SECURITY REPORT

2022

FEB

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 - 2022年2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。

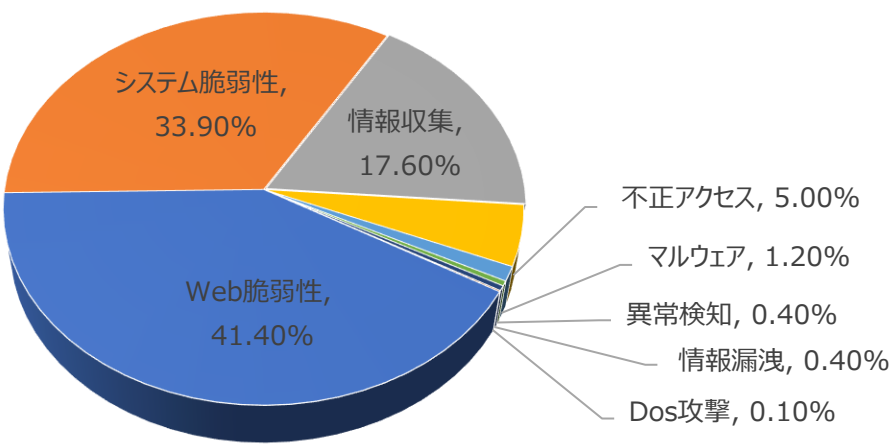
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	41.4%	▲1
システム脆弱性(System Vulnerability)	33.9%	▼1
情報収集(Information Gathering)	17.6%	-
不正アクセス(Unauthorized access)	5.0%	-
マルウェア(Malware)	1.2%	-
異常検知(Anomaly Detection)	0.4%	▲1
情報漏洩(Information Exposure)	0.4%	▼1
Dos攻撃(Denial of service attack)	0.1%	-

2022年2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。

特にシステム脆弱性に関連する攻撃は約20%減少しました。Apache Log4j RCE攻撃数が減少したためです。

一方、Web脆弱性関連の攻撃は前月から15%増加し、ThinkPHP Remote Code Execution 攻撃数が増加ししたため、1位にランキングされています。



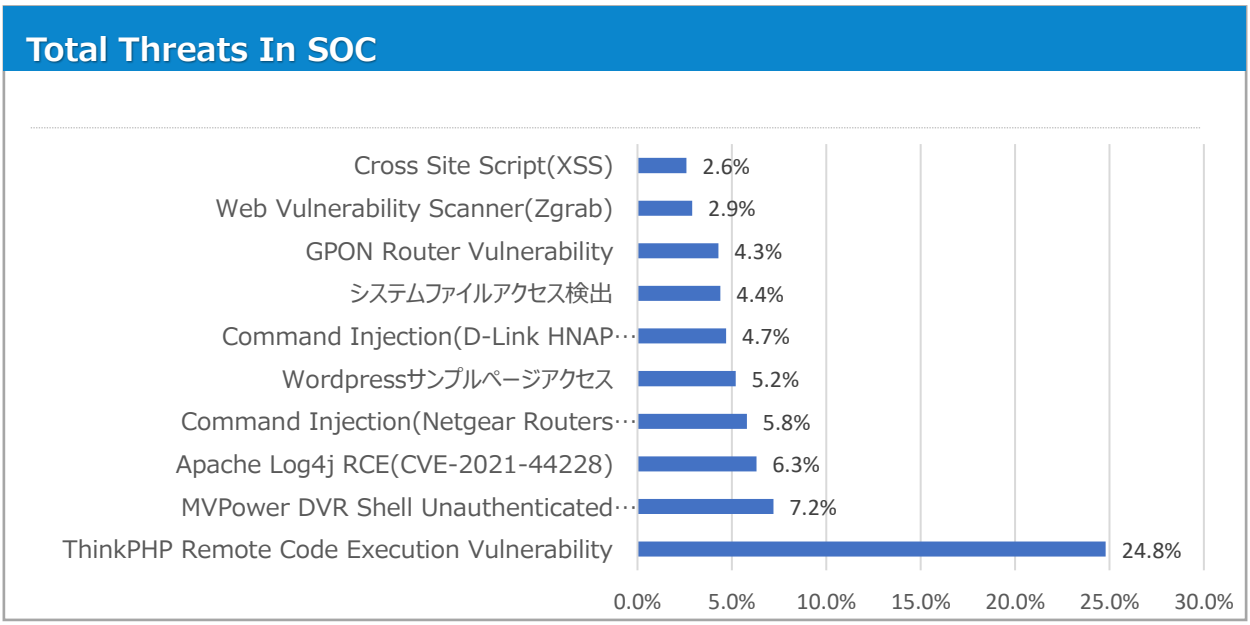
Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2022年2月

