SECURITY REPORT

2024

APR

2024年04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04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。

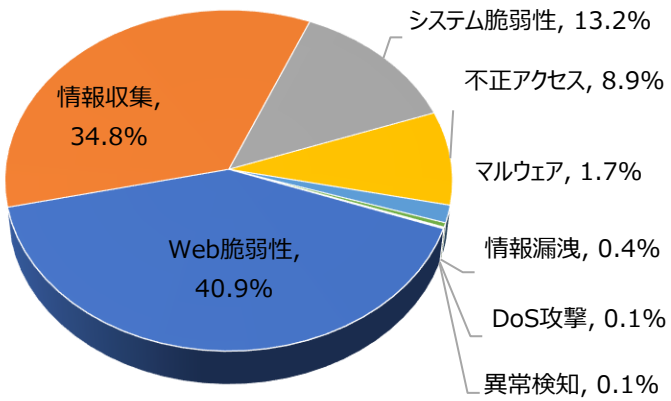
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	40.9%	-
情報収集(Information Gathering)	34.8%	-
システム脆弱性(System Vulnerability)	13.2%	-
不正アクセス(Unauthorized access)	8.9%	-
マルウェア(Malware)	1.7%	-
情報漏洩(Information Exposure)	0.4%	-
DoS攻撃(Denial of service attack)	0.1%	-
異常検知(Anomaly Detection)	0.1%	-

2024年04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0.8倍ぐらい減少した。

そのうち、Web脆弱性に関する攻撃は先月比べて約1,100件ほど減少し、これはSQL 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1,500件ぐらい減少し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数減少によるものだと確認できた。

