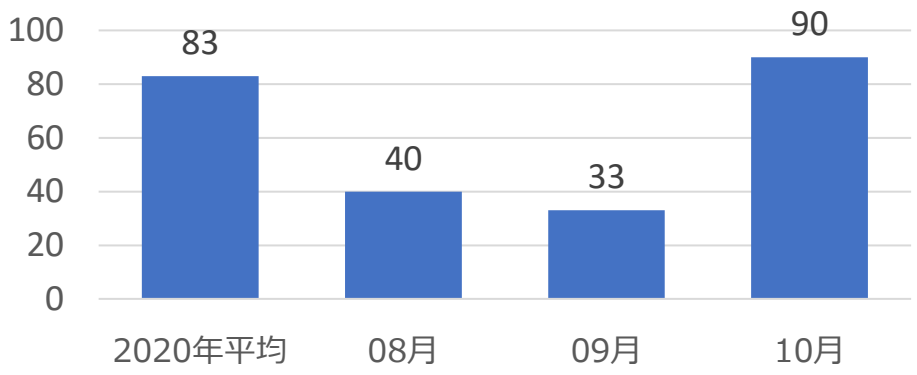
11月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

攻撃パターン	詳細分析結果
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。
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。
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。 この脆弱性は家庭用ルータにて発見された。
Directory Traversal	ホームページの表示もしくはダウンロードページのURLを使用せず、Webサーバ上のhomeディレクトリ外の任意のディレクトリ上のファイル(/etc/passwdファイルなど)を参照またはダウンロードすることが出来る。内部情報については、システム情報を含む/etc/pass/shadow、/etc/hosts/hostsなどの主要ファイルをダウンロードすることが可能であり、システム侵入や内部データ漏洩などの二次的な攻撃に悪用される可能性がある。
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。
SQL Injection	SQLインジェクション攻撃は、Webページでクエリなどステートメントにしようするする入力値を、文字(特殊文字、UnionやSelectなど)をフィルタ処理しない場合に、攻撃を受ける可能性がある。 攻撃者はDBに関連付けられたアカウントのアクセス許可内で様々なクエリを使用してアクセスし、格納された情報の取得、変更、削除を行うことができる。
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。
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。

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、2021年10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93件である。Ms Windows (CVE-2021-38647) 、MS Exchange (CVE-2021-34523)、Apache (CVE-2021-41773)およびMITRE ATT&CK の T1559.002 (DDECMdExec) 攻撃と脆弱性に関する検知ポリシーが配布された。



検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.05281 MS, Windows, CVE-2021-38647, Web Application Attack"; flow:to_server,established; content:"/wsman"; fast_pattern:only; http_uri; content:"<p:ExecuteShellCommand_INPUT"; nocase; http_client_body; content:!"Authorization"; http_header; sid:1005281;)	MS Windows(CVE-2021-38647) 脆弱性にてリモートコード試行実行を 検知するポリシー	MS, Windows, CVE-2021-38647
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.05305 MS, Exchange, CVE-2021-34523, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/autodiscover"; fast_pattern:only; http_uri; content:"Email="; nocase; http_uri; pcre:"/[?&]Email=[^&]*?₩x2fautodiscover/Ui"; sid:105305;)	MS Exchange (CVE-2021-34523) 脆弱性にて管理者特権取り消しの 試行実行を検知するポリシー	MS, Exchange, CVE-2021-34523
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.05324 Apache, CVE-2021-41773, Web Application Attack"; flow:to_server,established; content:"/cgi-bin/"; fast_pattern:only; content:"/cgi-bin/"; depth:9; nocase; http_raw_uri; pcre:"/cgi-bin₩/(₩x2e?(%2e|₩x2e₩x3b?|%2e%2e)₩/){2}/li"; sid:1005324;)	Apache(CVE-2021-41773) 脆弱性にてパス検索の 試行実行を検知するポリシー	Apache, CVE-2021-41773
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.05353 TTPs, T1559.002, DDECmdExec, A Network Trojan was detected"; flow:to_server,established; file_data; content:"cmd|7C 27|"; nocase; content:"|27 21|"; within:250; pcre:"/[=+-@](₩w+₩x28)?cmd₩x7C₩x27[^₩x27]+₩x27₩x21₩w+/i"; sid:805353;)	MITRE ATT&CK の T1559.002 (DDECMdExec) の脆弱性による攻撃を 検知するポリシー	TTPs, T1559.002, DDECmdExec