SECURITY REPORT

2024

MAR

2024年03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03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。

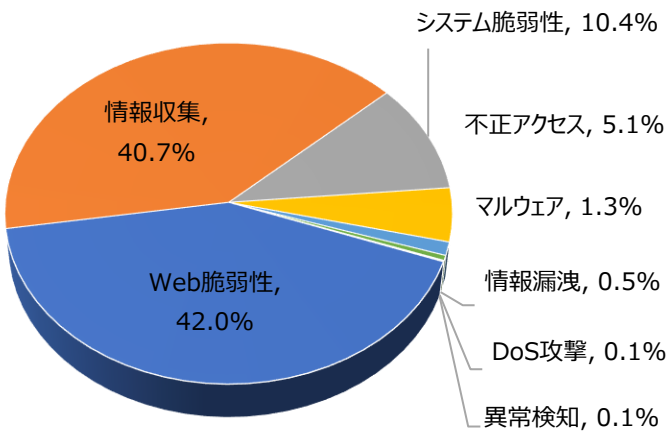
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	42.0%	-
情報収集(Information Gathering)	40.7%	-
システム脆弱性(System Vulnerability)	10.4%	-
不正アクセス(Unauthorized access)	5.1%	-
マルウェア(Malware)	1.3%	-
情報漏洩(Information Exposure)	0.5%	-
DoS攻撃(Denial of service attack)	0.1%	-
異常検知(Anomaly Detection)	0.1%	-

2024年03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1,600件ほど減少し、これはphpMyAdminサンプルページアクセス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300件ぐらい増加し、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。