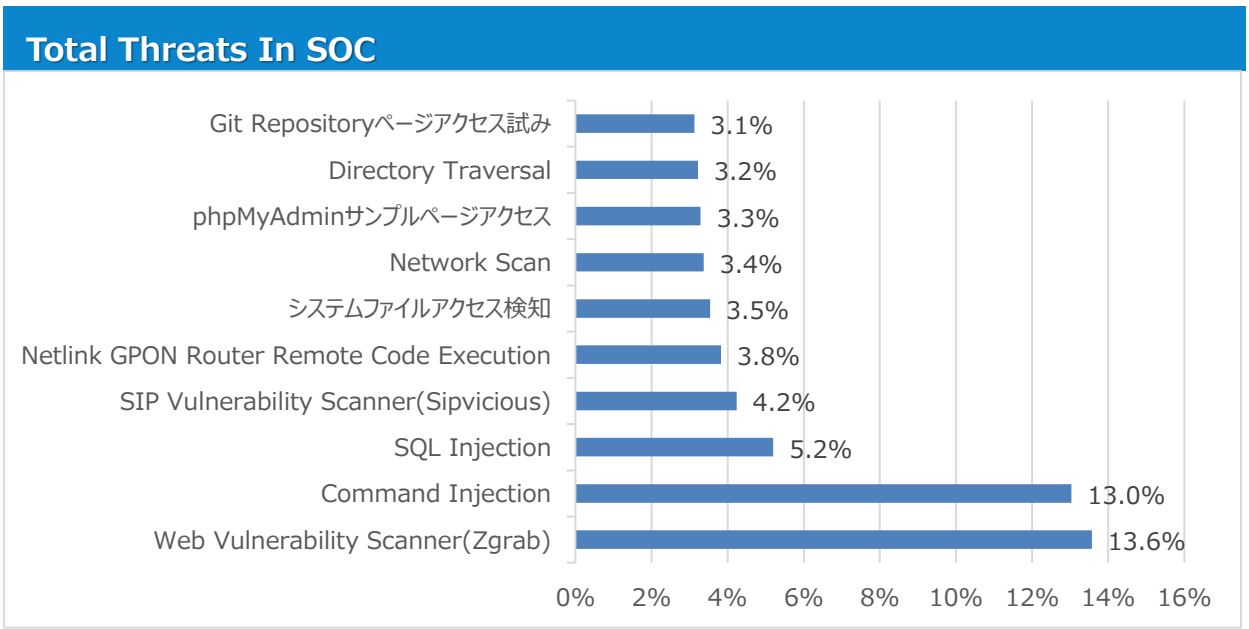


月次攻撃サービスの統計及び分析 - 2024年04月

02. 月次脆弱性攻撃TOP10

2024年04月の月次脆弱性TOP10を確認した結果、SQL Injection、システムファイルアクセス検知、Network Scan、Directory Traversal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Web Vulnerability Scanner(Zgrab)攻撃件数は先月と比べて約550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	Web Vulnerability Scanner(Zgrab)	13.6%	▲2
2	Command Injection	13.0%	▲2
3	SQL Injection	5.2%	NEW
4	SIP Vulnerability Scanner(Sipvicious)	4.2%	▲1
5	Netlink GPON Router Remote Code Execution	3.8%	▲1
6	システムファイルアクセス検知	3.5%	NEW
7	Network Scan	3.4%	NEW
8	phpMyAdminサンプルページアクセス	3.3%	▼7
9	Directory Traversal	3.2%	NEW
10	Git Repositoryページアクセス試み	3.1%	▼2



月次攻撃サービスの統計及び分析 - 2024年04月

03. 月次ブラックリストIPアドレスTOP 10

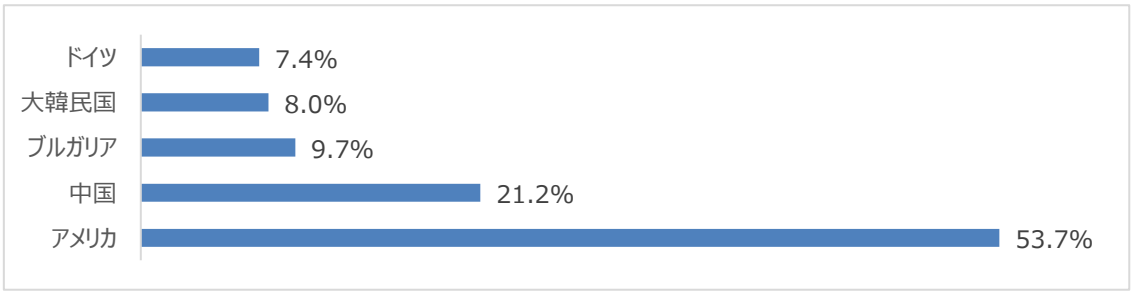
2024年04月についてTOP10を確認した結果、アメリカと中国とブルガリア、ドイツの攻撃比率が増加し、一方大韓民国の攻撃の比率は減少した。特にアメリカの攻撃比率が50%を超えていることが確認できた。

※ 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	80.94.92.60	GB	TP-Link Router Remote Code Execution(CVE-2023-1389)
2	49.142.107.130	KR	ThinkPHP Remote Code Execution Vulnerability
3	87.121.69.52	NL	Method(Connect)
4	212.70.149.134	BG	Network Scanner(masscan)
5	63.251.106.21	US	SIP Vulnerability Scanner(Sipvicious)
6	83.97.73.245	RU	etcpasswd Detect
7	137.220.197.141	JP	Apache Struts2 Jakarta RCE (CVE-2017-5638)
8	91.92.252.130	NL	Command Injection
9	69.164.217.74	US	Web Vulnerability Scanner(Zgrab)
10	192.155.88.231	US	Web Vulnerability Scanner(Zgrab)

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	80.94.92.60	GB	6	83.97.73.245	RU
2	49.142.107.130	KR	7	137.220.197.141	JP
3	87.121.69.52	NL	8	91.92.252.130	NL
4	212.70.149.134	BG	9	69.164.217.74	US
5	63.251.106.21	US	10	192.155.88.231	US