02. 月次脆弱性攻撃TOP10

2022年2月の月次脆弱性TOP10を確認した結果、 Cross Site Script(XSS)がTOP10に入り、Apache Log4j RCE(CVE-2021-44228)攻撃は前月から5分の1に減少しました。
ThinkPHP RCEは約2倍に増加し、全体の4分の1を占めて1位にランキングしています。

順位	検知名	比率(%)	比較
1	ThinkPHP Remote Code Execution Vulnerability	24.8%	▲1
2	MVPower DVR Shell Unauthenticated Command Execution	7.2%	▲2
3	Apache Log4j RCE(CVE-2021-44228)	6.3%	▼2
4	Command Injection (Netgear Routers Vulnerability)	5.8%	▼1
5	Wordpressサンプルページアクセス	5.2%	▲2
6	Command Injection (D-Link HNAP Vulnerability)	4.7%	▼1
7	システムファイルアクセス検出	4.4%	▲1
8	GPON Router Vulnerability	4.3%	▼2
9	Web Vulnerability Scanner(Zgrab)	2.9%	▲1
10	Cross Site Script(XSS)	2.6%	NEW



Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2022年2月

03. 月次ブラックリストIPアドレスTOP 10

2022年2月についてTOP10を確認し結果、アメリカ、韓国、インドでの攻撃の割合が増加し、中国とロシアの割合は若干減少しました。

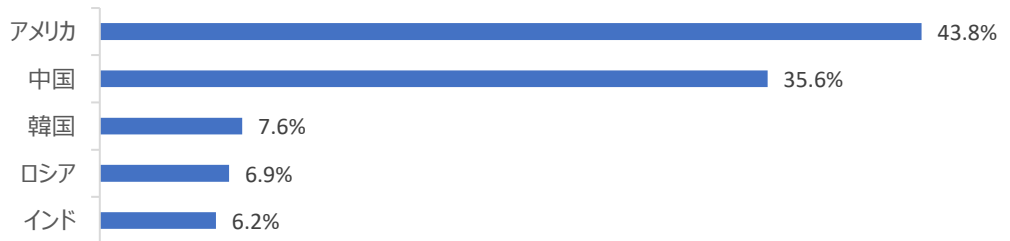
また、アメリカ、中国の攻撃率は全体の80%に上っています。

※ 下記の表を参考にした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	45.146.165.37	RU	Directory Traversal
2	109.237.103.9	RU	システムファイルアクセス検出
3	109.237.103.123	RU	システムファイルアクセス検出
4	209.141.47.28	US	Apache Log4j RCE(CVE-2021-44228)
5	161.35.188.242	US	Directory Traversal
6	109.237.103.38	RU	システムファイルアクセス検出
7	199.127.60.104	US	Apache log4j Remote Code Execution Vulnerability (CVE-2019-17571)
8	206.81.18.213	DE	Apache Log4j RCE (CVE-2021-44228)
9	45.134.144.108	DE	Fortinet FortiOS Directory Traversal (CVE-2018-13379)
10	34.138.49.128	US	Apache Log4j RCE (CVE-2021-44228)

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	45.146.165.37	RU
2	109.237.103.9	RU
3	109.237.103.123	RU
4	209.141.47.28	US
5	161.35.188.242	US

Rank	Source IP	Country
6	109.237.103.38	RU
7	199.127.60.104	US
8	206.81.18.213	DE
9	45.134.144.108	DE
10	34.138.49.128	US

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

攻撃パターン毎の詳細分析結果

2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。

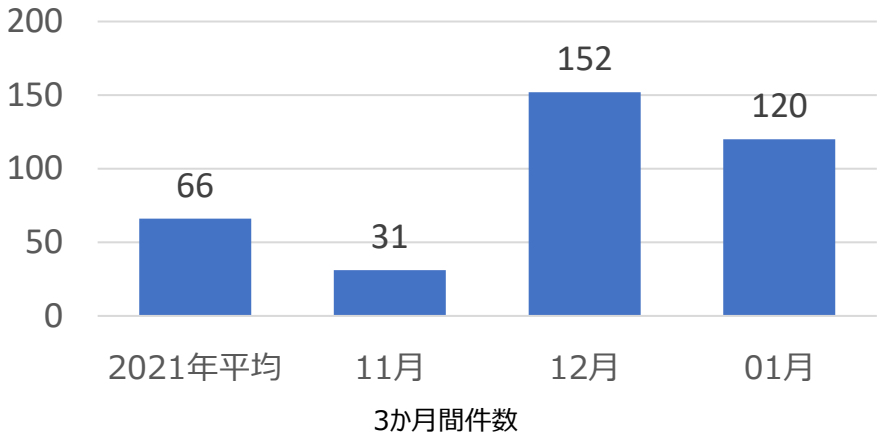
攻撃パターン	詳細分析結果
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード実行攻撃ができる脆弱性である。¥think¥*クラスを呼び出して脆弱なオブジェクトを介して攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥'shell¥'」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。
Apache Log4j RCE (CVE-2021-44228)	オープンソースのJava logging libraryのApache Log4jを使用することで、攻撃者は認証無しでサーバ上のリモートコマンドを実行できる。
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。
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。
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。
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。
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。
Cross Site Script (XSS)	攻撃者による悪質なスクリプトが入力されたページをユーザが表示した場合、スクリプトで実行可能な処理(ファイルのダウンロードやページの移動など)が実行される。

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

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、2022年1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120件である。
Apache Log4j2 (CVE-2021-44228)、(CVE-2021-45046)、 (CVE-2021-45105)、
RealTek(CVE-2021-35394)、MuddyWaterによるマルウェアの脆弱性に関するポリシーが配布された。



3か月間件数

5,635
全体配布量

120
今月配布量

152
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05557 log4shell, CVE-2021-45105, Attempted User Privilege Gain"; flow:to_server,established; content:"Content-Disposition"; nocase; http_client_body; content:"RelyingPartyEntityId"; distance:0; nocase; http_client_body; content:"|0D 0A 0D 0A|"; distance:0; http_client_body; base64_decode:bytes 64,relative; base64_data; pcre:"/¥x24¥x7b(jndi|[^¥x7d]*?¥x24¥x7b[^¥x7d]*?¥x3a[^¥x7d]*?¥x7d)/i"; content:"/websso/SAML2/SSOSSL/"; fast_pattern:only; http_uri; sid:205557;)	Log4jShellの脆弱性 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) VMware vSphere への攻撃を検出するポリシー	log4shell, CVE-2021-45105
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05558 log4shell, CVE-2021-45105, Attempted User Privilege Gain"; flow:to_server,established; content:"jndi"; fast_pattern:only; http_header; pcre:"/(%(25)?24|¥x24)(%(25)?7b|¥x7b)jndi(%(25)?3a|¥x3a)/Hi"; sid:205558;)	Log4jShellの脆弱性 (CVE-2021-44228、CVE-2021-45046、CVE-2021-45105) 攻撃を検出するポリシー	log4shell, CVE-2021-45105
alert udp $EXTERNAL_NET any -> $HOME_NET 9034 (msg:"IGRSS.2.05592 RealTek, CVE-2021-35394, Attempted User Privilege Gain"; flow:to_server; content:"orf"; depth:3; pcre:"/^orf.*([¥x60¥x3b¥x7c¥x23¥x26]|[¥x3c¥x3e¥x24]¥x28)/s"; sid:205592;)	RealTekのCVE-2021-35394 の脆弱性を悪用した アクセス許可継承の試行を 検出するポリシー	RealTek, CVE-2021-35394
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.05661 Malware, MuddyWater, A Network Trojan was detected"; flow:to_client,established; flowbits:isset,file.pdf; file_data; content:"/URI"; nocase; content:"snapfile.org"; within:100; nocase; sid:805661;)	MuddyWaterのマルウェアによる ネットワーク通信を検出する ポリシー	Malware, MuddyWater

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved