SECURITY REPORT

2023

FEB

2023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 - 2023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。

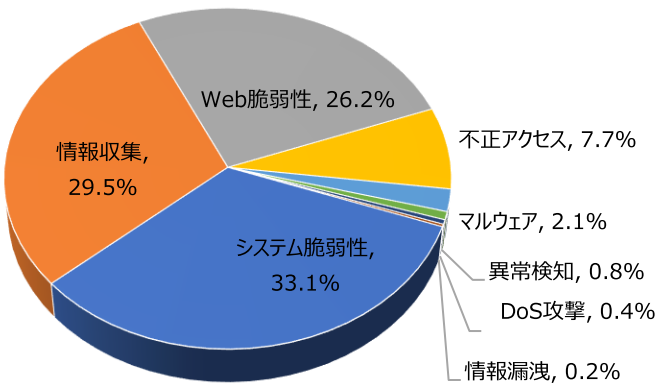
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	33.1%	-
情報収集(Information Gathering)	29.5%	▲1
Web脆弱性(Web Vulnerability)	26.2%	▼1
不正アクセス(Unauthorized access)	7.7%	-
マルウェア(Malware)	2.1%	▲1
異常検知(Anomaly Detection)	0.8%	▲1
DoS攻撃(Denial of service attack)	0.4%	▼2
情報漏洩(Information Exposure)	0.2%	-

2023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0.97倍ぐらい減少し、全体の攻撃件数が減少した。

そのうち、システム脆弱性に関する攻撃は先月比べて約400件ほど減少し、これはCommand Injection(LinkSys E-series Routers Vulnerability)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250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。



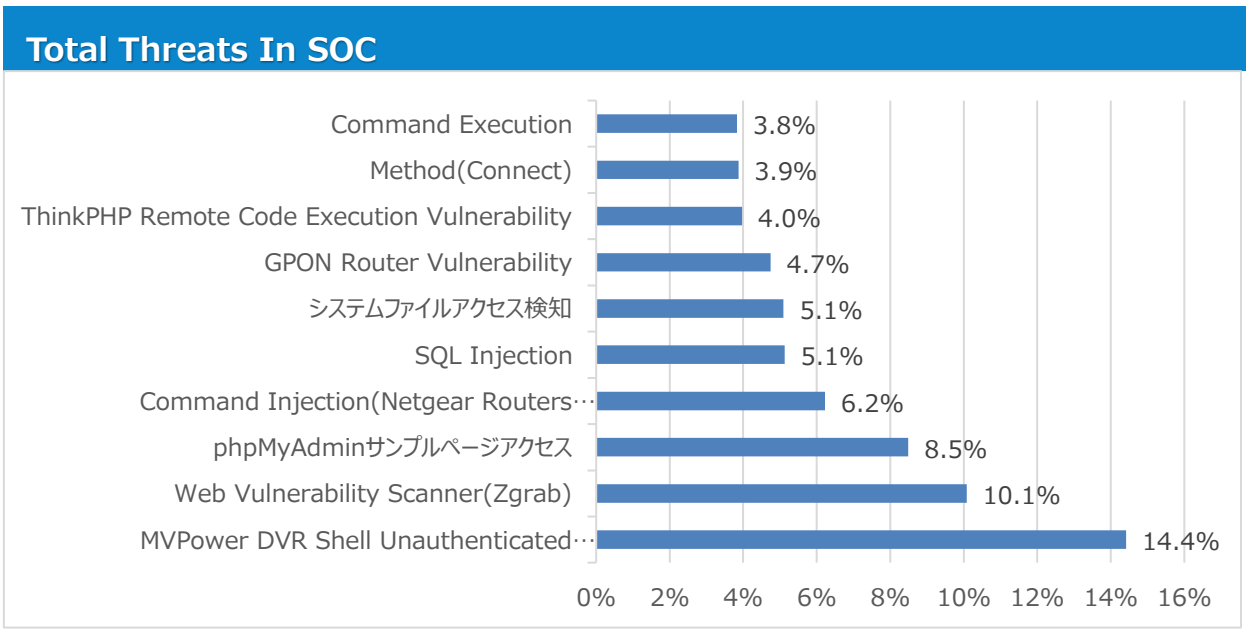
Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2023年02月

