SECURITY REPORT

2022

JUNE

2022年6月
攻撃統計情報

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6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。

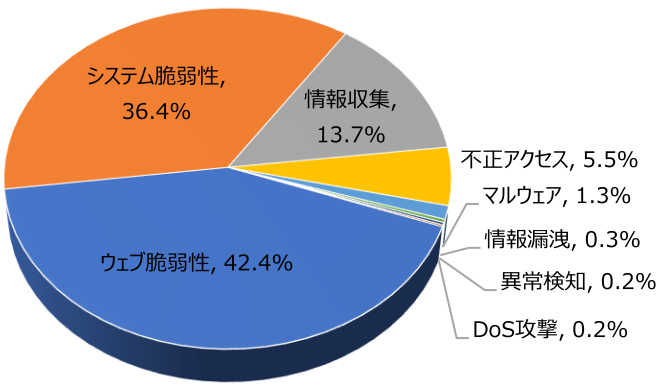
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	42.4%	-
システム脆弱性(System Vulnerability)	36.4%	-
情報収集(Information Gathering)	13.7%	-
不正アクセス(Unauthorized access)	5.5%	-
マルウェア(Malware)	1.3%	-
情報漏洩(Information Exposure)	0.3%	-
異常検知(Anomaly Detection)	0.2%	-
Dos攻撃(Denial of service attack)	0.2%	-

2022年6月の攻撃類型を確認した結果、全体の攻撃合計が先月と比べて約1.2倍ぐらい増加し、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た。

このうち、ウェブ脆弱性に関する攻撃は先月比べて約1,300件ほど増加し、これはThinkPHP Remote Code Execution Vulnerability攻撃件数の増加によるものだと確認できた。

また、システム脆弱性に関する攻撃は先月と比べて約1,000件ぐらい増加し、これはCommand Injection(NVMS-9000 DVR Vulneraility)攻撃件数増加によるものだと確認できた。

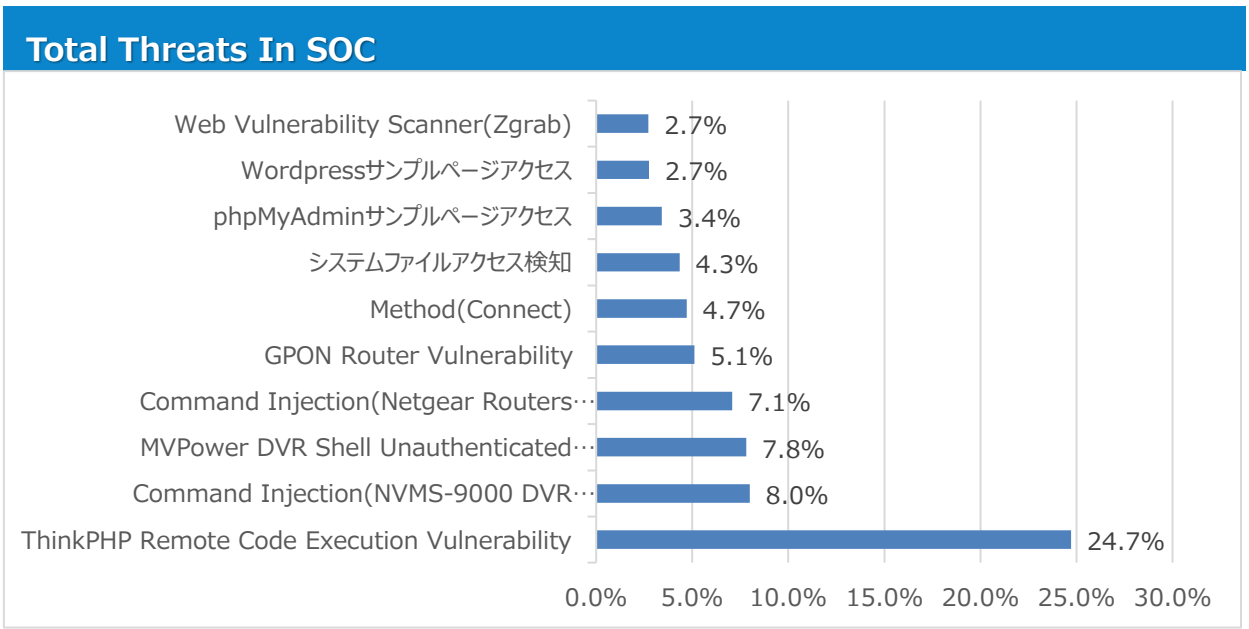


月次攻撃サービスの統計及び分析 - 2022年6月

02. 月次脆弱性攻撃TOP10

2022年6月の月次脆弱性TOP10を確認した結果、Method(Connect)とWeb Vulnerability Scanner(Zgrab)攻撃が新たにTOP10に登場し、全体的な攻撃件数が増加したことが確認できた。特にCommand Injection(NVMS-9000 DVR Vulnerability)攻撃が先月と比べて900件ぐらい大幅に増加した。

順位	検知名	比率(%)	比較
1	ThinkPHP Remote Code Execution Vulnerability	24.7%	-
2	Command Injection (NVMS-9000 DVR Vulnerability)	8.0%	▲6
3	MVPower DVR Shell Unauthenticated Command Execution	7.8%	▼1
4	Command Injection (Netgear Routers Vulnerability)	7.1%	▼1
5	GPON Router Vulnerability	5.1%	▲2
6	Method(Connect)	4.7%	NEW
7	システムファイルアクセス検出	4.3%	▼1
8	phpMyAdminサンプルページアクセス	3.4%	▼4
9	WordPressサンプルページアクセス	2.7%	-
10	Web Vulnerability Scanner(Zgrab)	2.7%	NEW



月次攻撃サービスの統計及び分析 - 2022年6月

03. 月次ブラックリストIPアドレスTOP 10

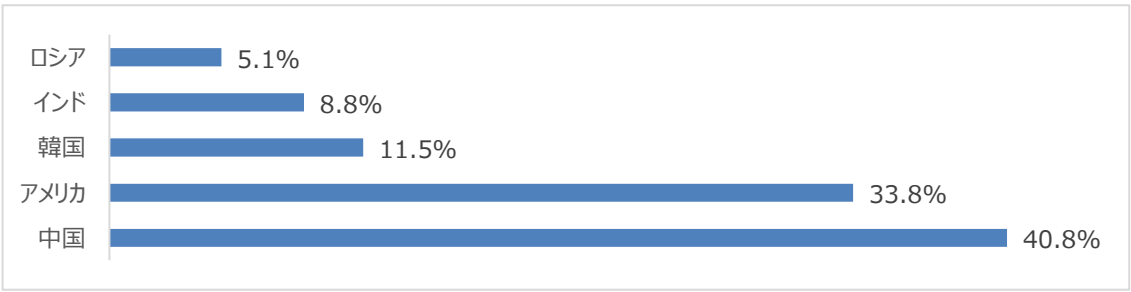
2022年6月についてTOP10を確認した結果、中国とインドの攻撃比率が増加し、一方アメリカと韓国、ロシアの攻撃の比率は減少した。アメリカと中国の攻撃比率の合計は全体に比べて約45%で、半分以下に減少したことが確認できた。

※ 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	195.3.221.30	PL	Apache Log4j RCE(CVE-2021-44228)
2	45.134.144.140	US	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
3	45.9.20.101	RU	Directory Traversal
4	49.143.32.6	KR	Command Injection(Netgear Routers Vulnerability)
5	192.64.113.244	US	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
6	143.244.35.193	US	Apache Log4j RCE(CVE-2021-44228)
7	213.226.123.30	RU	Application Vulnerability(PHPUnit)
8	3.21.162.140	US	システムファイルアクセス検出
9	164.90.204.15	NL	Method(Connect)
10	109.237.103.9	GB	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	195.3.221.30	PL	6	143.244.35.193	US
2	45.134.144.140	US	7	213.226.123.30	RU
3	45.9.20.101	RU	8	3.21.162.140	US
4	49.143.32.6	KR	9	164.90.204.15	NL
5	192.64.113.244	US	10	109.237.103.9	GB

攻撃パターン毎の詳細分析結果

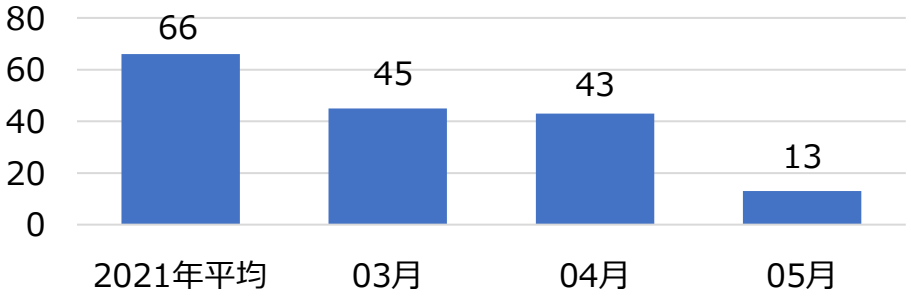
6月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
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。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security) トンネリングで内部アクセスを試す。これのためにConnect Methodを使用し、脆弱性が存在する場合攻撃のための中間経由地として使用される可能性がある。
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。
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。
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、ライセンスの無いポートなど、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5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13件です。
5月1か月の間、WolfRAT Malware, MS社のMSDT(CVE-2022-30190)に対する検知ポリシーが配布された。



3か月間件数

5,768
全体配布量

13
今月配布量

43
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.05794 Malware, WolfRAT , A Network Trojan was detected"; flow:to_server,established; content:"/Filesend/delete_file"; fast_pattern:only; http_uri; content:"user_id"; nocase; http_client_body; content:"token"; nocase; http_client_body; content:"eyJhbGciOiJSUzI1NiJ9"; nocase; http_client_body; sid:805794;)	WolfRAT Malwareの ネットワーク通信を検知するポリシー	Malware, WolfRAT
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.2.05795 MS, MSDT, CVE-2022-30190, Attempted User Privilege Gain"; flow:to_client,established; file_data; content:"ms-msdt|3A|"; fast_pattern; nocase; content:"id"; distance:0; nocase; pcre:"/ms-msdt¥x3a.*?([¥x2f¥x2d]?id¥s*PCWDiagnostic|IT_BrowseForFile)/is"; sid:205795;)	MS MSDTの CVE-2022-30190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	MS, MSDT, CVE-2022-30190
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.2.05804 MS, MSDT, CVE-2022-30190, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"ms-msdt|3A|"; fast_pattern; nocase; content:"id"; distance:0; nocase; pcre:"/href¥s*=¥s*[¥x22¥x27]?¥s*ms-msdt¥x3a/i"; sid:205804;)	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	MS, MSDT, CVE-2022-30190
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.05805 Malware, WolfRAT , A Network Trojan was detected"; flow:to_server,established; content:"/Authen/verify_token"; fast_pattern:only; http_uri; content:"user_id"; nocase; http_client_body; content:"token"; nocase; http_client_body; content:"eyJhbGciOiJSUzI1NiJ9"; nocase; http_client_body; sid:805805;)	WolfRAT Malwareの ネットワーク通信を検知するポリシー	Malware, WolfRAT