SECURITY REPORT

2023

JAN

2023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 - 2023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。

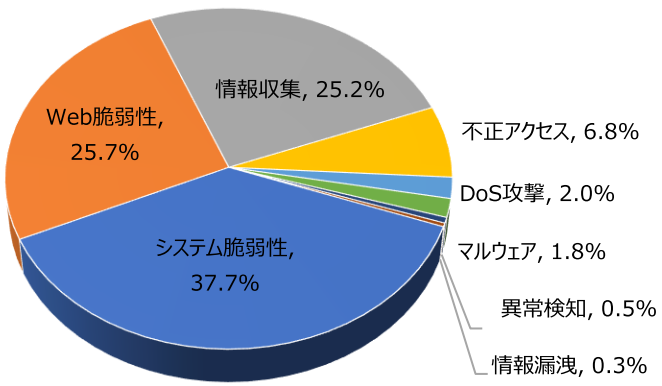
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	32.7%	-
Web脆弱性(Web Vulnerability)	28.5%	▲1
情報収集(Information Gathering)	26.7%	▼1
不正アクセス(Unauthorized access)	7.5%	-
DoS攻撃(Denial of service attack)	1.9%	▲2
マルウェア(Malware)	1.3%	▼1
異常検知(Anomaly Detection)	1.0%	▼1
情報漏洩(Information Exposure)	0.4%	-

2023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0.98倍ぐらい減少し、全体の攻撃件数が減少した。

そのうち、情報収集に関する攻撃は先月比べて約300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。

また、システム脆弱性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Command Injection(LinkSys E-series Routers Vulnerability)攻撃件数増加によるものだと確認できた。

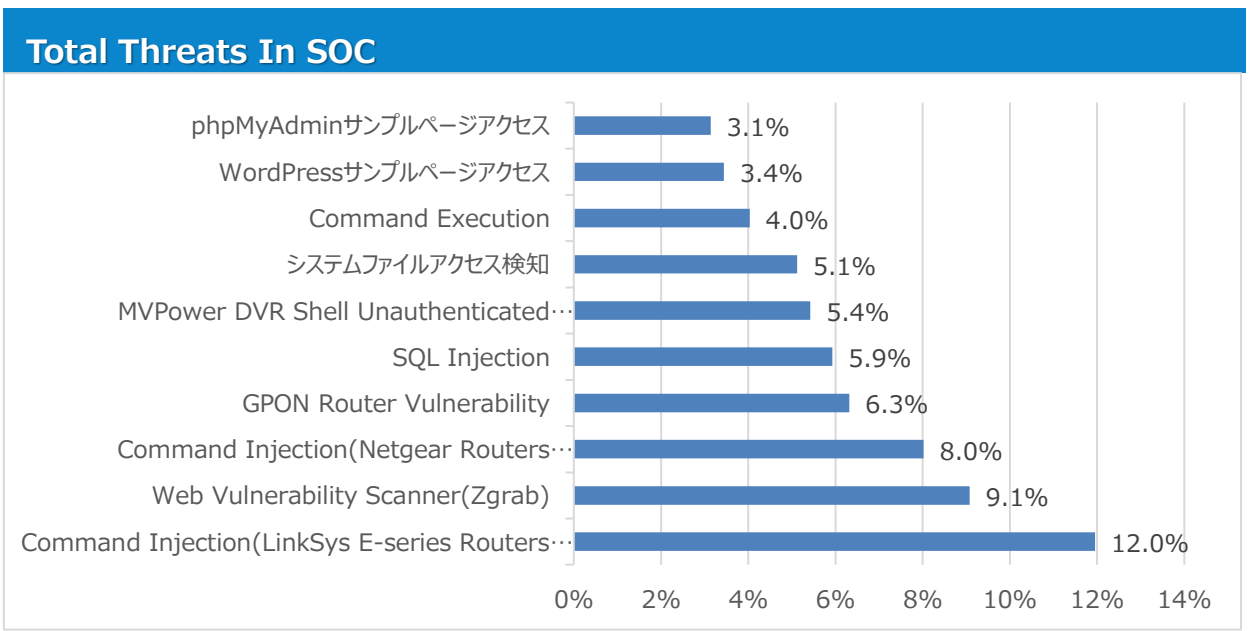


月次攻撃サービスの統計及び分析 - 2023年01月

02. 月次脆弱性攻撃TOP10

2023年01月の月次脆弱性TOP10を確認した結果、 Command Injection(LinkSys E-series Routers Vulnerability), phpMyAdminサンプルページアクセス攻撃が新たに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。一方Command Injection(LinkSys E-series Routers Vulnerability)攻撃件数が800件ぐらい増加したことが確認できた。