攻撃パターン毎の詳細分析結果

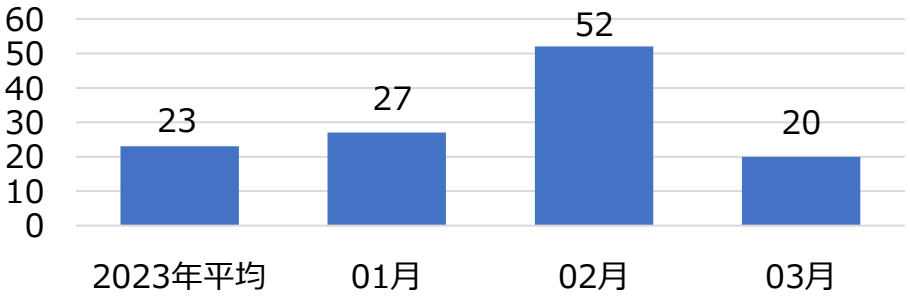
04月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
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。.
Netlink GPON Router Remote Code Execution	NetlinkGPONルータで発見された脆弱性として、ターゲットアドレスの後に /boaform/admin/formPing文字列を入力して認証手順を通過する可能性がある。この脆弱 性を悪用し、認証されていない攻撃者が端末からリモートでコマンドを実行、悪意のあるファイルをアッ プロードするなどが可能になる。
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。
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。
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。
Directory Traversal	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。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年03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20件である。
03月1か月の間、MS Outlook(CVE-2024-21413), Ivanti(CVE-2024-21893), JetBrains(CVE-2024-27198), Jenkins(CVE-2024-23897)などに対する検知ポリシーが配布された。



3か月間件数

6,411
全体配布量

20
今月配布量

52
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 -> $SMTP_SERVERS [25,587] (msg:"IGRSS.2.06395 FILE-OFFICE, MS, Outlook, CVE-2024-21413, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"href"; nocase; content:"file|3A|///|5C 5C|"; within:100; nocase; content:"|21|"; distance:0; pcre:"/<a[^>]*?href¥s*=¥s*[¥x22¥x27]file¥x3a¥x2f¥x2f¥x2f¥x5c¥x5c[^¥x22¥x27]*?¥x21/i"; sid:206395;)	Microsoft OutlookのCVE-2024-21413脆弱性を悪用したリモートコード実行攻撃を検知するポリシー	FILE-OFFICE, MS, Outlook, CVE-2024-21413
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06432 SERVER-WEBAPP, Ivanti, CVE-2024-21893, Web Application Attack"; flow:to_server,established; content:"SAMLResponse="; nocase; http_uri; base64_decode:bytes 1000,relative; base64_data; content:"RetrievalMethod"; nocase; content:"URI"; nocase; pcre:"/RetrievalMethod[^>]*?¥sURI¥s*=/i"; content:"/dana-ws/saml"; fast_pattern:only; http_uri; sid:1006432;)	Ivanti製品から発見された脆弱性である CVE-2024-21893を悪用したSSRF試みを検知するポリシー	SERVER-WEBAPP, Ivanti, CVE-2024-21893
alert tcp $EXTERNAL_NET any -> $HOME_NET [$HTTP_PORTS,8111] (msg:"IGRSS.10.06433 SERVER-WEBAPP, JetBrains, CVE-2024-27198, Web Application Attack"; flow:to_server,established; content:"jsp=/app/rest/"; fast_pattern:only; pcre:"/[?&]jsp=¥x2fapp¥x2frest¥x2f[^&¥r¥n]*?¥x2ejsp¥s+HTTP¥x2f/i"; sid:1006433;)	JetBrains TeamCityの脆弱性であるCVE-2024-27198を悪用した認証バイパス攻撃を検知するポリシー	SERVER-WEBAPP, JetBrains, CVE-2024-27198
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.06440 SERVER-WEBAPP, Jenkins, CLI, CVE-2024-23897, Web Application Attack"; flow:to_server,established; content:"/cli?"; http_uri; content:"remoting=false"; fast_pattern:only; nocase; http_uri; content:"Side: upload"; nocase; http_header; content:"|00 00 00|"; http_client_body; content:"|00 00|"; within:2; distance:1; http_client_body; content:"@"; within:1; distance:1; http_client_body; sid:1006440;)	Jenkins CLIの脆弱性であるCVE-2024-23897を悪用した任意ファイル読み取り試みを検知するポリシー	SERVER-WEBAPP, Jenkins, CLI, CVE-2024-23897