SECURITY REPORT

2022 APR

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4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頂ければと思います。

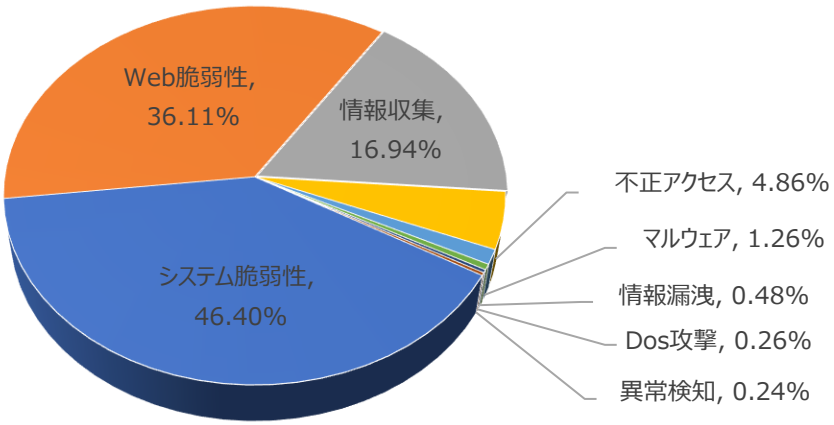
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	39.84%	-
Web脆弱性(Web Vulnerability)	36.11%	-
情報収集(Information Gathering)	16.94%	-
不正アクセス(Unauthorized access)	4.86%	-
マルウェア(Malware)	1.26%	-
情報漏洩(Information Exposure)	0.48%	-
Dos攻撃(Denial of service attack)	0.26%	▲1
異常検知(Anomaly Detection)	0.24%	▼1

2022年4月の攻撃類型を確認した結果、攻撃の総数は前月比で約1.2%ほど増加し、それぞれの攻撃パターン件数も増加していることが確認できる。

このうち、Web脆弱性関連攻撃率が前月比で4.5%ほど増加し、これはThinkPHP Remote Code Execution Vulnerability 攻撃数の増加によるものであることがわかる。