順位	検知名	比率(%)	比較
1	Command Injection(LinkSys E-series Routers Vulnerability)	12.0%	NEW
2	Web Vulnerability Scanner(Zgrab)	9.1%	▼1
3	Command Injection(Netgear Routers Vulnerability)	8.0%	▼1
4	GPON Router Vulnerability	6.3%	▼1
5	SQL Injection	5.9%	▲1
6	MVPower DVR Shell Unauthenticated Command Execution	5.4%	▲1
7	システムファイルアクセス検知	5.1%	▼2
8	Command Execution	4.0%	-
9	WordPressサンプルページアクセス	3.4%	▲1
10	phpMyAdminサンプルページアクセス	3.1%	NEW



月次攻撃サービスの統計及び分析 - 2023年01月

03. 月次ブラックリストIPアドレスTOP 10

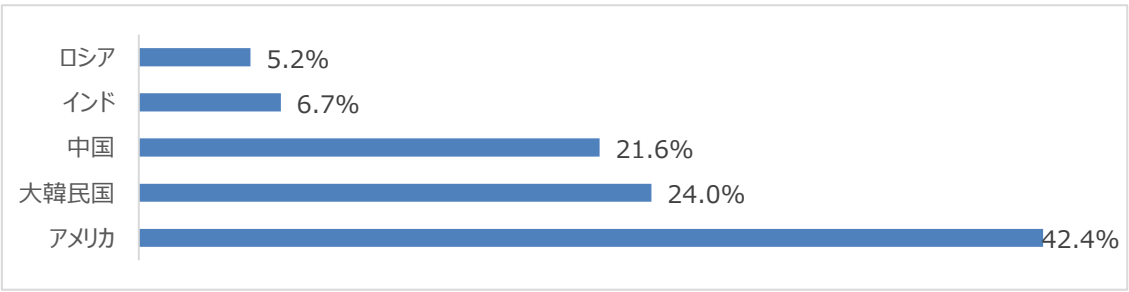
2023年01月についてTOP10を確認した結果、大韓民国の攻撃比率が増加し、一方アメリカと中国、インド、ロシアの攻撃の比率は減少した。特に大韓民国は11.5%、約800件ぐらい増加したことが確認できた。

※ 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	14.36.39.167	KR	Apache Log4j RCE(CVE-2021-44228)
2	185.7.214.218	RU	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
3	15.235.118.56	CA	システムファイルアクセス検知
4	14.36.38.179	KR	Directory Traversal
5	81.17.22.106	CH	WordPressサンプルページアクセス
6	85.31.44.156	US	Command Execution
7	165.232.160.6	SG	phpMyAdminサンプルページアクセス
8	109.237.98.226	GB	システムファイルアクセス検知
9	109.237.97.180	GB	システムファイルアクセス検知
10	195.178.120.130	US	Web-CGI Vulnerability

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	14.36.39.167	KR
2	185.7.214.218	RU
3	15.235.118.56	CA
4	14.36.38.179	KR
5	81.17.22.106	CH

Rank	Source IP	Country
6	85.31.44.156	US
7	165.232.160.6	SG
8	109.237.98.226	GB
9	109.237.97.180	GB
10	195.178.120.130	US

