SECURITY REPORT

2024

OCT

2024年10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09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。

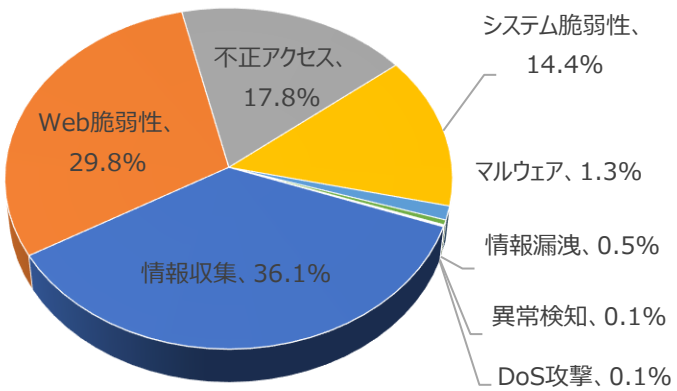
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	36.1%	▲1
Web脆弱性(Web Vulnerability)	29.8%	▼1
不正アクセス(Unauthorized access)	17.8%	▲1
システム脆弱性(System Vulnerability)	14.4%	▼1
マルウェア(Malware)	1.3%	▲2
情報漏洩(Information Exposure)	0.5%	-
異常検知(Anomaly Detection)	0.1%	▼2
DoS攻撃(Denial of service attack)	0.1%	-

2024年09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0.5倍ぐらい増加減少した。

そのうち、Web脆弱性に関する攻撃は先月比べて約5,212件ほど減少し、これはApache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)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増加し、これはWeb Vulnerability Scanner(Zgrab), network scanなどの攻撃件数の増加によるものだと確認できた。

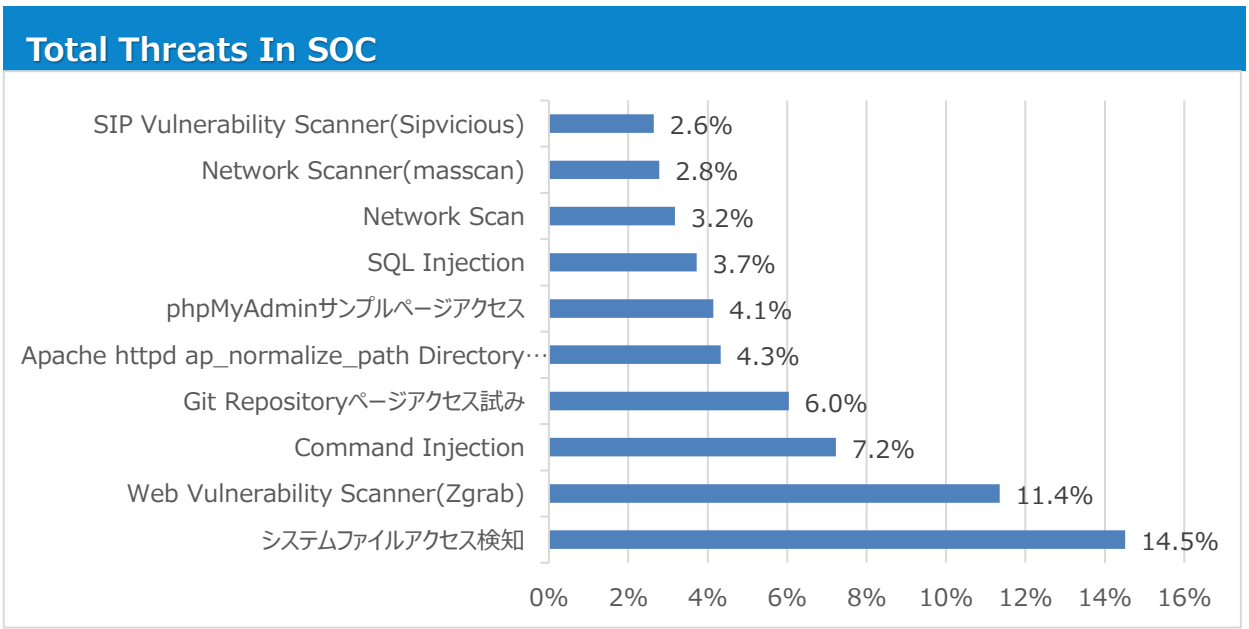


月次攻撃サービスの統計及び分析 - 2024年09月

02. 月次脆弱性攻撃TOP10

2024年09月の月次脆弱性TOP10を確認した結果、 network scan攻撃が新たにTOP10に登場した。
全体的な攻撃件数は減少し、特にウェブスキャン攻撃件数は先月と比べて約5,212件ぐらい減少したことが確認できた。

