SECURITY REPORT

2022 MAR

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3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。

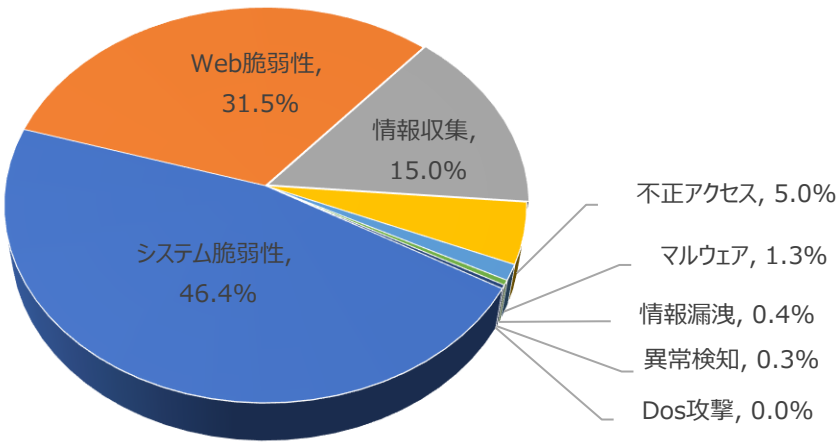
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	46.4%	▲1
Web脆弱性(Web Vulnerability)	31.5%	▼1
情報収集(Information Gathering)	15.0%	-
不正アクセス(Unauthorized access)	5.0%	-
マルウェア(Malware)	1.3%	-
情報漏洩(Information Exposure)	0.4%	▲1
異常検知(Anomaly Detection)	0.3%	▼1
Dos攻撃(Denial of service attack)	0.0%	-

2022年3月の攻撃類型を確認した結果、攻撃の総数は前月と同様でしたが、システム脆弱性関連の攻撃は前月から12%増加してTOPとなり、MVPower DVR Shell Unauthenticated Command Execution攻撃数が増加しました。

一方、Web脆弱性関連の攻撃は前月から10%減少しています。

これはThinkPHP Remote Code Execution 攻撃数が減少した結果として見ることができます。

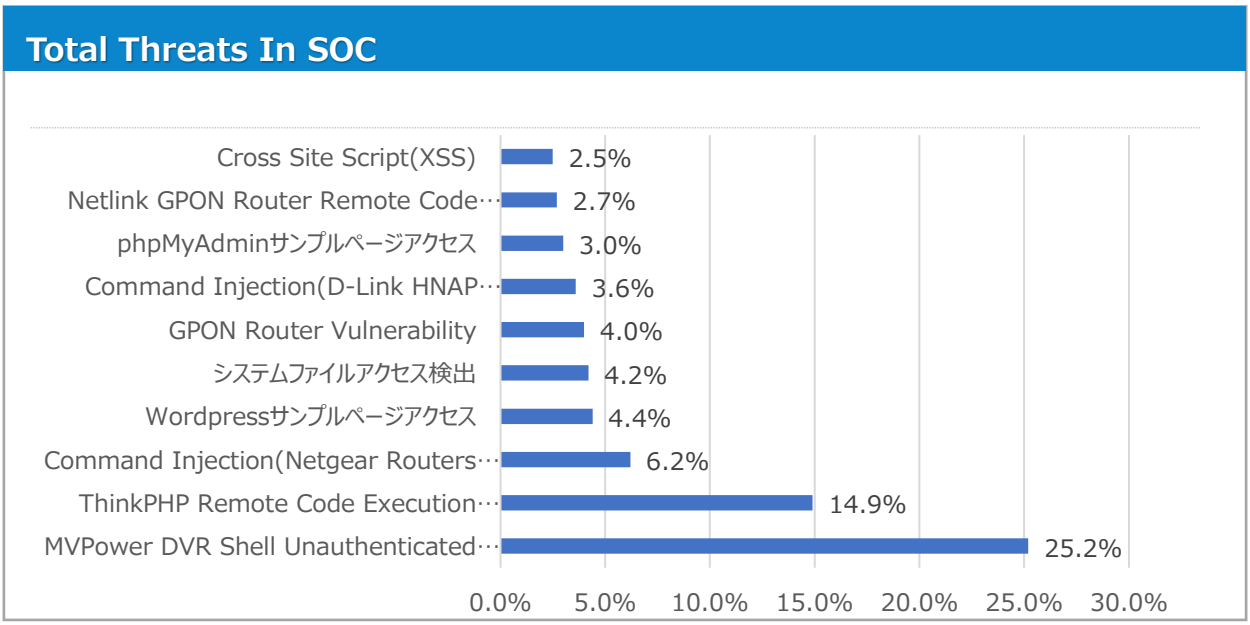


月次攻撃サービスの統計及び分析 - 2022年3月

02. 月次脆弱性攻撃TOP10

2022年3月の月次脆弱性TOP10を確認した結果、 phpMyAdminサンプルページアクセス、 Netlink GPON Router Remote Code Execution攻撃が新たにTOP10に入り、 MVPower DVR Shell Unauthenticated Command Execution攻撃は前月に比べて約3.5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	MVPower DVR Shell Unauthenticated Command Execution	25.2%	▲1
2	ThinkPHP Remote Code Execution Vulnerability	14.9%	▼1
3	Command Injection (Netgear Routers Vulnerability)	6.2%	▲1
4	Wordpressサンプルページアクセス	4.4%	▲1
5	システムファイルアクセス検出	4.2%	▲2
6	GPON Router Vulnerability	4.0%	▲2
7	Command Injection (D-Link HNAP Vulnerability)	3.6%	▼1
8	phpMyAdminサンプルページアクセス	3.0%	NEW
9	Netlink GPON Router Remote Code Execution	2.7%	NEW
10	Cross Site Script(XSS)	2.5%	-