02. 月次脆弱性攻撃TOP10

2023年02月の月次脆弱性TOP10を確認した結果、ThinkPHP Remote Code Execution Vulnerability, Method(Connect)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 MVPower DVR Shell Unauthenticated Command Execution攻撃件数が600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	MVPower DVR Shell Unauthenticated Command Execution	14.4%	▲5
2	Web Vulnerability Scanner(Zgrab)	10.1%	-
3	phpMyAdminサンプルページアクセス	8.5%	▲7
4	Command Injection(Netgear Routers Vulnerability)	6.2%	▼1
5	SQL Injection	5.1%	-
6	システムファイルアクセス検知	5.1%	▲1
7	GPON Router Vulnerability	4.7%	▼3
8	ThinkPHP Remote Code Execution Vulnerability	4.0%	NEW
9	Method(Connect)	3.9%	NEW
10	Command Execution	3.8%	▼2



Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

月次攻撃サービスの統計及び分析 - 2023年02月

03. 月次ブラックリストIPアドレスTOP 10

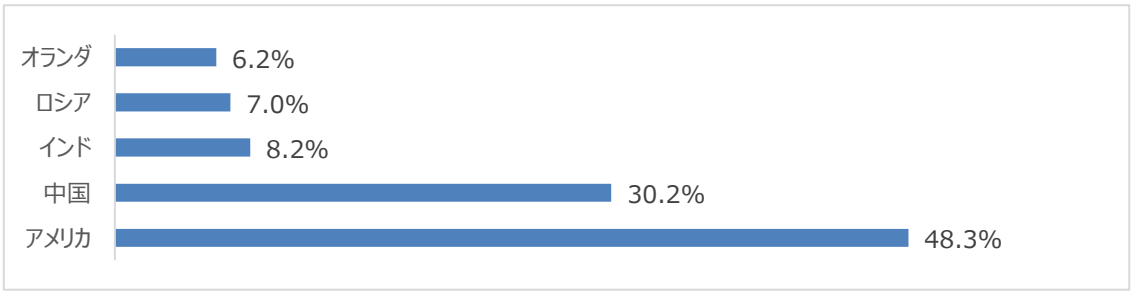
2023年02月についてTOP10を確認した結果、アメリカと中国、インド、ロシア、オランダの攻撃比率が増加し、一方大韓民国の攻撃の比率は減少した。特に大韓民国は13.5%、約1000件ぐらい減少したことが確認できた。

※ 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	112.47.34.246	CN	phpMyAdminサンプルページアクセス
2	152.89.196.211	GB	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
3	45.12.253.180	NL	Command Injection(D-Link HNAP Vulnerability)
4	80.85.241.15	RU	phpMyAdminサンプルページアクセス
5	51.161.197.46	AU	phpMyAdminサンプルページアクセス
6	195.133.40.81	NL	Alcatel-Lucent OmniPCX MasterCGI Command Execution
7	89.248.168.235	NL	phpMyAdminサンプルページアクセス
8	173.201.19.193	US	phpMyAdminサンプルページアクセス
9	179.43.143.186	CH	Method(Connect)
10	147.185.239.98	US	Method(Connect)

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	112.47.34.246	CN	6	195.133.40.81	NL
2	152.89.196.211	GB	7	89.248.168.235	NL
3	45.12.253.180	NL	8	173.201.19.193	US
4	80.85.241.15	RU	9	179.43.143.186	CH
5	51.161.197.46	AU	10	147.185.239.98	US

