SECURITY REPORT

2022 JAN

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01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。

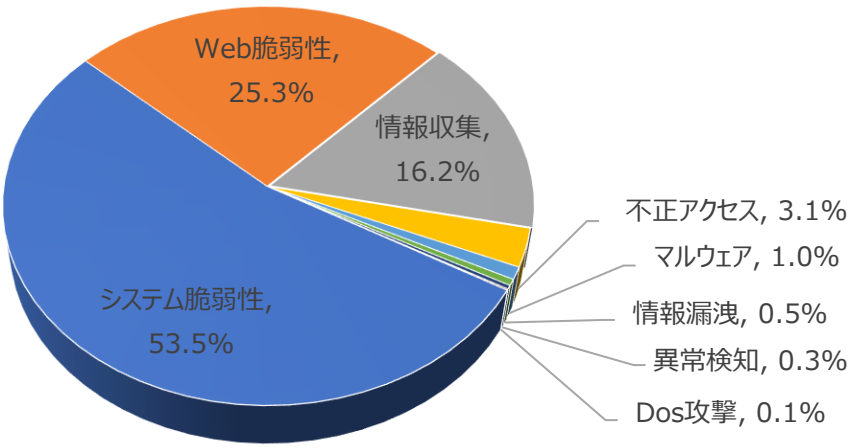
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	53.5%	▲1
Web脆弱性(Web Vulnerability)	25.3%	▼1
情報収集(Information Gathering)	16.2%	-
不正アクセス(Unauthorized access)	3.1%	-
マルウェア(Malware)	1.0%	-
情報漏洩(Information Exposure)	0.5%	▲1
異常検知(Anomaly Detection)	0.3%	▼1
Dos攻撃(Denial of service attack)	0.1%	-