月次攻撃サービスの統計及び分析 - 2022年3月

03. 月次ブラックリストIPアドレスTOP 10

2022年3月についてTOP10を確認し結果、インド、韓国、ロシアでの攻撃の割合が増加しています。

一方、中国とアメリカの割合は若干減少しました。

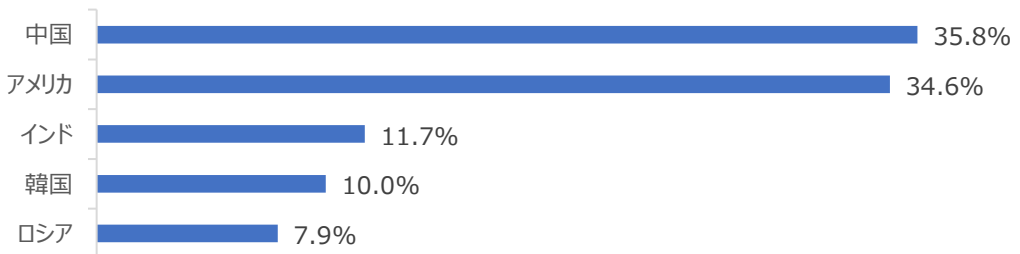
また、アメリカ、中国の攻撃率合計は、先月での全体80%より下がりましたが、70%に迫っています。

※ 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ます。

順位	ブックリストIP	国	攻撃情報
1	125.247.163.99	KR	ThinkPHP Remote Code Execution Vulnerability
2	45.77.178.30	JP	Apache Log4j RCE(CVE-2021-44228)
3	178.239.21.16	CN	Directory Traversal
4	109.237.103.118	RU	システムファイルアクセス検出
5	209.141.61.40	US	phpMyAdminサンプルページのアクセス
6	164.90.204.15	NL	Method(Connect)
7	109.237.103.9	RU	システムファイルアクセス検出
8	205.185.127.43	US	phpMyAdminサンプルページのアクセス
9	205.185.125.167	US	phpMyAdminサンプルページのアクセス
10	209.141.52.239	US	phpMyAdminサンプルページのアクセス

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	125.247.163.99	KR
2	45.77.178.30	JP
3	178.239.21.16	CN
4	109.237.103.118	RU
5	209.141.61.40	US

Rank	Source IP	Country
6	164.90.204.15	NL
7	109.237.103.9	RU
8	205.185.127.43	US
9	205.185.125.167	US
10	209.141.52.239	US

攻撃パターン毎の詳細分析結果

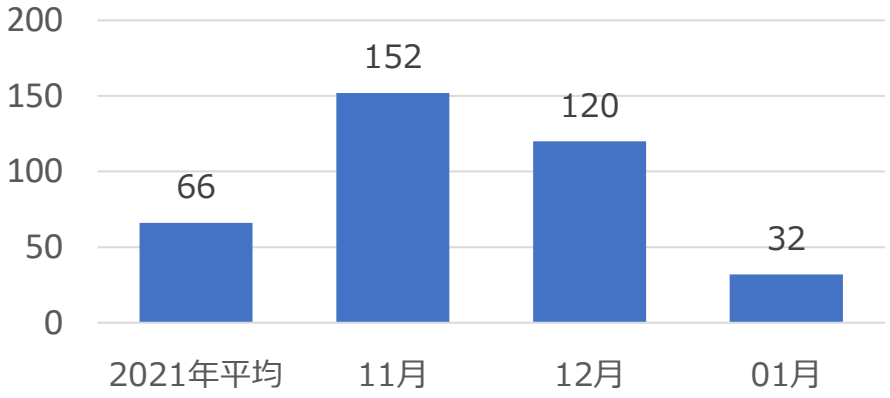
3月に発生した攻撃パターンTOP10の詳細分析を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該のシステムの脆弱性を事前に処置されることを推奨します。

攻撃パターン	詳細分析結果
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。
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。
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。
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。
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。
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。
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。

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2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32件である。
主にAntichat、 AyyildizTim、AK74、Alpha の各PHP Webshell 検出ポリシーが配布された。



3か月間件数

5,667
全体配布量

32
今月配布量

120
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.8.05675 Webshell, PHP, Antichat, A Network Trojan was detected"; flow:to_server,established; file_data; content:"<?"; content:"Antichat Shell"; fast_pattern:only; sid:805675;)	PHP.Webshell.Antichatのネットワーク通信を検出するポリシー	Webshell, PHP, Antichat
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"IGRSS.8.05677 Webshell, PHP, AyyildizTim, A Network Trojan was detected"; flow:to_client,established; file_data; content:"<title>"; content:"Ayyildiz Tim"; within:25; fast_pattern; nocase; sid:805677;)	PHP.Webshell.AyyildizTimのネットワーク通信を検出するポリシー	Webshell, PHP, AyyildizTim
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05684 Webshell, PHP, AK74, A Network Trojan was detected"; flow:to_server,established; content:".php?act=exesys"; fast_pattern:only; http_uri; sid:805684;)	PHP.Webshell.AK74のネットワーク通信を検出するポリシー	Webshell, PHP, AK74
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"IGRSS.8.05689 Webshell, PHP, Alpha, A Network Trojan was detected"; flow:to_client,established; file_data; content:"<title>"; nocase; content:"ALFA TEaM Shell"; within:100; fast_pattern; nocase; sid:805689;)	PHP.Webshell.Alphaのネットワーク通信を検出するポリシー	Webshell, PHP, Alpha