SECURITY REPORT

2024

JUN

2024年06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 - 2024年06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。

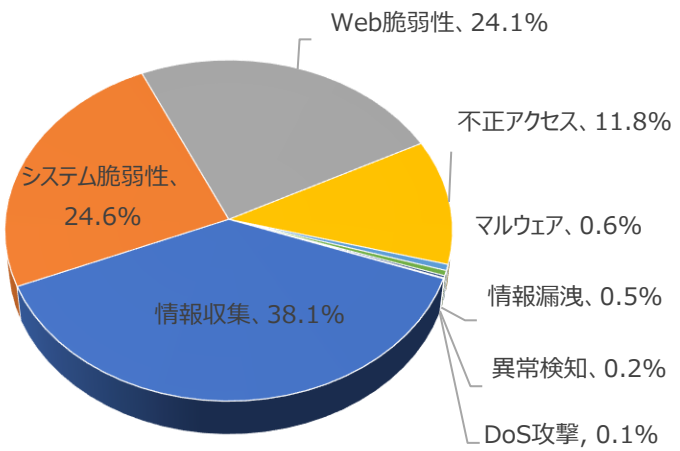
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	38.1%	-
システム脆弱性(System Vulnerability)	24.6%	▲1
Web脆弱性(Web Vulnerability)	24.1%	▼1
不正アクセス(Unauthorized access)	11.8%	-
マルウェア(Malware)	0.6%	-
情報漏洩(Information Exposure)	0.5%	-
異常検知(Anomaly Detection)	0.2%	-
DoS攻撃(Denial of service attack)	0.1%	-

2024年06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1.6倍ぐらい増加した。

そのうち、Web脆弱性に関する攻撃は先月比べて約528件ほど減少し、これはCommand Injection攻撃件数の減少によるものだと確認できた。

また、情報収集に関する攻撃は先月と比べて約2,121件ぐらい増加し、これはApache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)攻撃件数増加によるものだと確認できた。

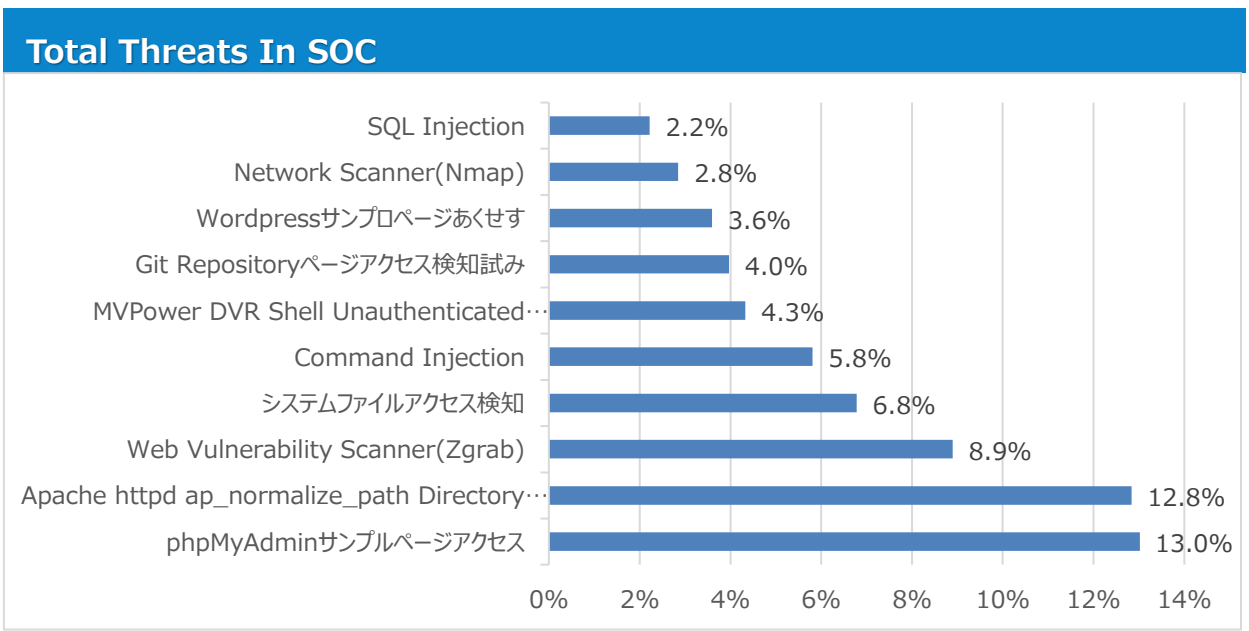


月次攻撃サービスの統計及び分析 - 2024年06月

02. 月次脆弱性攻撃TOP10

2024年06月の月次脆弱性TOP10を確認した結果、Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)攻撃が新たにTOP10に登場した。
全体的な攻撃件数は増加し、特にApache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)攻撃件数は先月と比べて約1,1120件ぐらい増加したことが確認できた。

