SECURITY REPORT

2021 DEC

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12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。

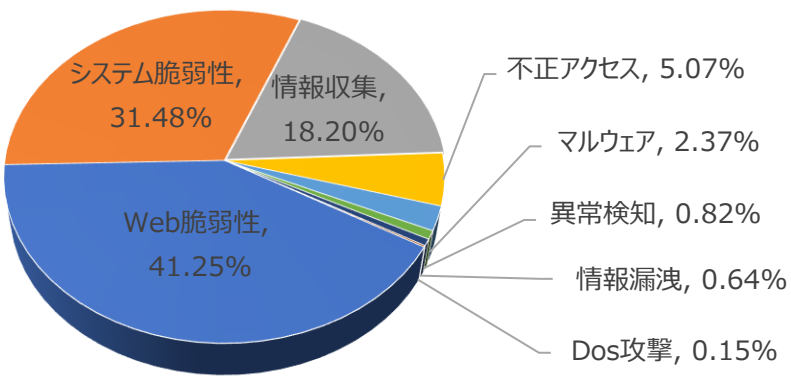
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	41.25%	-
システム脆弱性(System Vulnerability)	31.48%	-
情報収集(Information Gathering)	18.20%	-
不正アクセス(Unauthorized access)	5.07%	-
マルウェア(Malware)	2.37%	-
異常検知(Anomaly Detection)	0.82%	-
情報漏洩(Information Exposure)	0.64%	-
Dos攻撃(Denial of service attack)	0.15%	-

2021年12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減少しています。

しかし Web脆弱性に関連するものは約 4.5 倍に増加しました。これはThinkPHP RCE攻撃数が増加したためです。

一方、TOP10のランキング順序が先月と変わりないことが分かります。

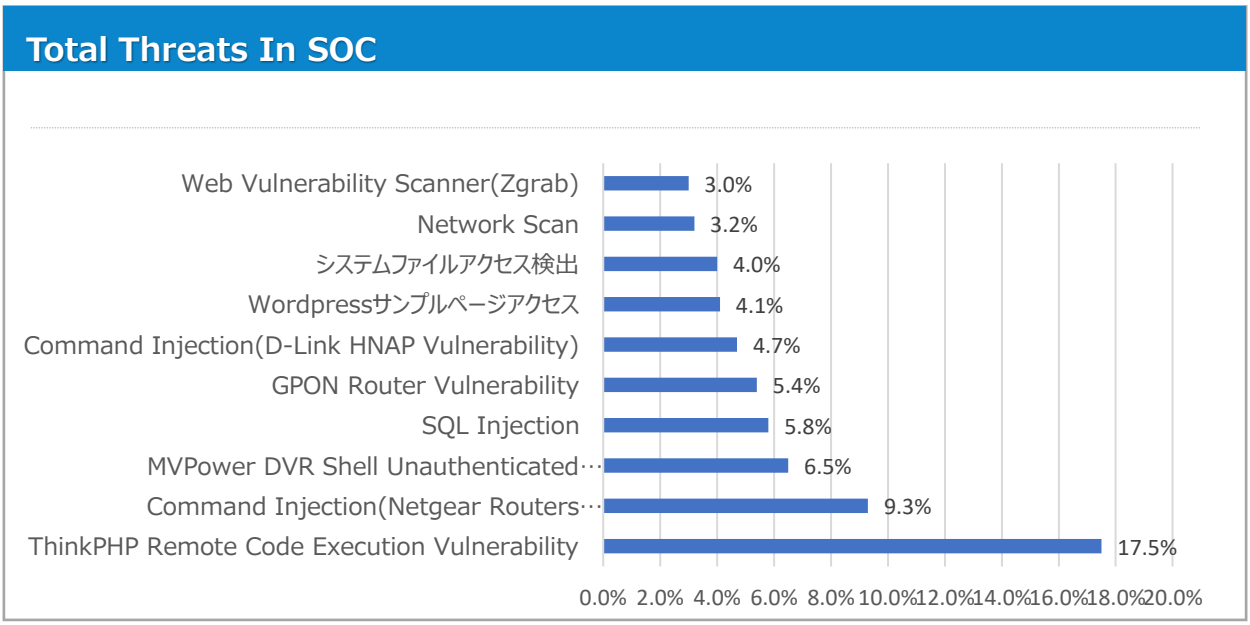


月次攻撃サービスの統計及び分析 - 2021年12月

02. 月次脆弱性攻撃TOP10

2021年12月の月次脆弱性TOP10を確認した結果、Web Vulnerability Scanner(Zgrab)攻撃がTOP10に入り、ThinkPHP Remote Code Execution Vulnerability攻撃の数は前月に比べて1.25倍増加し、全体で17.5%という最大割合を占めています。
一方、Network Scan攻撃は、前月から約半分に減少しました。

順位	検知名	比率(%)	比較
1	ThinkPHP Remote Code Execution Vulnerability	17.5%	-
2	Command Injection (Netgear Routers Vulnerability)	9.3%	-
3	MVPower DVR Shell Unauthenticated Command Execution	6.5%	-
4	SQL Injection	5.8%	▲4
5	GPON Router Vulnerability	5.4%	▼1
6	Command Injection (D-Link HNAP Vulnerability)	4.7%	▲1
7	Wordpressサンプルページアクセス	4.1%	▲2
8	システムファイルアクセス検出	4.0%	▲2
9	Network Scan	3.2%	▼3
10	Web Vulnerability Scanner(Zgrab)	3.0%	NEW