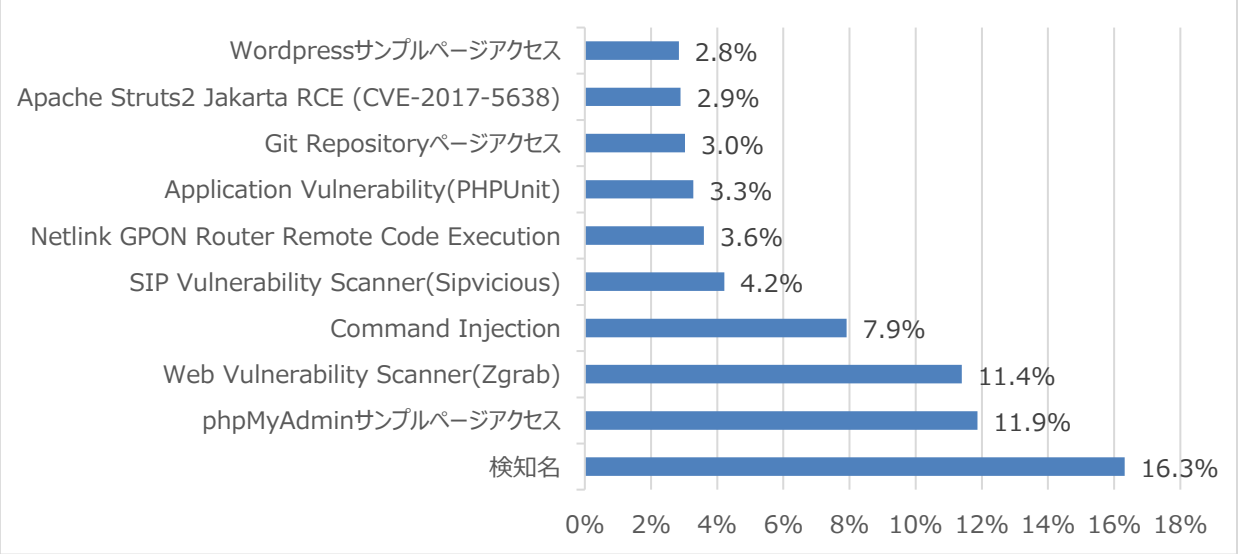
月次攻撃サービスの統計及び分析 - 2024年03月

02. 月次脆弱性攻撃TOP10

2024年03月の月次脆弱性TOP10を確認した結果、Application Vulnerability(PHPUnit)、Apache Struts2 Jakarta RCE (CVE-2017-5638)、Wordpressサンプルページアクセス攻撃が新たにTOP10に登場した。全体的な攻撃件数は減少し、特にphpMyAdminサンプルページアクセス攻撃件数は先月と比べて約1,400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	phpMyAdminサンプルページアクセス	16.3%	▲2
2	Zyxel Router zhttpd RCE_A	11.9%	▼1
3	Web Vulnerability Scanner(Zgrab)	11.4%	▼1
4	Command Injection	7.9%	▲2
5	SIP Vulnerability Scanner(Sipvicious)	4.2%	▲2
6	Netlink GPON Router Remote Code Execution	3.6%	▲2
7	Application Vulnerability(PHPUnit)	3.3%	NEW
8	Git Repositoryページアクセス	3.0%	▲1
9	Apache Struts2 Jakarta RCE (CVE-2017-5638)	2.9%	NEW
10	Wordpressサンプルページアクセス	2.8%	NEW

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2024年03月

03. 月次ブラックリストIPアドレスTOP 10

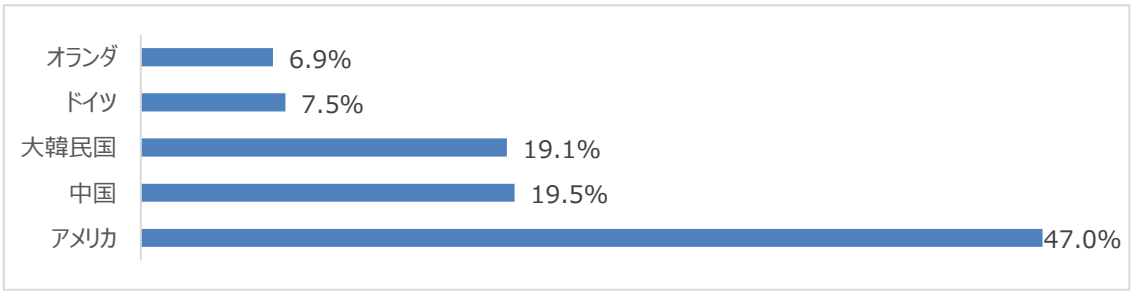
2024年03月についてTOP10を確認した結果、中国とドイツの攻撃比率が増加し、一方アメリカと大韓民国、オランダの攻撃の比率は減少した。特にアメリカの攻撃比率が約50%に近いことが確認できた。

※ 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	185.224.128.10	NL	Command Injection
2	63.251.106.21	US	SIP Vulnerability Scanner(Sipvicious)
3	83.97.73.245	RU	Synacor Zimbra Collaboration Suite autodiscover XXE (CVE-2019-9670)
4	45.155.91.46	PL	SIP Vulnerability Scanner(Sipvicious)
5	185.224.128.200	NL	Command Injection
6	69.164.217.74	US	Web Vulnerability Scanner(Zgrab)
7	91.92.252.208	NL	Command Injection
8	45.155.91.57	PL	SIP Vulnerability Scanner(Sipvicious)
9	45.33.87.154	US	Web Vulnerability Scanner(Zgrab)
10	69.164.217.245	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
1	185.224.128.10	NL
2	63.251.106.21	US
3	83.97.73.245	RU
4	45.155.91.46	PL
5	185.224.128.200	NL

Rank	Source IP	Country
6	69.164.217.74	US
7	91.92.252.208	NL
8	45.155.91.57	PL
9	45.33.87.154	US
10	69.164.217.245	US

攻撃パターン毎の詳細分析結果

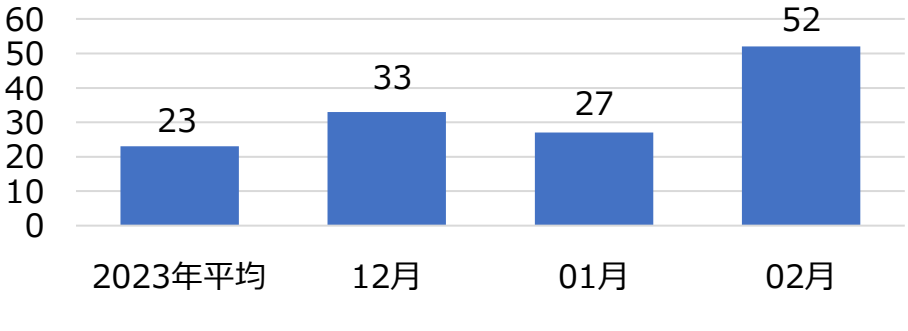
03月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
Zyxel Router zhttpd RCE_A	Zyel RouterにREC(Remote Code Execution)脆弱性が存在する。当該の脆弱性は/bin/zhttpd/パスにユーザーの入力値の不適切な有効性の検証で発生する。リモート攻撃者は悪意的に操作されたリクエストを送信して攻撃できる。攻撃成功時、任意のコードが実行できる。
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。
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。
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。.
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。.
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 Struts2 Jakarta RCE (CVE-2017-5638)	プラグインを利用してファイルアップロードを処理する際、攻撃者はHTTP Requestヘッダーの Content-Type値にOGNL(Object Graph Navigation Language)表現式を利用してリモートコードが実行できる。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年02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52件である。
02月1か月の間、ConnectWise ScreenConnect(CVE-2024-1708、CVE-2024-1709)、Microsoft Outlook(CVE-2023-35636、CVE-2024-21413)などに対する検知ポリシーが配布された。



3か月間件数

月間配布件数

検知ポリシー	説明	タグ
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06428 SERVER-WEBAPP, ConnectWise, ScreenConnect, CVE-2024-1708, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"|22|"; http_client_body; base64_decode:bytes 1000,offset 0,relative; base64_data; content:"PK|03 04|"; byte_extract:2,22,filename_len,relative,little; content:"|2E 2E|"; within:filename_len; distance:2; content:"/Services/ExtensionService.ashx/InstallExtension"; fast_pattern:only; http_uri; sid:106428;)	ConnectWise ScreenConnectの脆弱性であるCVE-2024-1708を悪用したパス巡回攻撃試みを検知するポリシー	SERVER-WEBAPP, ConnectWise, ScreenConnect, CVE-2024-1708
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06427 SERVER-WEBAPP, ConnectWise, ScreenConnect, CVE-2024-27215, Attempted User Privilege Gain"; flow:to_server,established; content:"/SetupWizard.aspx/"; fast_pattern:only; http_uri; sid:206427;)	ConnectWise ScreenConnectの脆弱性であるCVE-2024-1709, CVE-2024-27215を悪用した認証バイパス試みを検知するポリシー	SERVER-WEBAPP, ConnectWise, ScreenConnect, CVE-2024-1709, CVE-2024-27215
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 -> $SMTP_SERVERS 25 (msg:"IGRSS.2.06396 FILE-OFFICE, MS, Outlook, CVE-2023-35636, Attempted User Privilege Gain"; flow:to_server,established; content:"X-Sharing-Config-Url"; fast_pattern:only; content:"|5C 5C|"; content:"Content-Class"; nocase; content:"Sharing"; nocase; pcre:"/X-Sharing-Config-Url¥s*¥x3a¥s*¥x5c¥x5c[^¥r¥n]*?¥x2eics/i"; sid:206396;)	Microsoft OutlookのCVE-2023-35636脆弱性を悪用した資格漏洩試みを検知するポポリシー	FILE-OFFICE, MS, Outlook, CVE-2023-35636