順位	検知名	比率(%)	比較
1	phpMyAdminサンプルページアクセス	13.0%	▲2
2	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	12.8%	NEW
3	Web Vulnerability Scanner(Zgrab)	8.9%	▼2
4	システムファイルアクセス検知	6.8%	▲1
5	Command Injection	5.8%	▼3
6	MVPower DVR Shell Unauthenticated Command Execution	4.3%	NEW
7	Git Repositoryページアクセス検知試み	4.0%	-
8	Wordpressサンプロページあくせす	3.6%	NEW
9	Network Scanner(Nmap)	2.8%	▲1
10	SQL Injection	2.2%	▼6



月次攻撃サービスの統計及び分析 - 2024年06月

03. 月次ブラックリストIPアドレスTOP 10

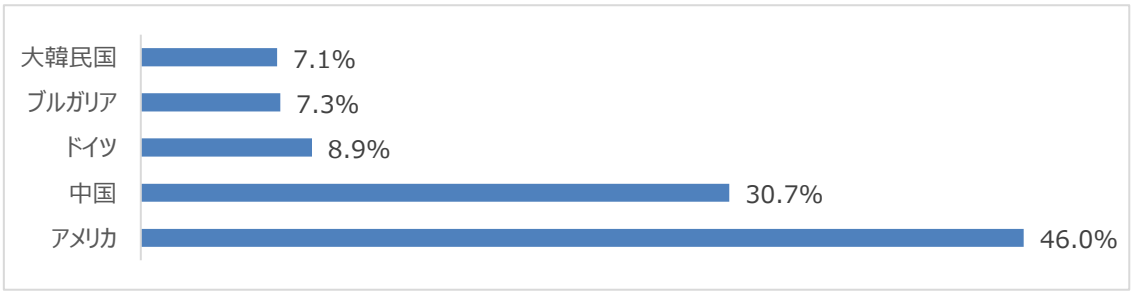
2024年06月についてTOP10を確認した結果、ドイツ、リトアニア、中国の攻撃比率が増加し、一方大韓民国の攻撃の比率は減少した。特にアメリカの攻撃比率が46%を超えていることが確認できた。

※ 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	78.153.140.177	GB	システムファイルアクセス
2	78.153.140.179	GB	システムファイルアクセス
3	141.98.11.79	LT	Method(Connect)
4	223.100.28.112	CN	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)
5	124.165.198.25	CN	Directory Traversal検知
6	195.1.144.109	NO	Command Injection
7	183.81.169.139	HK	TP-Link Router Remote Code Execution(CVE-2023-1389)
8	111.59.56.6	CN	ThinkPHP lang Remote Code Execution
9	51.158.205.47	NL	Network Scanner(masscan)
10	83.97.73.245	RU	etcpasswd Detect

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	78.153.140.177	GB
2	78.153.140.179	GB
3	141.98.11.79	LT
4	223.100.28.112	CN
5	124.165.198.25	CN

Rank	Source IP	Country
6	195.1.144.109	NO
7	183.81.169.139	HK
8	111.59.56.6	CN
9	51.158.205.47	NL
10	83.97.73.245	RU