順位	検知名	比率(%)	比較
1	システムファイルアクセス検知	14.5%	▲4
2	Web Vulnerability Scanner(Zgrab)	11.4%	▲1
3	Command Injection	7.2%	▲1
4	Git Repositoryページアクセス試み	6.0%	▲4
5	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	4.3%	▼3
6	phpMyAdminサンプルページアクセス	4.1%	▲4
7	SQL Injection	3.7%	▲2
8	Network Scan	3.2%	NEW
9	Network Scanner(masscan)	2.8%	NEW
10	SIP Vulnerability Scanner(Sipvicious)	2.6%	NEW



月次攻撃サービスの統計及び分析 - 2024年09月

03. 月次ブラックリストIPアドレスTOP 10

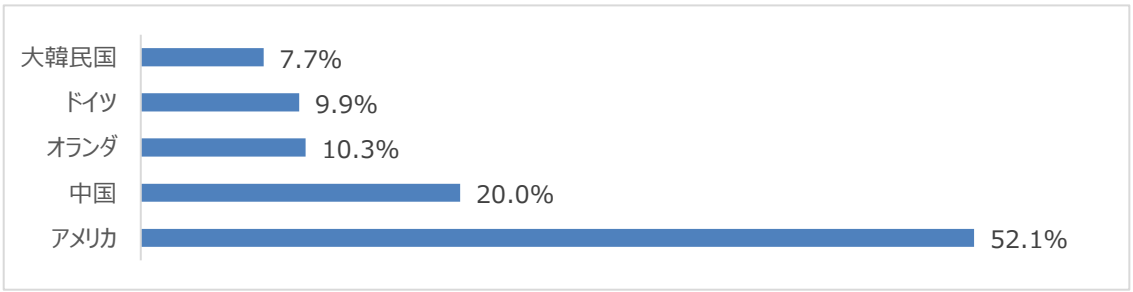
2024年09月についてTOP10を確認した結果、オランダ、ロシアの攻撃比率が増加し、特にアメリカの攻撃比率が52%を超えていることが確認できた。

※ 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	179.43.190.218	CH	TP-Link Router Remote Code Execution(CVE-2023-1389)
4	83.97.73.245	RU	Stealth Commanding
5	92.118.39.120	US	ThinkPHP lang Remote Code Execution
6	80.94.92.60	RO	PUT method Detection
7	106.75.137.241	CN	Git Repositoryページアクセス試み
8	45.88.90.89	KZ	システムファイルアクセス
9	185.243.5.55	HK	SIP Vulnerability Scanner(Sipvicious)
10	5.181.190.250	PL	TP-Link Router Remote Code Execution(CVE-2023-1389)

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	78.153.140.177	GB	6	80.94.92.60	RO
2	78.153.140.179	GB	7	106.75.137.241	CN
3	179.43.190.218	CH	8	45.88.90.89	KZ
4	83.97.73.245	RU	9	185.243.5.55	HK
5	92.118.39.120	US	10	5.181.190.250	PL