これに対し、システム脆弱性関連攻撃率は前月比約6.5%ほど低下した。

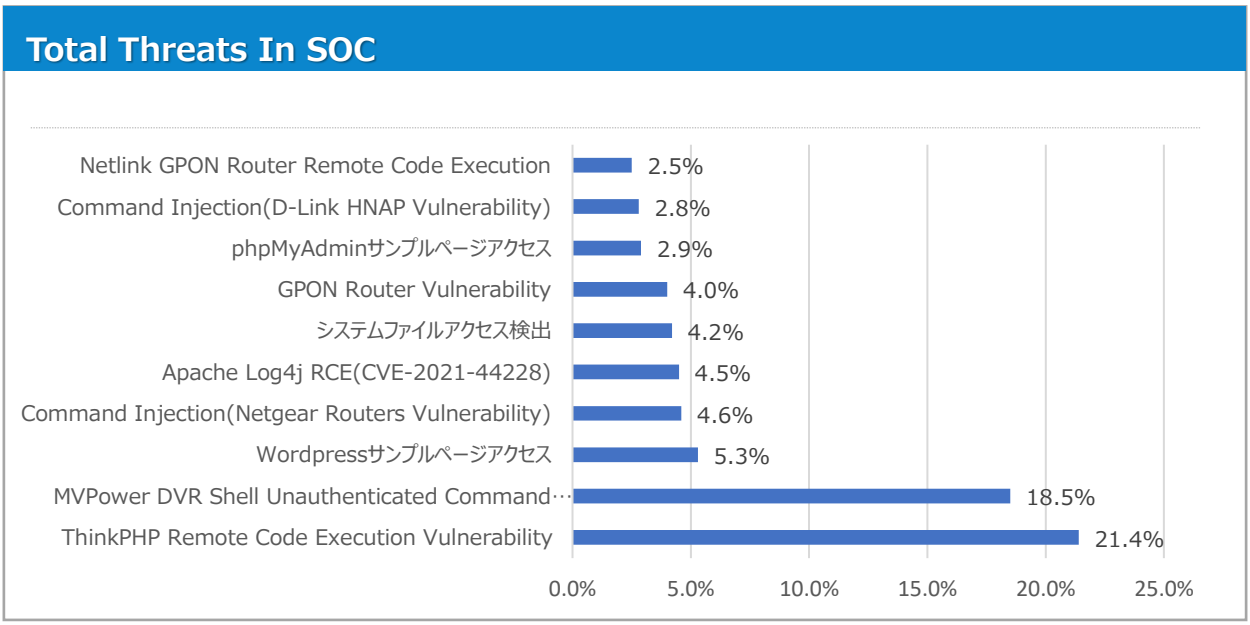


月次攻撃サービスの統計及び分析 - 2022年4月

02. 月次脆弱性攻撃TOP10

2022年4月の月次脆弱性TOP10を確認した結果、 Apache Log4j RCE(CVE-2021-44228) 攻撃が新たにTOP10に入り、 ThinkPHP Remote Code Execution Vulnerability攻撃は前月に比べて約1.8倍増加し、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	21.4%	▲1
2	MVPower DVR Shell Unauthenticated Command Execution	18.5%	▼1
3	Wordpressサンプルページアクセス	5.3%	▲1
4	Command Injection (Netgear Routers Vulnerability)	4.6%	▼1
5	Apache Log4j RCE(CVE-2021-44228)	4.5%	NEW
6	システムファイルアクセス検出	4.2%	▼1
7	GPON Router Vulnerability	4.0%	▼1
8	phpMyAdminサンプルページアクセス	2.9%	-
9	Command Injection (D-Link HNAP Vulnerability)	2.8%	▼2
10	Netlink GPON Router Remote Code Execution	2.5%	▼1



月次攻撃サービスの統計及び分析 - 2022年4月

03. 月次ブラックリストIPアドレスTOP 10

2022年4月についてTOP10を確認した結果、アメリカとエジプトの攻撃比率が上昇し、中国とインド、韓国の攻撃比率が少し減少しました。

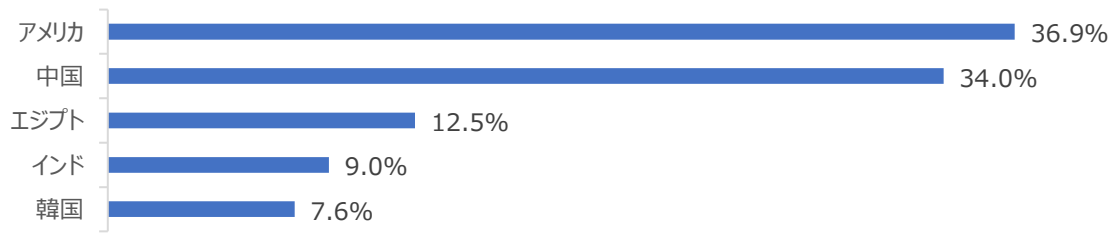
アメリカと中国の攻撃比率の合計は全体の45%となり、半分以下に減少したことが確認できます。

※ 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ます。

順位	ブックリストIP	国	攻撃情報
1	45.134.144.140	DE	Fortinet FortiOS Directory Traversal (CVE-2018-13379)
2	45.155.204.146	RU	ThinkPHP Remote Code Execution Vulnerability
3	109.237.103.118	RU	システムファイルアクセス検出
4	45.134.144.143	DE	Fortinet FortiOS Directory Traversal (CVE-2018-13379)
5	128.136.255.76	US	Apache Log4j RCE(CVE-2021-44228)
6	109.237.103.9	RU	システムファイルアクセス検出
7	49.143.32.6	KR	MVPower DVR Shell Unauthenticated Command Execution
8	45.134.144.144	DE	Fortinet FortiOS Directory Traversal (CVE-2018-13379)
9	148.72.213.165	SG	Apache Log4j RCE(CVE-2021-44228)
10	109.237.103.38	RU	システムファイルアクセス検出

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	45.134.144.140	DE
2	45.155.204.146	RU
3	109.237.103.118	RU
4	45.134.144.143	DE
5	128.136.255.76	US

Rank	Source IP	Country
6	109.237.103.9	RU
7	49.143.32.6	KR
8	45.134.144.144	DE
9	148.72.213.165	SG
10	109.237.103.38	RU

