SECURITY REPORT

2022 MAY

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5月

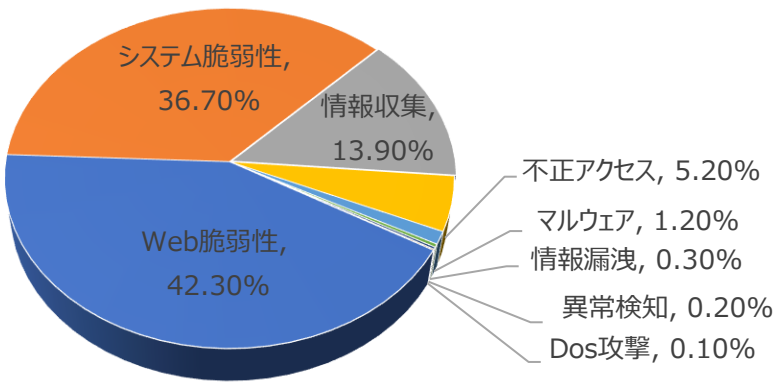
株式会社サイバーフォートレスでは攻撃情報を収集し、分析しています。
分析内容から、月次攻撃類型、脆弱性攻撃、ブラックリストのTOP10を確認し、過去データと比較し、
攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てて頂ければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	42.3%	▲1
システム脆弱性(System Vulnerability)	36.7%	▼1
情報収集(Information Gathering)	13.9%	-
不正アクセス(Unauthorized access)	5.2%	-
マルウェア(Malware)	1.2%	-
情報漏洩(Information Exposure)	0.3%	-
異常検知(Anomaly Detection)	0.2%	▲1
Dos攻撃(Denial of service attack)	0.1%	▼1

2022年5月の攻撃類型を確認した結果、攻撃の総数は前月比で約0.85倍ほど減少し、それぞれの攻撃パターン件数も減少していることが確認できる。

このうち、システム脆弱性関連攻撃率が前月比約3.15%ほど減少し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃数件数の減少によるものであることがわかる。



Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

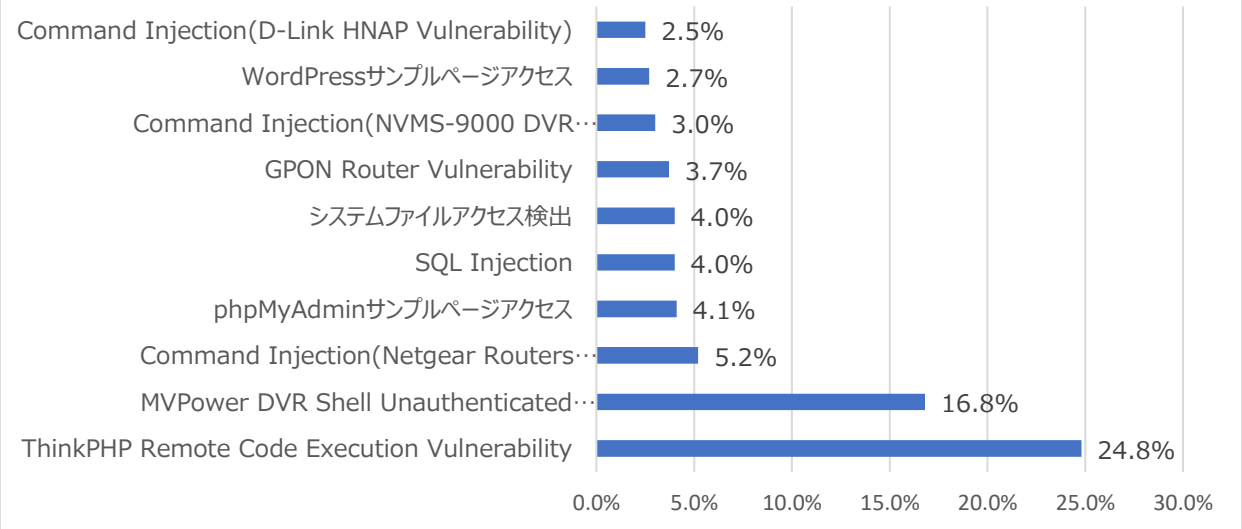
月次攻撃サービスの統計及び分析 - 2022年5月

02. 月次脆弱性攻撃TOP10

2022年5月の月次脆弱性TOP10を確認した結果、 SQL Injectionと Command Injection（NVMS-9000 DVR Vulnerability）攻撃が新たにTOP10に入り、全体的な攻撃件数が減少したことを確認することができます。特に MVPower DVR Shell Unauthenticated Command Execution攻撃は前月に比べて700件ほど大幅に減少しています。