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

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。

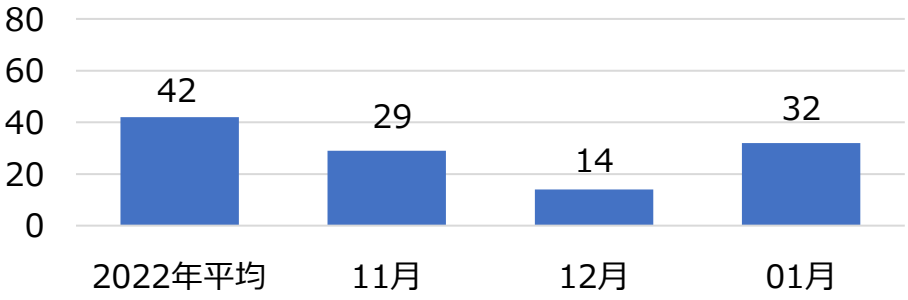
攻撃パターン	詳細分析結果
MVPower DVR Shell Unauthenticated Command Execution	HTTPリクエストを処理する際にユーザーが送った入力値の有効性検査が充分に行われず、リモート攻撃者がWebインターフェースの「¥'shell¥'」ファイルを利用することでクエリの文字列の中から任意のシステムコマンドが実行できるようになる。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)は、Webサーバの設定ページや許可方法、許可されていないWebページ、ライセンスのないポートなど、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。
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。
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。
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。
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。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security) トンネリングで内部アクセスを試す。これのためにConnect Methodを使用し、脆弱性が存在する場合攻撃のための中間経由地として使用される可能性がある。
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。

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved

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、2023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32件である。
01月1か月の間、Xiaoqiyingハッカーグループ、VMクラウド(CVE-2022-31678, CVE-2021-39144)、
Linux(CVE-2022-47942)などに対する検知ポリシーが配布された。



3か月間件数

6,060
全体配布量

32
今月配布量

14
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.1.06073 Vmware Cloud Foundation, NSX Manager, CVE-2022-31678, CVE-2021-39144, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/services/usermgmt/password/"; fast_pattern:only; http_uri; content:"java|2E|"; nocase; http_client_body; pcre:"/<¥w+¥s+class¥s*?¥x3D¥s*?[¥x22¥x27]java¥x2e/Pi"; sid:106073;)	Vmware Cloud Foundation NSX ManagerのCVE-2022-31678, CVE-2021-39144脆弱性を悪用したリモートコマンド実行攻撃を検知するポリシー	Vmware Cloud Foundation, NSX Manager, CVE-2022-31678, CVE-2021-39144
alert tcp any any -> $HOME_NET 445 (msg:"IGRSS.2.06075 Linux, ksmbd, CVE-2022-47942, Attempted User Privilege Gain"; flow:to_server,established; content:"|FE|SMB|40 00|"; content:"|11 00|"; within:2; distance:6; content:"|21 00 03 00|"; within:4; distance:50; byte_math:bytes 4, offset 0, oper -, rvalue 8, result SetInfoSizeMinus8, relative, endian little; byte_test:4, >, SetInfoSizeMinus8, 44, relative, little; sid:206075;)	Linux ksmbdのCVE-2022-47942脆弱性を亜興したBOF攻撃を検知するポリシー	Linux, ksmbd, CVE-2022-47942
alert tcp any any -> [$HOME_NET,$HTTP_SERVERS] any (msg:"IGRSS.1.06090 WordPress, Oturia Smart Google Code Inserter, CVE-2018-3810, Attempted Administrator Privilege Gain"; flow:established,to_server; content:"POST"; nocase; http_method; content:"/options-general.php?page=smartcode"; nocase; fast_pattern; http_uri; content:"sgcgoogleanalytic="; nocase; depth:35; http_client_body; sid:106090;)	XiaoqiyingグループのWordPress Oturia Smart Google Code InserterプラグインのCVE-2018-3810脆弱性を悪用する攻撃を検知するポリシー	Xiaoqiying, 晓骑营
alert tcp any any -> [$HOME_NET,$HTTP_SERVERS] any (msg:"IGRSS.1.06091 phpMyAdmin, Attempted Administrator Privilege Gain"; flow:established,to_server; content:"/scripts/setup.php"; nocase; fast_pattern; http_uri; content:"action="; nocase; depth:7; http_client_body; content:"configuration="; nocase; http_client_body; content:"PMA_Config"; nocase; http_client_body; content:"source"; nocase; http_client_body; sid:106091;)	XiaoqiyingグループのphpMyAdminのデフォルト設定ファイルのアクセス試みを検知するポリシー	Xiaoqiying, 晓骑营

Copyright ⓒ Cyberfortress, Inc. 2020. All rights reserved