攻撃パターン毎の詳細分析結果

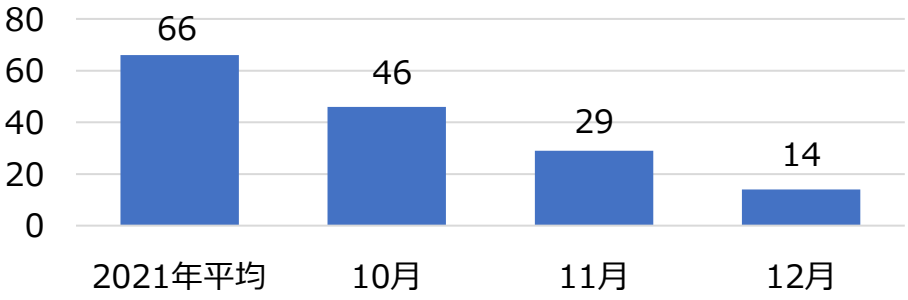
01月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
CommandInjection (Netgear Routers Vulnerability)	NetGear DGNシリーズのルータ内のウェブサーバが一部のURLに対して認証をせず、「setup.cgi」スクリプトの「syscmd」機能を活用して任意のコマンドを実行することができる。
GPON Router Vulnerability	Dasan GPON家庭用のルータから発見された脆弱性で「?images」の文字列を機器アクセス用URLに入力することで認証をスルー出来る脆弱性である。 当該の脆弱性を利用して認証されていない攻撃者が機器へリモートでコマンドを実行し、DNS設定修正などの様々な攻撃が可能である。 この脆弱性は家庭用ルータにて発見された。
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングで不適切なコントローラがクラスに呼び出されてリモートコード実行攻撃ができる脆弱性である。¥think¥*クラスを呼び出して脆弱なオブジェクトを介して攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
システムファイル アクセス検出	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。
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。
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥'shell¥'」ファイルを利用することでクエリの文字列の中から任意のシステムコマンドが実行できるようになる。
Command Execution	適切な認証が行われていない使用者の入力値がOSコマンドの一部、もしくはその他のコマンドで構成され実行される場合、意図しないシステムコマンドが実行され、不正に権限が変更されたり、システム動作及び運用に悪影響を及ぼす可能性がある。一般的なコマンドラインのパラメータやストリーム入力など、外部入力を使用しシステムコマンドを生成するプログラムはたくさん存在するが、この場合、外部の入力文字列は信頼できないため、適切な処理（チェック処理）をしないと攻撃者が望むコマンドが実行可能になる。
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

SPIDER TM のポリシーにて、2022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14件である。12月1か月の間、Google Chrome(CVE-2022-2998), Windows(CVE-2022-44673), Linux(CVE-2022-47939), MS Exchange(CVE-2022-41040, CVE-2022-41082)などに対する検知ポリシーが配布された。



3か月間件数

6,028
全体配布量

14
今月配布量

29
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 (msg:"IGRSS.2.06051 Google, Chrome, CVE-2022-2998, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:".contentWindow.getSelection().selectAllChildren("; content:".contentDocument.addEventListener("; within:500; content:"focus()|3B|"; distance:0; content:"setTimeout("; within:500; content:".remove()|3B|"; within:500; sid:206051;)	Google ChromeのCVE-2022-2998脆弱性を悪用したUAF攻撃を検知するポリシー	Google, Chrome, CVE-2022-2998
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.1.06056 MS, Windows Client Server, CVE-2022-44673, Attempted Administrator Privilege Gain"; flow:to_client,established; file_data; content:"|89 75 C8 89 74 24 60 48 89 75 B0 48 89 75 F8 89 75 00 FF 15 1C 1E 00 00 66 0F 6F 05 74 22 00 00|"; fast_pattern:only; sid:106056;)	MS Windows Client ServerのCVE-2022-44673脆弱性を悪用した権限上昇攻撃を検知するポリシー	MS, Windows Client Server, CVE-2022-44673
alert tcp any any -> $HOME_NET 445 (msg:"IGRSS.2.06063 Linux, SMB2, CVE-2022-47939, Attempted User Privilege Gain"; flow:to_server,established; content:"|FE|SMB"; depth:4; offset:4; nocase; content:"|04 00|"; within:2; distance:8; byte_extract:4,22,tree_id,relative,little; byte_extract:4,0,session_id,relative,little; content:"|FE|SMB"; distance:0; nocase; content:"|04 00|"; within:2; distance:8; byte_test:4,=,tree_id,22,relative,little; byte_test:4,=,session_id,26,relative,little; content:"|04 00 00 00|"; within:4; distance:50; sid:206063;)	Linux SMB2のCVE-2022-47939脆弱性を悪用したUAF攻撃を検知するポリシー	Linux, SMB2, CVE-2022-47939
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06064 MS, Exchange, CVE-2022-41040, CVE-2022-41082, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/owa/"; nocase; http_uri; content:"@"; distance:0; http_uri; content:"/powershell"; distance:0; fast_pattern; nocase; http_uri; sid:106064;)	MS ExchangeのCVE-2022-41040, CVE-2022-41082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	MS, Exchange, CVE-2022-41040, CVE-2022-41082