順位	検知名	比率(%)	比較
1	ThinkPHP Remote Code Execution Vulnerability	24.8%	-
2	MVPower DVR Shell Unauthenticated Command Execution	16.8%	-
3	Command Injection (Netgear Routers Vulnerability)	5.2%	▲1
4	phpMyAdminサンプルページアクセス	4.1%	▲4
5	SQL Injection	4.0%	NEW
6	システムファイルアクセス検出	4.0%	-
7	GPON Router Vulnerability	3.7%	-
8	Command Injection (NVMS-9000 DVR Vulnerability)	3.0%	NEW
9	WordPressサンプルページアクセス	2.7%	▼6
10	Command Injection (D-Link HNAP Vulnerability)	2.5%	▼1

Total Threats In SOC



Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2022年5月

03. 月次ブラックリストIPアドレスTOP 10

2022年5月についてTOP10を確認した結果、韓国の攻撃比率が上昇し、アメリカと中国、エジプト、インドの攻撃比率が少し減少しました。

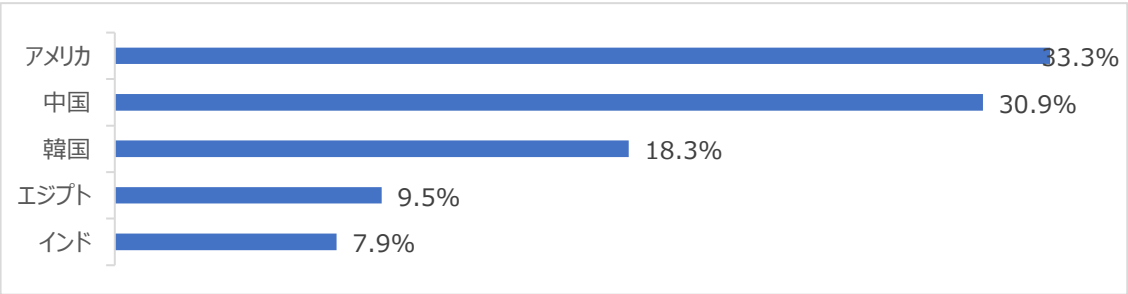
アメリカと中国の攻撃比率合計は全体の40%になり、半分以下に減少したことに加えて減少傾向にあることが確認できます。

※ 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	45.155.204.146	RU	Directory Traversal
2	213.226.123.30	PL	ThinkPHP Remote Code Execution Vulnerability
3	92.223.86.24	SG	Command Injection
4	92.223.86.10	SG	Oracle WebLogic wls-wsat RCE(CVE-2017-10271)
5	45.134.144.140	DE	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
6	38.114.114.55	US	etcpasswd Detect
7	49.143.32.6	KR	Command Injection(Netgear Routers Vulnerability)
8	144.22.198.141	BR	Apache Log4j RCE(CVE-2021-44228)
9	81.17.20.98	CH	Apache Log4j RCE(CVE-2021-44228)
10	109.237.103.9	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	Rank	Source IP	Country
1	45.155.204.146	RU	6	38.114.114.55	US
2	213.226.123.30	PL	7	49.143.32.6	KR
3	92.223.86.24	SG	8	144.22.198.141	BR
4	92.223.86.10	SG	9	81.17.20.98	CH
5	45.134.144.140	DE	10	109.237.103.9	RU

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

攻撃パターン毎の詳細分析結果

5月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
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システムの脆弱性を事前に対処されることを推奨いたします。