2022年01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。

特にシステム脆弱性に関連する攻撃は約22%増加しました。Apache Log4j RCE攻撃数が増加したためです。

また、全体的なランキングは前月とあまり変わりませんが、システム脆弱性は全体の50%以上を占めています。

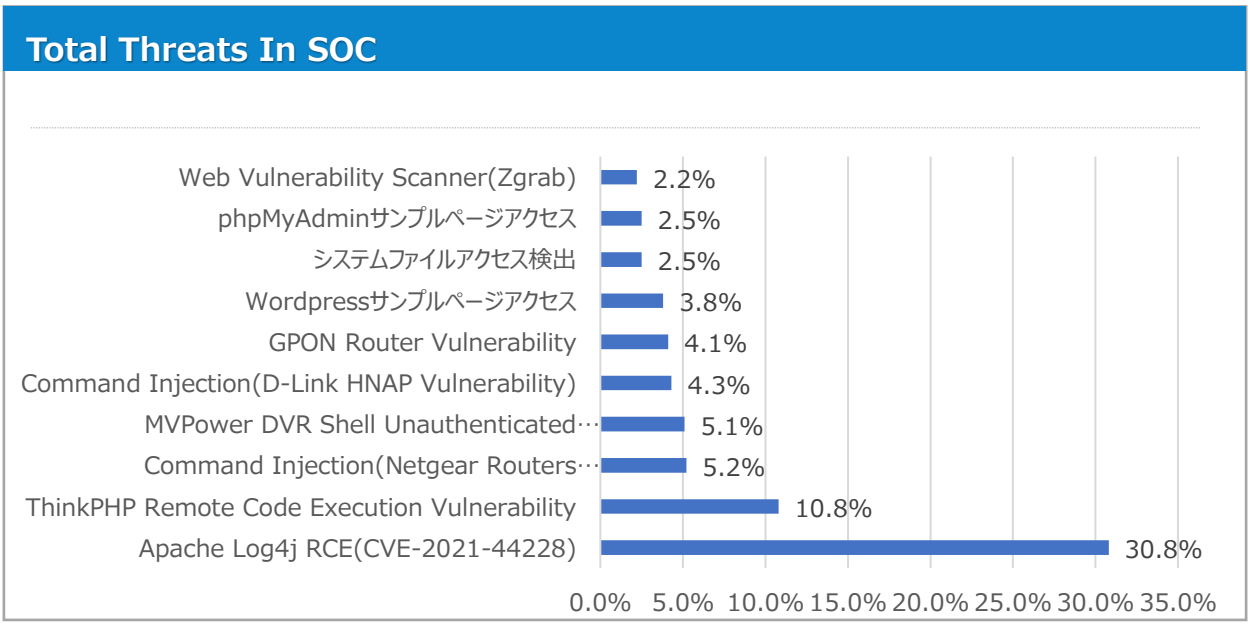


月次攻撃サービスの統計及び分析 - 2022年01月

02. 月次脆弱性攻撃TOP10

2022年01月の月次脆弱性TOP10を確認した結果、Apache Log4j RCE(CVE-2021-44228)攻撃とphpMyAdminサンプルページアクセス攻撃がトップ10に入り、Apache Log4j RCE(CVE-2021-44228)攻撃は全体の3分の1を占めました。
これは、TOP10の攻撃数合計が先月と比較して2倍に増加したことを示しています。

順位	検知名	比率(%)	比較
1	Apache Log4j RCE(CVE-2021-44228)	30.8%	NEW
2	ThinkPHP Remote Code Execution Vulnerability	10.8%	▼1
3	Command Injection (Netgear Routers Vulnerability)	5.2%	▼1
4	MVPower DVR Shell Unauthenticated Command Execution	5.1%	▼1
5	Command Injection (D-Link HNAP Vulnerability)	4.3%	▲1
6	GPON Router Vulnerability	4.1%	▼1
7	Wordpressサンプルページアクセス	3.8%	-
8	システムファイルアクセス検出	2.5%	-
9	phpMyAdminサンプルページアクセス	2.5%	NEW
10	Web Vulnerability Scanner(Zgrab)	2.2%	-



月次攻撃サービスの統計及び分析 - 2022年01月

03. 月次ブラックリストIPアドレスTOP 10

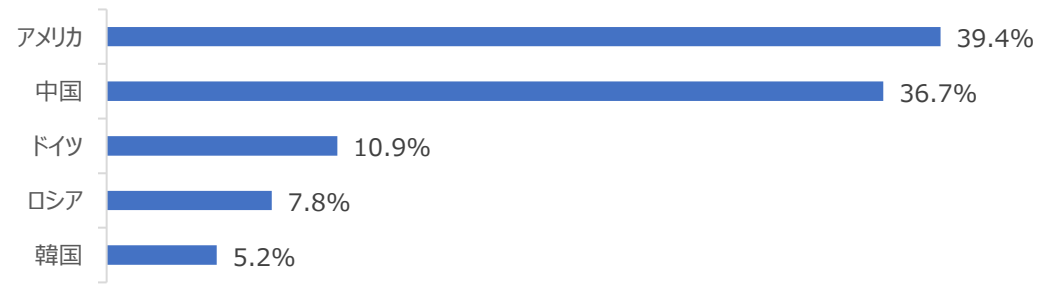
2022年01月についてTOP10を確認し結果、アメリカでの攻撃の割合は前月から1.7倍に増加しました。
一方、中国の攻撃率はやや低下していますが、依然として高い値です。

※ 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	45.155.205.233	RU	ThinkPHP Framework index.php controller RCE
2	195.54.160.149	FR	Directory Traversal
3	167.71.175.10	US	Apache Log4j RCE(CVE-2021-44228)
4	5.157.38.50	SE	Apache Log4j RCE(CVE-2021-44228)
5	84.17.48.84	DE	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
6	170.210.45.163	AR	Apache Log4j RCE(CVE-2021-44228)
7	77.37.134.80	RU	Apache Log4j RCE(CVE-2021-44228)
8	86.109.208.194	RU	Apache Log4j RCE(CVE-2021-44228)
9	175.6.210.66	CN	Apache Log4j RCE(CVE-2021-44228)
10	47.241.208.155	SG	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	45.155.205.233	RU
2	195.54.160.149	FR
3	167.71.175.10	US
4	5.157.38.50	SE
5	84.17.48.84	DE

Rank	Source IP	Country
6	170.210.45.163	AR
7	77.37.134.80	RU
8	86.109.208.194	RU
9	175.6.210.66	CN
10	47.241.208.155	SG

