SECURITY REPORT

2024

JAN

2024年01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01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。

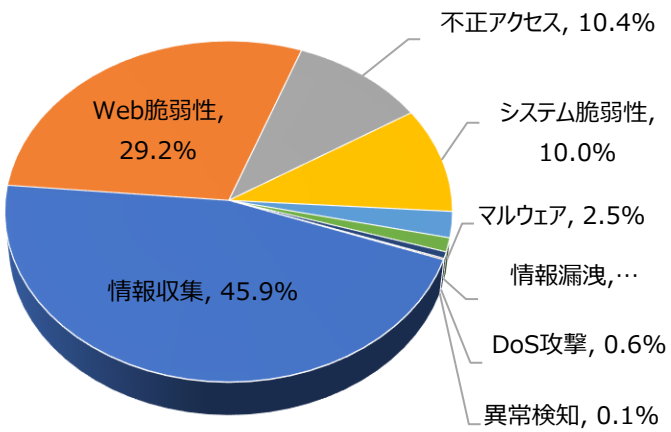
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	45.9%	-
Web脆弱性(Web Vulnerability)	29.2%	-
不正アクセス(Unauthorized access)	10.4%	▲1
システム脆弱性(System Vulnerability)	10.0%	▼1
マルウェア(Malware)	2.5%	-
情報漏洩(Information Exposure)	1.3%	-
DoS攻撃(Denial of service attack)	0.6%	-
異常検知(Anomaly Detection)	0.1%	-

2024年01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0.72倍ぐらい減少した。

そのうち、情報収集に関する攻撃は先月比べて約800件ほど減少し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数の減少によるものだと確認できた。

一方システム脆弱性に関する攻撃は先月と比べて約1,250件ぐらい減少し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃件数減少によるものだと確認できた。

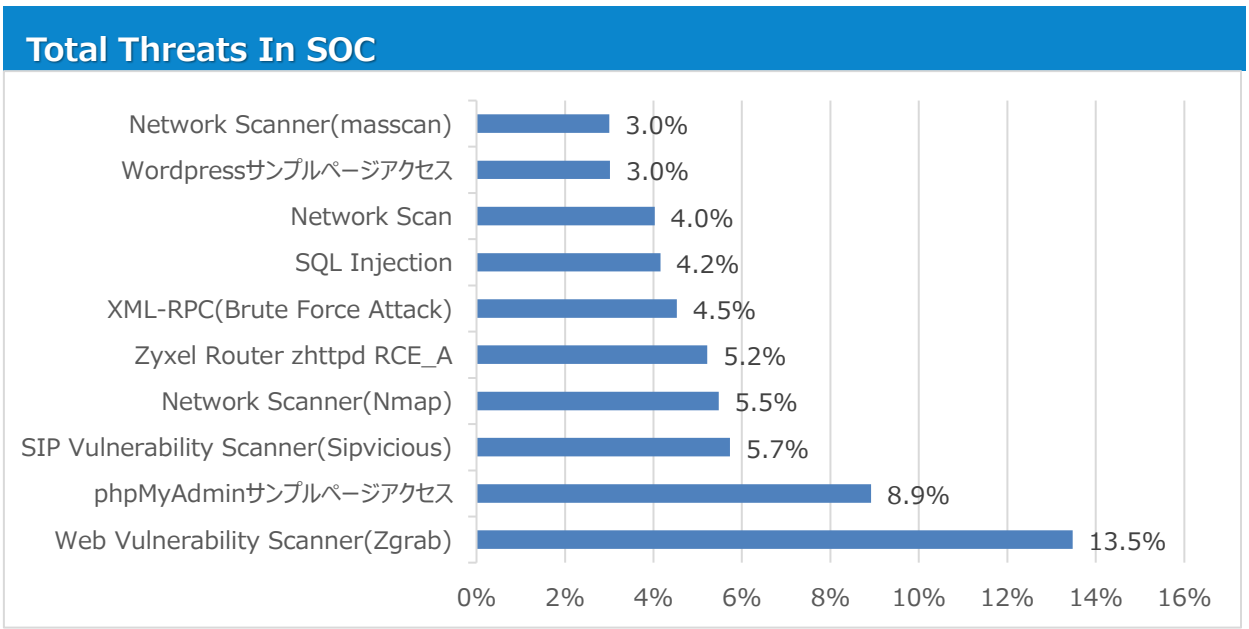


月次攻撃サービスの統計及び分析 - 2024年01月

02. 月次脆弱性攻撃TOP10

2024年01月の月次脆弱性TOP10を確認した結果、Wordpressサンプルページアクセス、Network Scanner(masscan)攻撃が新たにTOP10に登場し、全体的な攻撃件数が減少したことが確認できた。特にWeb Vulnerability Scanner(Zgrab)攻撃件数は先月と比べて約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	Web Vulnerability Scanner(Zgrab)	13.5%	-
2	phpMyAdminサンプルページアクセス	8.9%	▲2
3	SIP Vulnerability Scanner(Sipvicious)	5.7%	▲3
4	Network Scanner(Nmap)	5.5%	▲5
5	Zyxel Router zhttpd RCE_A	5.2%	▲2
6	XML-RPC(Brute Force Attack)	4.5%	▲4
7	SQL Injection	4.2%	▲1
8	Network Scan	4.0%	▼3
9	Wordpressサンプルページアクセス	3.0%	NEW
10	Network Scanner(masscan)	3.0%	NEW



月次攻撃サービスの統計及び分析 - 2024年01月

03. 月次ブラックリストIPアドレスTOP 10

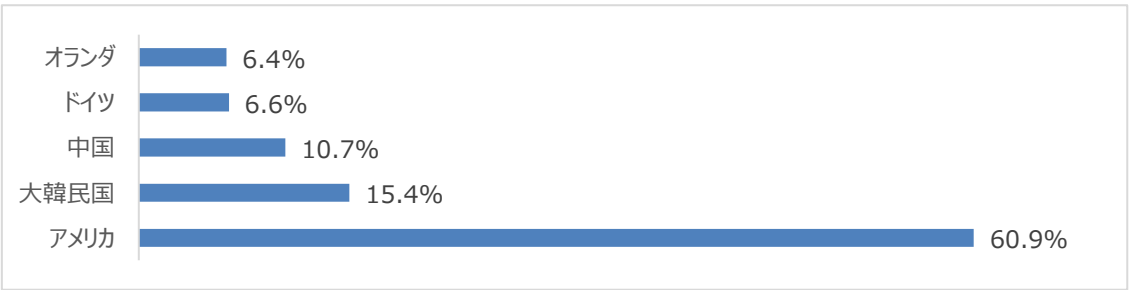
2024年01月についてTOP10を確認した結果、アメリカ、中国、オランダの攻撃比率が増加し、一方大韓民国とドイツの攻撃の比率は減少した。特にアメリカの攻撃比率が約60%を超えていることが確認できた。

※ 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	187.33.53.204	BR	SIP Vulnerability Scanner(Sipvicious)
2	185.22.153.154	RU	Cross Site Script(XSS)
3	8.212.169.72	PH	ThinkPHP Remote Code Execution Vulnerability
4	72.251.232.180	US	SIP Vulnerability Scanner(Sipvicious)
5	45.155.91.237	PL	SIP Vulnerability Scanner(Sipvicious)
6	83.97.73.87	RU	XML External ENTITY Injection
7	84.54.51.29	NL	Web-CGI Vulnerability
8	91.92.241.50	NL	Command Injection
9	96.44.143.190	US	SIP Vulnerability Scanner(Sipvicious)
10	96.44.142.10	US	SIP Vulnerability Scanner(Sipvicious)

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	187.33.53.204	BR	6	83.97.73.87	RU
2	185.22.153.154	RU	7	84.54.51.29	NL
3	8.212.169.72	PH	8	91.92.241.50	NL
4	72.251.232.180	US	9	96.44.143.190	US
5	45.155.91.237	PL	10	96.44.142.10	US

攻撃パターン毎の詳細分析結果

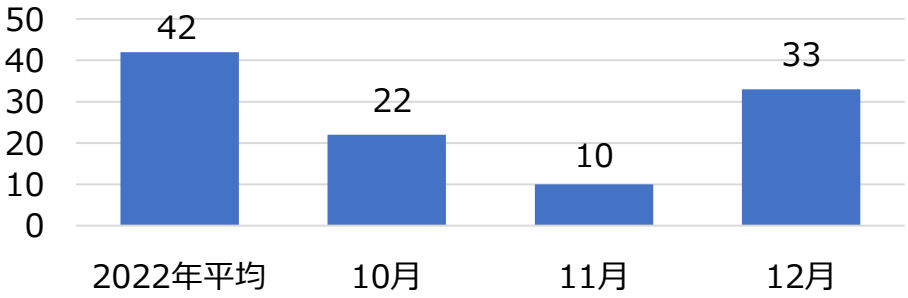
01月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。.
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。
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。
XML-RPC(Brute Force Attack)	XML-RPC(Brute Force Attack)はリモートブログページXML-RPCを利用して総当たり攻撃のログイン代入剛撃ができる。攻撃者は¥"system.multicall¥"メソッドを呼び出し、一つの要請パケットに数百のID/PWを挿入し攻撃を試みる。
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。
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(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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2023年12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33件である。
11月1か月の間、Juniper Junos(CVE-2023-36845)、ownCloud(CVE-2023-49103)、Apache Struts(CVE-2023-50164)、Atlassian Confluence(CVE-2023-22518)などに対する検知ポリシーが配布された。



3か月間件数

6,312
全体配布量

33
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 $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06323 SERVER-WEBAPP, Juniper, Junos, CVE-2023-36845, Web Application Attack"; flow:to_server,established; content:"PHPRC=/dev/fd/0"; fast_pattern:only; http_uri; content:"auto_prepend_file="; http_client_body; sid:1006323;)	Juniper Junosの脆弱性であるCVE-2023-36845を悪用した情報漏洩試みを検知するポリシー	SERVER-WEBAPP, Juniper, Junos, CVE-2023-36845
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06327 SERVER-WEBAPP, ownCloud, CVE-2023-49103, Web Application Attack"; flow:to_server,established; content:"/apps/graphapi/vendor/microsoft/microsoft-graph/tests/GetPhpInfo.php"; fast_pattern:only; http_uri; sid:1006327;)	ownCloudの脆弱性であるCVE-2023-49103を悪用したGraph API情報公開試みを検知するポリシー	SERVER-WEBAPP, ownCloud, CVE-2023-49103
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06345 SERVER-WEBAPP, Apache, Struts, CVE-2023-50164, Web Application Attack"; flow:to_server,established; content:"/upload.action"; fast_pattern:only; http_uri; content:"uploadFileName"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?uploadFileName((?!^--).)*?¥x2e¥x2e[¥x2f¥x5c]/Psim"; sid:1006345;)	Apache Strutsの脆弱性であるCVE-2023-50164を悪用したでれぃくとりトラバーサル攻撃を検知するポリシー	SERVER-WEBAPP, Apache, Struts, CVE-2023-50164
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06349 SERVER-WEBAPP, Atlassian, Confluence, CVE-2023-22518, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/json/setup-restore"; fast_pattern; nocase; http_uri; content:".action"; distance:0; nocase; http_uri; sid:106349;)	Atlassian Confluenceの脆弱性であるCVE-2023-22518を悪用した認証バイパス試みを検知するポリシー	SERVER-WEBAPP, Atlassian, Confluence, CVE-2023-22518