攻撃パターン毎の詳細分析結果

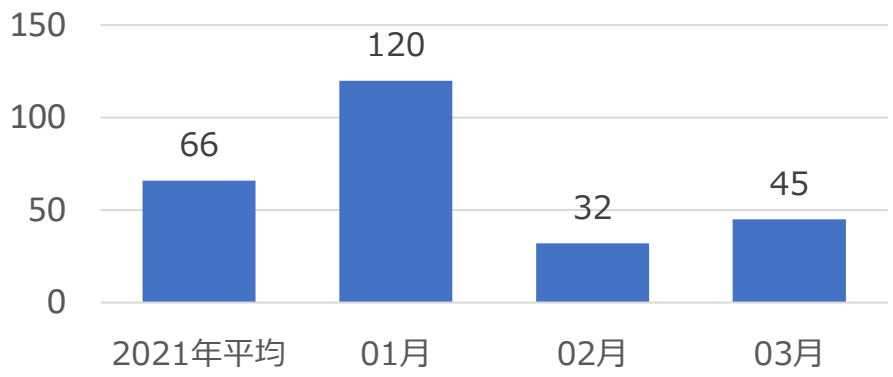
4月に発生した攻撃パターンTOP10の詳細分析を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該のシステムの脆弱性を事前に処置されることを推奨します。

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。
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。
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。
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。
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。
phpMyAdmin サンプルページへ アクセス	phpMyAdminはMySQLをWebサーバで管理する目的にてPHPで作成されたオープンソースツールである。MySQLサーバを対象に脆弱性を見つけ、データベースの作成/削除、テーブルの作成/削除、フィールドの生成/削除、SQL文の実行など、権限を利用した管理機能実行による攻撃が可能となる。その脆弱性が存在する場合、phpMyAdminのscript/setup.phpファイルに `?` 引数を使用して任意の関数を挿入し、システム命令を実行できる。
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。
Netlink GPON Router Remote Code Execution	Netlink GPONルータで発見された脆弱性として、ターゲットアドレスの後に/boaform/admin/formPing文字列を入力して認証手順を通過する可能性がある。この脆弱性を悪用し、認証されていない攻撃者が端末からリモートでコマンドを実行、悪意のあるファイルをアップロードする などが可能になる。

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3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45件である。
主にApache、VMWare、MS IE、PHP、WebShell に対する検出ポリシーが配布された。



3か月間件数

5,712
全体配布量

45
今月配布量

32
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.10.05711 Apache, CVE-2021-42013, 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?|((%(2|%32)(e|%[46]5))|¥x2e){2})¥/){2}/Ii"; sid:1005711;)	Apache Webアプリケーションの CVE-2021-42013脆弱性を悪用したディレクトリパスナビゲーションを検出するポリシー	Apache, CVE-2021-42013
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.05722 Vmware, vCenter, CVE-2021-22005, Web Application Attack"; flow:to_server,established; content:"/analytics/telemetry/ph-stg/api/hyper/send"; fast_pattern:only; http_uri; sid:1005722;)	VMWare vCenterの CVE-2021-22005脆弱性を悪用したファイルアップロードの試みを検出するポリシー	Vmware, vCenter, CVE-2021-22005
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.2.05728 MS, IE, CVE-2022-24502, Attempted User Privilege Gain"; flow:to_client,established; file_data; content:"href"; nocase; content:"ms-"; within:100; nocase; content:"|3A|ofe|7C|u|7C|"; within:50; nocase; content:"|5C 5C|"; distance:0; pcre:"/href¥s*=¥s*[¥x22¥x27][^¥x22¥x27]*?ms-[a-z]+¥x3aofe¥x7cu¥x7c[^¥x22¥x27]*?¥x5c¥x5c[¥x2e¥x3f]¥x5c/i"; sid:205728;)	MS IEの CVE-2022-24502脆弱性を悪用したユーザ権限奪取を検出するポリシー	MS, IE, CVE-2022-24502
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05739 Webshell, PHP, C0ders, A Network Trojan was detected"; flow:to_server,established; content:".php?mode=phpcode"; fast_pattern:only; http_uri; sid:805739;)	C0ders PHP Webshellの ネットワーク通信を検出するポリシー	Webshell, PHP, C0ders