月次攻撃サービスの統計及び分析 - 2021年12月

03. 月次ブラックリストIPアドレスTOP 10

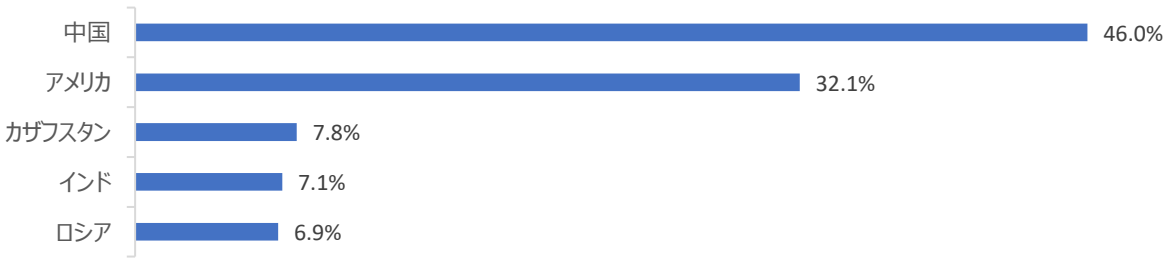
2021年12月についてTOP10を確認し結果、カザフスタンの攻撃率は前月から約2.5%増加しました。
中国、アメリカ、インド、ロシアは若干攻撃を減らしていますが、依然として中国とアメリカの攻撃率は高いです。

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	195.154.119.181	FR	etcpasswd Detect
3	47.253.82.78	US	Directory Traversal
4	161.35.188.242	US	Web Scanner(LeakIX)
5	131.161.83.246	HN	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-42013)
6	47.90.161.18	US	Directory Traversal
7	206.189.185.88	US	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
8	164.90.204.15	NL	Method(Connect)
9	109.237.103.118	RU	システムファイルアクセス検出
10	47.252.38.12	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	195.154.119.181	FR
3	47.253.82.78	US
4	161.35.188.242	US
5	131.161.83.246	HN

Rank	Source IP	Country
6	47.90.161.18	US
7	206.189.185.88	US
8	164.90.204.15	NL
9	109.237.103.118	RU
10	47.252.38.12	US

攻撃パターン毎の詳細分析結果

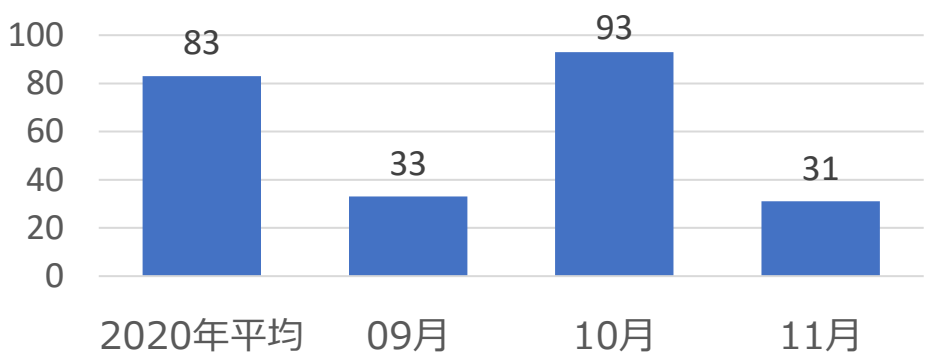
12月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
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。
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。 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。
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。
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。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)は、Webサーバの設定ページや許可方法、許可されていないWebページ、ライセンスのないポートなど、脆弱性部分の存在を判断するために使用される。

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11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31件である。MS IE(CVE-2021-42298) 、Oracle WebLogic(CVE-2020-14883) の攻撃と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

月間配布件数

検知ポリシー	説明	タグ
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"IGRSS.8.05370 Webshell, Generic, A Network Trojan was detected"; flow:to_client,established; file_data; content:"Back Connect"; fast_pattern:only; sid:805370;)	PHP Webshell Genericで ネットワーク通信を検出するポリシー	Webshell, Generic
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.05379 Malware, Kimsuky, A Network Trojan was detected"; flow:to_server,established; content:"/report.php?filename="; depth:21; fast_pattern; http_uri; sid:805379;)	Kimsuky Malwareの ネットワーク通信を検出するポリシー	Malware, Kimsuky
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.2.05382 MS, IE, CVE-2021-42298, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"new Array("; content:".length"; within:50; distance:10; content:"new Array("; within:50; distance:85; fast_pattern; content:".sort("; within:50; distance:10; content:".apply("; within:30; sid:205382;)	MS IE CVE-2021-42298の脆弱性を 悪用したユーザによる挙動を 検出するポリシー	MS, IE, CVE-2021- 42298
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.05391 Oracle, WebLogic, CVE-2020-14883, Web Application Attack"; flow:to_server,established; content:"/console.portal"; fast_pattern:only; http_uri; pcre:"/(¥x2e|%(25)?2e){2}([¥x2f¥x5c]|%(25)?(2f|5c))console.portal/Ii"; sid:1005391;)	Oracle WebLogic CVE-2020-14883のリモート コード実行の試行を検出する ためのポリシー	Oracle, WebLogic, CVE-2020- 14883