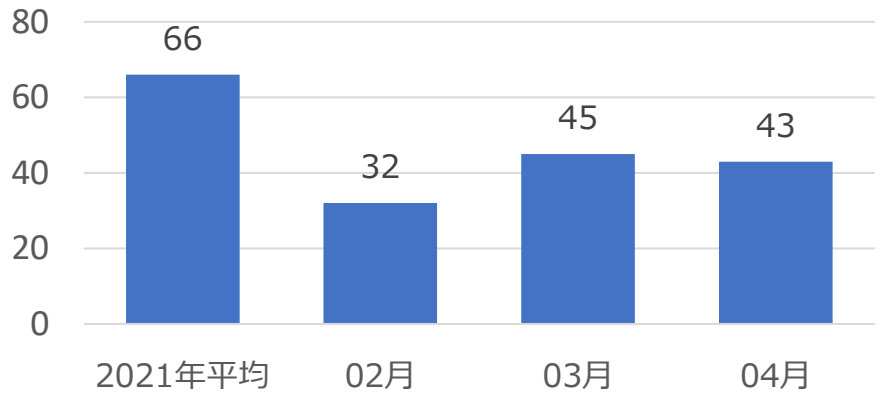
攻撃パターン	詳細分析結果
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード実行攻撃ができる脆弱性である。¥think¥*クラスを呼び出して脆弱なオブジェクトを介して攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥'shell¥'」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。
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。
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。
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使用する入力値において、文字(特殊文字、UnionやSelectなど)をフィルタリングせずに入力値がクエリ文に使用される場合、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。
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 (NVMS-9000 DVR Vulnerability)	Shenzhen TVT社のNVMS-9000 DVR機器の複数の脆弱性が検出された。攻撃者は該当DVR機器の基本アカウント情報をハードコードにて認証後、BOF(Buffer OverFlow)、XMLパケットを利用したRCE(Remote Code Execution)攻撃が可能となる。
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。
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。

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4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43件です。
主にSpring4Shell（CVE-2022-22963、CVE-2022-22965）、Lazarus Malwareに対する検出ポリシーが配布されました。



3か月間件数

5,755
全体配布量

43
今月配布量

45
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.2.05759 Java, getRuntime, Vul, Attempted User Privilege Gain"; flow:to_server,established; content:"<%"; http_header; content:"getRuntime"; distance:0; nocase; http_header; content:"exec("; distance:0; nocase; http_header; sid:205759;)	Java get Runtimeの脆弱性によるユーザー権限の奪取の試みを検出するポリシー	Java, getRuntime, Vul
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.05760 Spring, Cloud, CVE-2022-22963, Web Application Attack"; flow:to_server,established; content:"/functionRouter"; fast_pattern:only; http_uri; content:"spring.cloud.function.routing-expression|3A|"; nocase; http_header; content:"java."; distance:0; nocase; http_header; pcre:"/spring¥x2ecloud¥x2efunction¥x2erouting-expression¥x3a[^¥r¥n]*java¥x2e[^¥r¥n]*¥x28/Hi"; sid:1005760;)	Spring Cloudの CVE-2022-22963脆弱性を悪用したリモートシステムコマンド実行攻撃を検出するポリシー	Spring, Cloud, CVE-2022-22963
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05771 Java, getRuntime, CVE-2022-22965, Attempted User Privilege Gain"; flow:to_server,established; content:"<%"; http_header; content:"getRuntime"; distance:0; nocase; http_header; content:"exec("; distance:0; nocase; http_header; sid:205771;)	Java getRuntimeの CVE-2022-22965 脆弱性を悪用したユーザー権限を奪う試みを検出するポリシー	Java, getRuntime, CVE-2022-22965
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.05788 Malware, Dropper, Lazarus, A Network Trojan was detected"; flow:to_server,established; content:"/repos/DanielManwarningRep/ERPLocalSys"; fast_pattern:only; http_uri; sid:805788;)	Lazarusで使用されるDropperのネットワーク通信を検出するためのポリシー	Malware, Dropper, Lazarus

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved