SECURITY REPORT

2024

FEB

2024年02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02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。

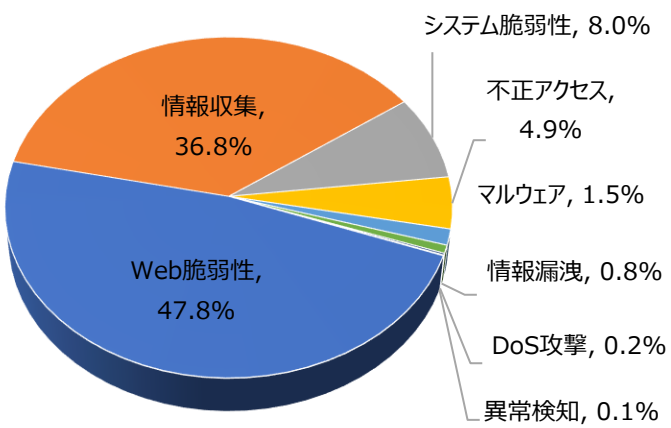
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	47.8%	▲1
情報収集(Information Gathering)	36.8%	▼1
システム脆弱性(System Vulnerability)	8.0%	▲1
不正アクセス(Unauthorized access)	4.9%	▼1
マルウェア(Malware)	1.5%	-
情報漏洩(Information Exposure)	0.8%	-
DoS攻撃(Denial of service attack)	0.2%	-
異常検知(Anomaly Detection)	0.1%	-

2024年02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2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4,300件ほど増加し、これはZyxel Router zhttpd RCE_A攻撃件数の増加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1,700件ぐらい増加し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数増加によるものだと確認できた。

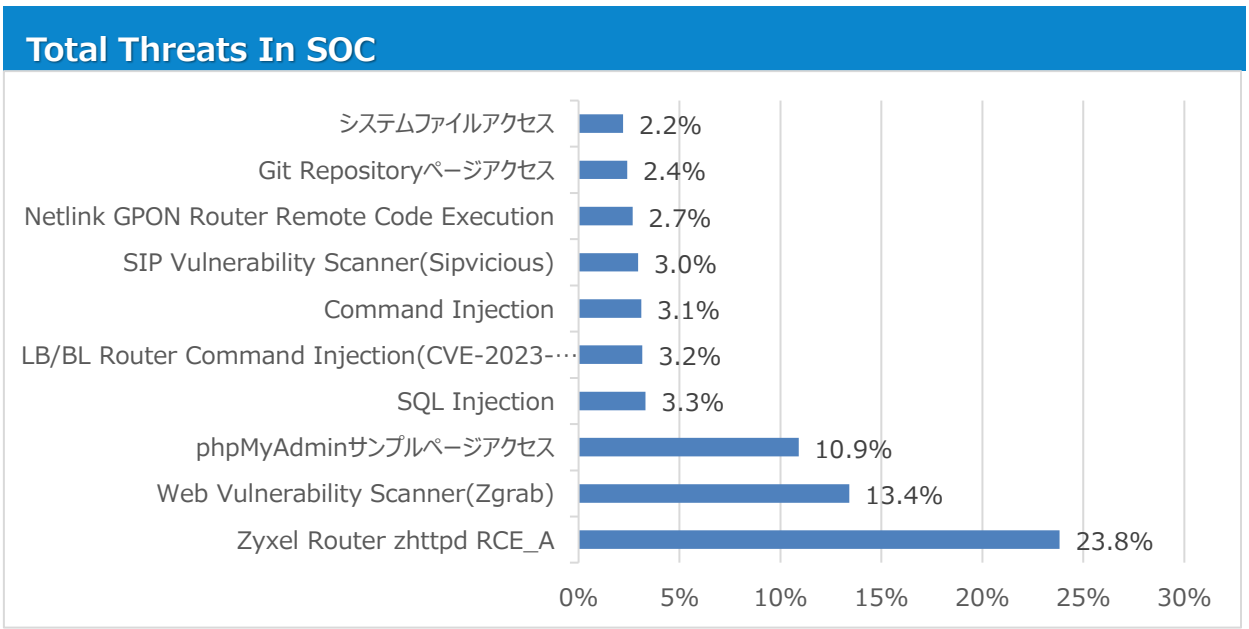


月次攻撃サービスの統計及び分析 - 2024年02月

02. 月次脆弱性攻撃TOP10

2024年02月の月次脆弱性TOP10を確認した結果、 LB/BL Router Command Injection(CVE-2023-26801)、Command Injection、Netlink GPON Router Remote Code Execution、Git Repository ページアクセス 攻撃が新たにTOP10に登場した。

順位	検知名	比率(%)	比較
1	Zyxel Router zhttpd RCE_A	23.8%	▲4
2	Web Vulnerability Scanner(Zgrab)	13.4%	▼1
3	phpMyAdminサンプルページアクセス	10.9%	▼1
4	SQL Injection	3.3%	▲3
5	LB/BL Router Command Injection(CVE-2023-26801)	3.2%	NEW
6	Command Injection	3.1%	NEW
7	SIP Vulnerability Scanner(Sipvicious)	3.0%	▼4
8	Netlink GPON Router Remote Code Execution	2.7%	NEW
9	Git Repositoryページアクセス	2.4%	NEW
10	システムファイルアクセス	2.2%	NEW



月次攻撃サービスの統計及び分析 - 2024年02月

03. 月次ブラックリストIPアドレスTOP 10

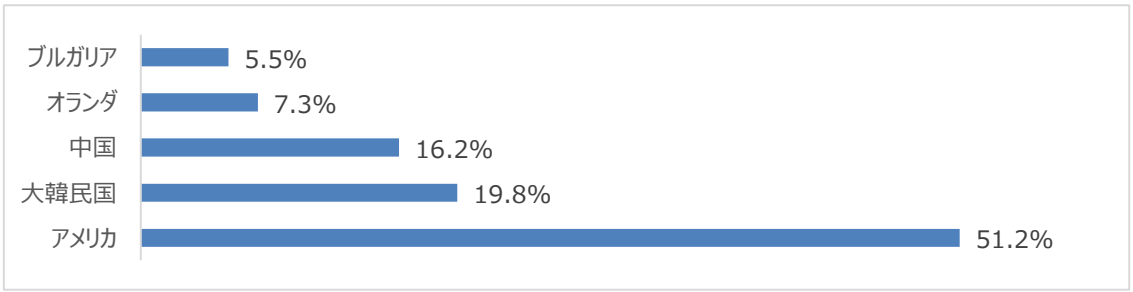
2024年02月についてTOP10を確認した結果、大韓民国、中国、オランダ、ブルガリアの攻撃比率が増加し、一方アメリカのの攻撃の比率は減少した。特にアメリカの攻撃比率が約50%を超えていることが確認できた。

※ 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	83.97.73.245	RU	Synacor Zimbra Collaboration Suite autodiscover XXE(CVE-2019-9670)
2	45.155.91.160	PL	SIP Vulnerability Scanner(Sipvicious)
3	187.33.53.204	BR	SIP Vulnerability Scanner(Sipvicious)
4	45.155.91.75	HK	SIP Vulnerability Scanner(Sipvicious)
5	193.35.18.39	NL	Apache Struts2 Jakarta RCE (CVE-2017-5638)
6	45.155.91.104	PL	SIP Vulnerability Scanner(Sipvicious)
7	45.33.87.154	US	Web Vulnerability Scanner(Zgrab)
8	89.248.168.37	NL	Network Scanner(masscan)
9	69.164.217.74	US	Web Vulnerability Scanner(Zgrab)
10	94.156.67.16	NL	Web Scanner(muieblackcat)

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	83.97.73.245	RU	6	45.155.91.104	PL
2	45.155.91.160	PL	7	45.33.87.154	US
3	187.33.53.204	BR	8	89.248.168.37	NL
4	45.155.91.75	HK	9	69.164.217.74	US
5	193.35.18.39	NL	10	94.156.67.16	NL

攻撃パターン毎の詳細分析結果

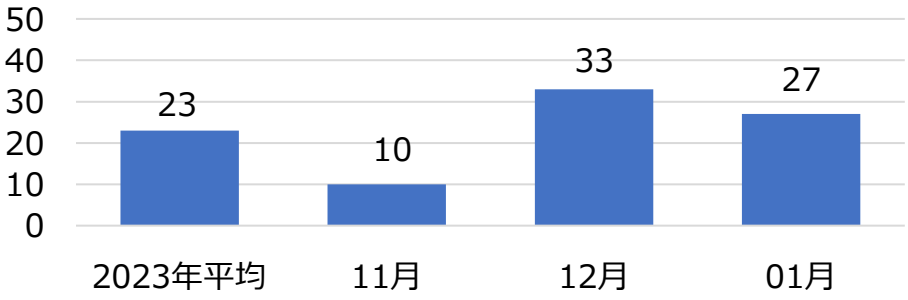
02月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
LB/BL Router Command Injection(CVE-2023-26801)	LB-LINK BL-AC1900_2.0 V1.0.1, BL-WR9000 V2.4.9, BL-X26 V1.2.5 and BL-LTE300 V1.0.8 Wireless RoutersはCommand injection脆弱性が含まれていることが確認できた。この脆弱性はmacパラメータのチェック不備によって発生する。この脆弱性を悪用して権限がない攻撃者が/goform/set_LimitClient_cfgをリクエスト時、リモートで任意のコマンドを実行して送ることができる。
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。.
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。
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。
システムファイル アクセス検	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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年01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27件である。
01月1か月の間、Ivanti(CVE-2024-21887、CVE-2023-46805)、Adobe ColdFusion(CVE-2023-38204)、Atlassain Confluence(CVE-2023-22527)などに対する検知ポリシーが配布された。



3か月間件数

6,339
全体配布量

27
今月配布量

33
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.1.06362 SERBER-WEBAPP, Ivanti, Connect Secure, CVE-2024-21887, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/api/v1/license/keys-status"; fast_pattern:only; http_uri; pcre:"/keys-status¥x2f[^¥x2f¥x3f]*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24])/Ui"; sid:106362;)	Ivanti Connect Secureの脆弱性であるCVE-2024-21887を悪用したコマンド挿入試みを検知するポリシー	SERBER-WEBAPP, Ivanti, Connect Secure, CVE-2024-21887
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.1.06364 SERBER-WEBAPP, Ivanti, Connect Secure, CVE-2023-46805, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/api/v1/totp/user-backup-code"; fast_pattern:only; content:"/api/v1/totp/user-backup-code"; nocase; http_raw_uri; pcre:"/user-backup-code¥x2f+[^¥x3f]*?(¥x2e|%(25)?2e){2}([¥x2f¥x5c]|%(25)?(2f|5c))/Ii"; sid:106364;)	Ivanti Connect Secureの脆弱性であるCVE-2023-46805を悪用した認証バイパス試みを検知するポリシー	SERBER-WEBAPP, Ivanti, Connect Secure, CVE-2023-46805
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06372 SERVER-WEBAPP, Adobe, ColdFusion, CVE-2023-38204, Attempted User Privilege Gain"; flow:to_server,established; content:"/CFIDE/"; fast_pattern:only; http_uri; content:".cf"; nocase; http_uri; content:"Content-Disposition"; nocase; http_client_body; content:"argumentCollection"; nocase; http_client_body; content:"<wddxPacket"; nocase; http_client_body; content:"<struct"; nocase; http_client_body; content:"type"; nocase; http_client_body; isdataat:52,relative; content:!"coldfusion"; within:50; distance:2; nocase; http_client_body; pcre:"/¥x2fCFIDE¥x2f[^¥x3f]*?¥x2ecf[cm]/Ui"; sid:206372;)	Adobe ColdFusionの脆弱性であるCVE-2023-28203を悪用した客直列化攻撃試みを検知するポリシー	SERVER-WEBAPP, Adobe, ColdFusion, CVE-2023-38204
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.10.06374 SERVER-WEBAPP, Atlassian, Confluence, CVE-2023-22527, Web Application Attack"; flow:to_server,established; content:"/template/aui/text-inline.vm"; fast_pattern:only; http_uri; content:"label="; nocase; http_uri; pcre:"/[?&]label=[^&]*?(¥x5cu0027|ognl)/Ui"; sid:1006374;)	Atlassain Confluenceの脆弱性であるCVE-2023-22527を悪用したテンプレート挿入試みを検知するポリシー	SERVER-WEBAPP, Atlassian, Confluence, CVE-2023-22527