SECURITY REPORT

2024

JUL

2024年07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。

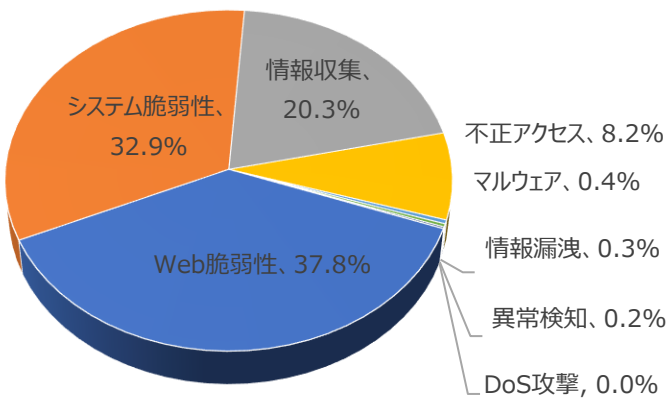
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	37.8%	▲1
システム脆弱性(System Vulnerability)	32.9%	▲1
情報収集(Information Gathering)	20.3%	▼2
不正アクセス(Unauthorized access)	8.2%	-
マルウェア(Malware)	0.4%	-
情報漏洩(Information Exposure)	0.3%	-
異常検知(Anomaly Detection)	0.2%	-
DoS攻撃(Denial of service attack)	0.0%	-

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1.4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5,208件ほど増加し、これはTraversal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5,831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。

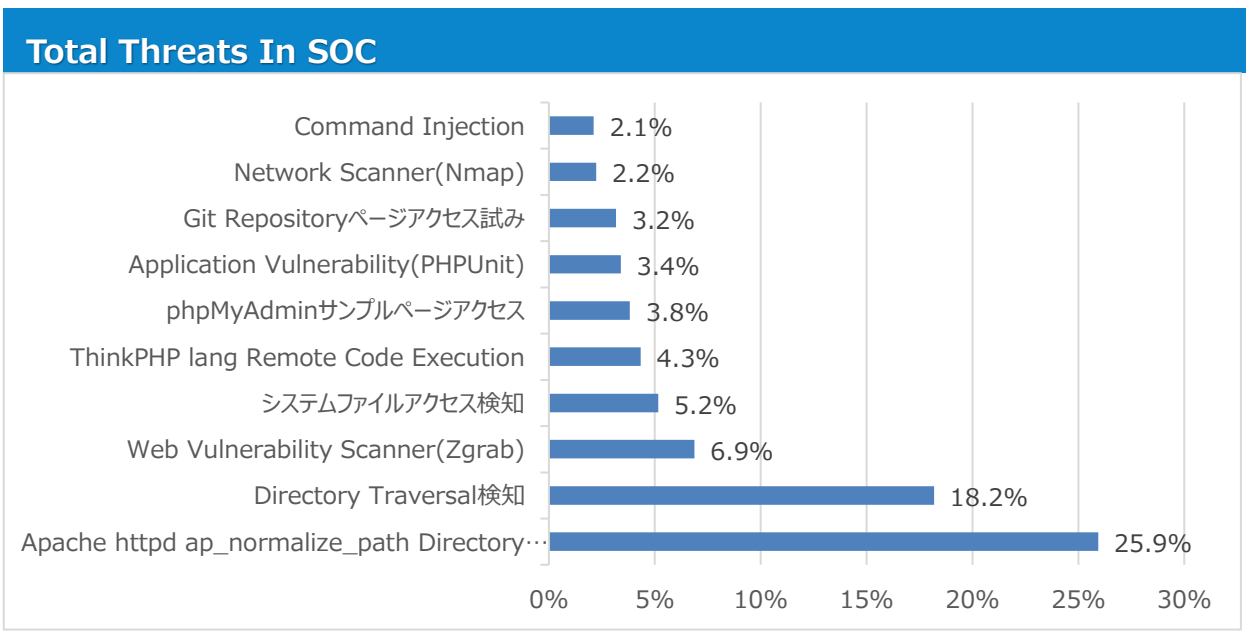


月次攻撃サービスの統計及び分析 - 2024年06月

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、 Directory Traversal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3,729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	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	25.9%	▲1
2	Directory Traversal検知	18.2%	NEW
3	Web Vulnerability Scanner(Zgrab)	6.9%	-
4	システムファイルアクセス検知	5.2%	-
5	ThinkPHP lang Remote Code Execution	4.3%	NEW
6	phpMyAdminサンプルページアクセス	3.8%	▼5
7	Application Vulnerability(PHPUnit)	3.4%	NEW
8	Git Repositoryページアクセス試み	3.2%	NEW
9	Network Scanner(Nmap)	2.2%	-
10	Command Injection	2.1%	▼5



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

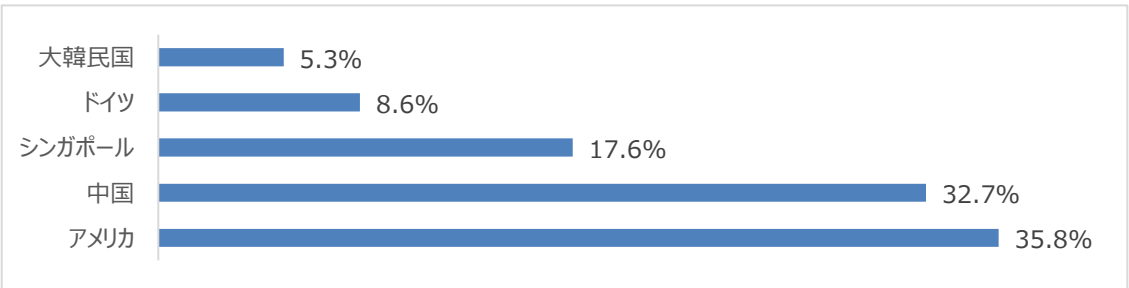
2024年06月についてTOP10を確認した結果、インドネシア、アメリカ、ロシア攻撃比率が増加し、一方シンガポールの攻撃の比率は減少した。特にアメリカの攻撃比率が35%を超えていることが確認できた。