攻撃パターン毎の詳細分析結果

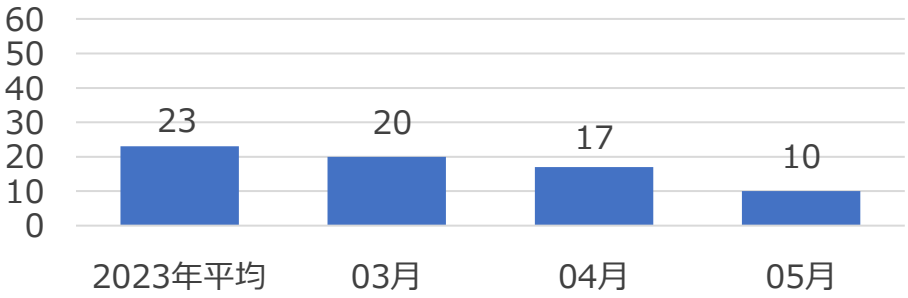
06月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
phpMyAdminサンプルページ 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。
Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	Apache httpd 에 Directory Traversal脆弱性が存在する。当該の脆弱性は「ap_normalize_path」関数でURIぱすに対する不適切な有効性検証から発生する。リモートの攻撃者は悪意的に改ざんされたHTTPリクエストを送信して攻撃できる。攻撃に成功すると情報が漏洩される。
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。
システムファイルアクセス検知	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。
Command Injection	システムコマンドが含まれている入力値が適切な検証プロセスを通らない場合、入力されたコマンドが実行 しうる。この脆弱性が存在する場合、攻撃者がシステムに直接コマンド送信できるため、ファイルの閲覧、 ダウンロード、実行などで追加被害が発生する可能性がある。
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。
Git Repository ページアクセス	ソースコードのバージョン管理のためにGit Repository(/.git/)をホスティングする場合、存在するそーそコード及び重要情報を確認するためにconfigやHEADなどのデフォルトパスの存在有無及びレポジトリのパスをスキャンする攻撃である。
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。
Network Scanner(Nmap)	代表的なNetwork Scanツールで、IP ScanとPort Scanの機能がある。ネットワーク脆弱性診断ツールとして活用されるが攻撃者から悪用されて攻撃ツールとして使用される。 .
SQL Injection	SQL Injection攻撃はウェブページから記号やUnion、Selectなどクエリで使用される文字列をフィ ルタリングせずに入力された値がクエリに使用される場合発生しうる。攻撃者はDBに繋がっているアカ ウントが持っている権限内で様々なクエリを使用して保存された情報の取得、修正、削除及びシステ ムアクセスなどが可能である。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年05の月の1か月間で共有されたサイバー脅威検知ポリシーは10件である。05月1か月間IcedID Malware, Commvault CommCell(CVE-2021-34996)などに対する検知ポリシーが配布された。



3か月間件数

6、438
全体配布量

10
今月配布量

17
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.8.06467 Malware, Trojan, IcedID, A Network Trojan was detected"; flow:to_server,established; content:"|2F 3F|status|3D|start|26|av|3D|"; fast_pattern:only; http_uri; content:" WindowsPowerShell|2F|"; nocase; http_header; content:"GET"; http_method; sid:806467;)	IcedID MalwareのPowershell Stagerのダウンロードを検知するポリシー	Malware, Trojan, IcedID
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.06468 Malware, Trojan, IcedID, A Network Trojan was detected"; flow:to_server,established; flowbits:isset,file.exe; file_data; content:"|33 C0 48 81 C4 08 04 00 00 C3|"; content:"|69 6E 69 74 00|"; within:7; content:"|4C 77 26 07|"; content:"|58 A4 53 E5|"; content:"|10 E1 8A C3|"; sid:806468;)	IcedID MalwareのDLLファイルのダウンロードを検知するポリシー	Malware, Trojan, IcedID
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.06474 Malware, Trojan, IcedID, A Network Trojan was detected"; flow:to_client,established; flowbits:isset,file.exe; file_data; content:"|33 C0 48 81 C4 08 04 00 00 C3|"; content:"|69 6E 69 74 00|"; within:7; content:"|4C 77 26 07|"; content:"|58 A4 53 E5|"; content:"|10 E1 8A C3|"; sid:806474;)	IcedID MalwareのDLLファイルのダウンロードを検知するポリシー	Malware, Trojan, IcedID
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.06475 SERVER-WEBAPP, Commvault, CommCell, CVE-2021-34996, Web Application Attack"; flow:to_server,established; content:"/webconsole/api/Workflow/Demo_ExecuteProcessOnGroup/Action/Execute"; fast_pattern:only; http_uri; sid:1006475;)	Commvault CommCellの脆弱性であるCVE-2021-34996を悪用したCommand Injection攻撃を検知するポリシー	SERVER-WEBAPP, Commvault, CommCell, CVE-2021-34996