攻撃パターン毎の詳細分析結果

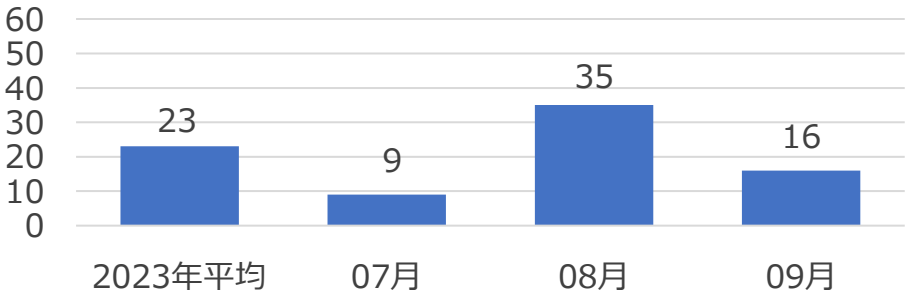
09月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
Git Repository ページアクセス試み	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、存在するソース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。
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。
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。
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。
Network Scan	ネットワーク脆弱性スキャン攻撃は送信先の多数のシステムに対してシステムそのもののバグ、構成上の問題点などハッキング可能なシステムのセキュリティ脆弱性を調べるための攻撃で、一番頻繁に行 われる攻撃である。
Network Scanner(masscan)	ネットワーク帯域スキャン攻撃ができるmasscanである。NMAPと似たようだがカスタムしたTCP/IP Stackを使用して速度的に効率的である。
SIP Vulnerability Scanner(Sipvicious)	SIPViciousはSIP(インターネット電話プロトコル)基盤のVoIP監査ツールであるが、攻撃者によって悪用されている。インターネットに繋がっているVoIP, PBX(電話交換システム)を探した後、Brute Force攻撃でアカウント奪取及び国際電話番号やプレミアム電話番号に電話をかけて課金を誘導する。主にUser-Agent methodにFriendly-ScannerやSIPViciousの文字列が使用されて、攻撃対象がVoIP, PBXシステムではない場合、攻撃に対する有効性はない。.

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年08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35件である。09月1か月間WordPressプラグイン(CVE-2024-5084)、Progress WhatsUp Gold(CVE-2024-5084)脆弱性とalogin、ValleyRATマルウェア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、512
全体配布量

16
今月配布量

35
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 $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.06540 malware-backdoor,Backdoor,agent, A Network Trojan was detected"; flow:to_client,established; flowbits:isset,file.elf; file_data; content:"|61 6C 6F 67 69 6E 3A 00 25 73 00 00 2F 62 69 6E 2F 73 68 00 2F 74 6D 70 2F 6C 6F 67 69 6E 00 00 41 73 75 73 50 61 73 73 31 32 33 00|"; sid:806540;)	alogin(63256)ボットネットのネットワーク通信を検知するポリシー	malware-backdoor,Backdoor,agent
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06541 server-webapp,wordpress,HashForm,cve-2024-5084, Web Application Attack"; flow:to_server,established; content:"/wp-admin/admin-ajax.php"; nocase; http_uri; content:"action=hashform_file_upload_action"; fast_pattern:only; http_uri; content:"Content-Disposition"; nocase; http_client_body; content:"qqfile"; nocase; http_client_body; content:"filename"; nocase; http_client_body; pcre:"/filename¥s*=¥s*[^¥r¥n]*?¥x2e(p(hp¥d?||html)|exe|ini|perl|cgi)/Pi"; sid:1006541;)	WordPress Hash Formぷr画院の脆弱性であるCVE-2024-5084を悪用したファイルアップロード試みを検知するポリシー	server-webapp,wordpress,HashForm,cve-2024-5084
alert tcp $HOME_NET any -> $EXTERNAL_NET [1024:] (msg:"IGRSS.8.06548 malware-cnc,trojan,valleyrat, A Network Trojan was detected"; flow:to_server,established; content:"GetRuntimeBroker"; fast_pattern:only; isdataat:!24; pcre:"/^GetRuntimeBroker(Size)?_¥d{2}¥x00$/"; sid:806548;)	ValleyRAT Malwareのネットワーク通信を検知するポリシー	malware-cnc,trojan,valleyrat
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06549 server-webapp,progress,whatsup,cve-2024-6670, Web Application Attack"; flow:to_server,established; content:"/NmConsole/Platform/PerformanceMonitorErrors/HasErrors"; fast_pattern:only; http_uri; content:"|22|classId|22|"; nocase; http_client_body; pcre:"/¥x22classId¥x22¥s*¥x3a¥s*¥x22((?!(?<!¥x5c)¥x22).)*?([¥x27¥x3b¥x23]|¥x2f¥x2a|¥x2d¥x2d)/Pi"; sid:1006549;)	Progress WhatsUp Goldの脆弱性であるCVE-2024-6670を悪用したSQL Injection試みを検知するポリシー	server-webapp,progress,whatsup,cve-2024-6670