攻撃パターン毎の詳細分析結果

1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。

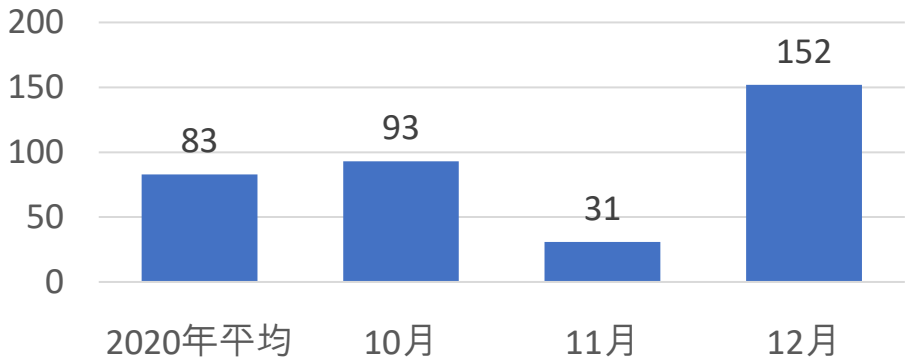
攻撃パターン	詳細分析結果
Apache Log4j RCE (CVE-2021-44228)	オープンソースのJava logging libraryのApache Log4jを使用することで、攻撃者は認証無しでサーバ上のリモートコマンドを実行できる。
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード実行攻撃ができる脆弱性である。￥think￥*クラスを呼び出して脆弱なオブジェクトを介して攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
CommandInjection (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。
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。
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。
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。
phpMyAdmin サンプルページ アクセス	PhpMyAdmin はWeb サーバ上で MySQL管理を目的としてPHP記述されたオープンソースツールであり、my-SQL サーバ上の脆弱性発見、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 文の実行、および権限管理機能の実行を可能とする。 この脆弱性が存在する場合、phpMyAdminのscript/setup.phpは、ファイル内引数 '?' を使用し、関数を挿入してシステムコマンドを実行できる脆弱性を持つ。
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、2022年12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152件である。

Apache Log4j2 (CVE-2021-44228)、(CVE-2021-45046)、 (CVE-2021-45105)の脆弱性に関するポリシーが配布された。



3か月間件数

5,515
全体配布量

152
今月配布量

31
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 $HTTP_PORTS (msg:"IGRSS.2.05436 Apache, Log4j2, CVE-2021-44228, Attempted User Privilege Gain"; flow:to_server,established; content:"${jndi:"; fast_pattern:only; http_uri; sid:205436;)	Apache Log4j2のCVE-2021-44228、CVE-2021-45046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	Apache, Log4j2, CVE-2021-44228
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05438 Apache, Log4j2, CVE-2021-44228, Attempted User Privilege Gain"; flow:to_server,established; content:"jndi"; fast_pattern:only; content:"jndi"; nocase; http_cookie; pcre:"/(%(25)?24|\x24)(%(25)?7b|\x7b)jndi(%(25)?3a|\x3a)/Ci"; sid:205438;)	Apache Log4j2のCVE-2021-44228、CVE-2021-45046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	Apache, Log4j2, CVE-2021-44228
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05441 Apache, Log4j2, CVE-2021-44228, Attempted User Privilege Gain"; flow:to_server,established; content:"%24%7b"; fast_pattern:only; http_client_body; pcre:"/%24%7b.{0,200}(%(25)?24|\x24)(%(25)?7b|\x7b).{0,200}(%(25)?3a|\x3a)(%(25)?(27|2d|5c|22)|[\x27\x2d\x5c\x22])*([jndi\x7d\x3a\x2d]|(%(25)?(7d|3a|2d))|(%(25)?5c|\x5c)u00[a-f0-9]{2}){1,4}(%(25)?(22|27)|[\x22\x27])?(%(25)?(3a|7d)|[\x3a\x7djndi])/Pi"; sid:205441;)	Apache Log4j2のCVE-2021-44228、CVE-2021-45046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	Apache, Log4j2, CVE-2021-44228
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05537 Apache, Log4j2, CVE-2021-44228, Attempted User Privilege Gain"; flow:to_server,established; content:"jndi"; fast_pattern:only; content:"jndi"; nocase; http_cookie; pcre:"/(%(25)?24|\x24)(%(25)?7b|\x7b)jndi(%(25)?3a|\x3a)/Ci"; sid:205537;)	Apache Log4j2のCVE-2021-44228、CVE-2021-45046、CVE-2021-45105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	Apache, Log4j2, CVE-2021-44228