※ 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	103.162.36.154	ID	Directory Traversal検知
2	34.172.237.230	US	ThinkPHP lang Remote Code Execution
3	47.245.32.141	JP	Directory Traversal検知
4	78.153.140.177	GB	システムファイルアクセス
5	110.14.63.139	KR	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
6	78.153.140.179	GB	システムファイルアクセス
7	141.98.11.79	LT	Method(Connect)
8	111.59.56.6	CN	ThinkPHP lang Remote Code Execution
9	118.107.44.111	HK	Directory Traversal検知
10	113.133.177.77	CN	ThinkPHP lang Remote Code Execution

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	103.162.36.154	ID	6	78.153.140.179	GB
2	34.172.237.230	US	7	141.98.11.79	LT
3	47.245.32.141	JP	8	111.59.56.6	CN
4	78.153.140.177	GB	9	118.107.44.111	HK
5	110.14.63.139	KR	10	113.133.177.77	CN

攻撃パターン毎の詳細分析結果

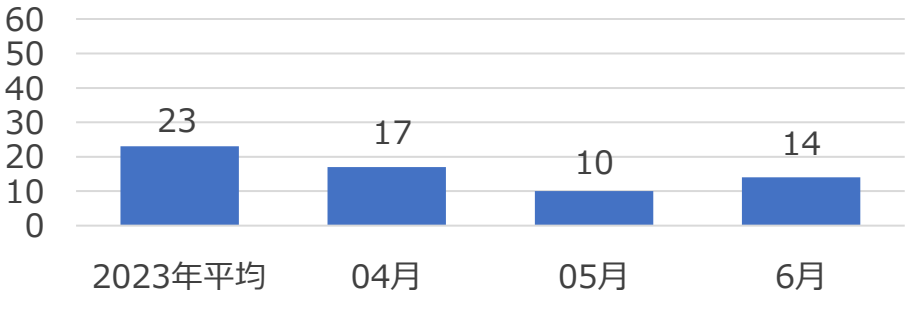
06月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	Apache httpdに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。
Directory Traversal 検知	ホームページの表示もしくはダウンロードページのURLを使用せず、Webサーバ上のhomeディレクトリ外の任意のディレクトリ上のファイル(/etc/passwdファイルなど)を参照またはダウンロードすることが出来る。内部情報については、システム情報を含む/etc/pass/shadow、/etc/hosts/hostsなどの主要ファイルをダウンロードすることが可能であり、システム侵入や内部データ漏洩などの二次的な攻 撃に悪用される可能性がある。
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。
ThinkPHP lang Remote Code Execution	ThinThinkPHP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。
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。
Application Vulnerability(PHPUnit)	PHPUnitはユニットテストフレームワークで/phpunit/src/Util/PHP/eval-stdin.phpファイルに存在す る脆弱性を利用してリモートで任意のコードが実行できる。攻撃者は?<phpの文字列から始まるHTTP POSTデータで任意のPHPコードが実行できる。
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。
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。 .
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年06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14件である。06月1か月間CheckPoint(CVE-2024-24919), PHP(CVE-2024-4577)脆弱性DarkGate, Goldoon Malware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、452
全体配布量

14
今月配布量

10
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.8.06478 malware, cnc, darkgate, A Network Trojan was detected"; flow:to_server,established; urilen:9; content:"/jvtobaqj"; fast_pattern; http_uri; sid:806478;)	DarkGateの変種Malwareのネットワーク通信を検知するポリシー	malware, cnc, darkgate
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06482 server-oracle, oracle, weblogic, cve-2020-14825, Web Application Attack"; flow:to_server,established; content:"/clients/MyCRL"; fast_pattern:only; http_uri; content:"CSHELL"; http_client_body; pcre:"/CSHELL(?i)(¥x2f|%(25)?2f)[^¥r¥n]*?(¥x2e|%(25)?2e){2}([¥x2f¥x5c]|%(25)?(2f|5c))/P"; sid:1006482;)	Check Point CloudGuardの脆弱性であえるCVE-2024-24919を悪用したDirectory Traversal攻撃を検知するポリシー	server-oracle, oracle, weblogic, cve-2020-14825
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.8.06486 malware, trojan, goldoon, A Network Trojan was detected"; flow:to_server,established; content:"/bins/"; depth:6; http_uri; content:"User-Agent: FBI-Agent (Checking You)|0D 0A|"; fast_pattern:only; http_header; sid:806486;)	Goldoonの変種Malwareのネットワーク通信を検知するポリシー	malware, trojan, goldoon
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06487 server-webapp, php, php-cgi, cve-2024-4577, Attempted User Privilege Gain"; flow:to_server,established; content:"|AD|d"; http_uri; content:"allow_url_include"; fast_pattern:only; http_uri; content:"php:/"; http_uri; sid:206487;)	PHP CGIの脆弱性であるCVE-2024-4577を悪用した Command Injection攻撃を検知するポリシー	server-webapp, php, php-cgi, cve-2024-4577