SECURITY REPORT

2023

MAY

2023年05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05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。

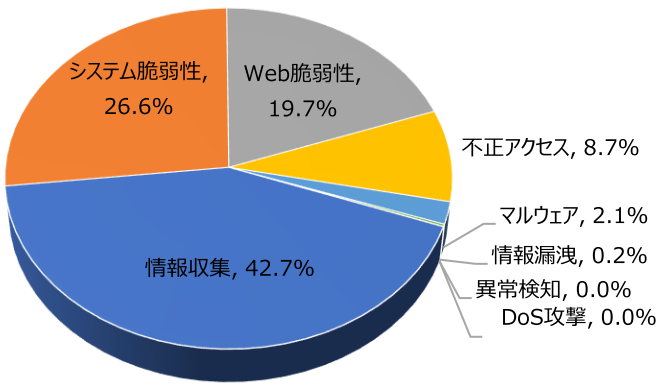
01. 月次攻撃類型

パターン	比率(%)	比較
情報収集(Information Gathering)	42.7%	▲1
システム脆弱性(System Vulnerability)	26.6%	▼1
Web脆弱性(Web Vulnerability)	19.7%	-
不正アクセス(Unauthorized access)	8.7%	-
マルウェア(Malware)	2.1%	-
情報漏洩(Information Exposure)	0.2%	-
DoS攻撃(Denial of service attack)	0.0%	-
異常検知(Anomaly Detection)	0.0%	-

2023年05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1.25倍ぐらい増加し、全体の攻撃件数が増加した。

そのうち、情報収集に関する攻撃は先月比べて約1,140件ほど増加し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数の増加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100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。

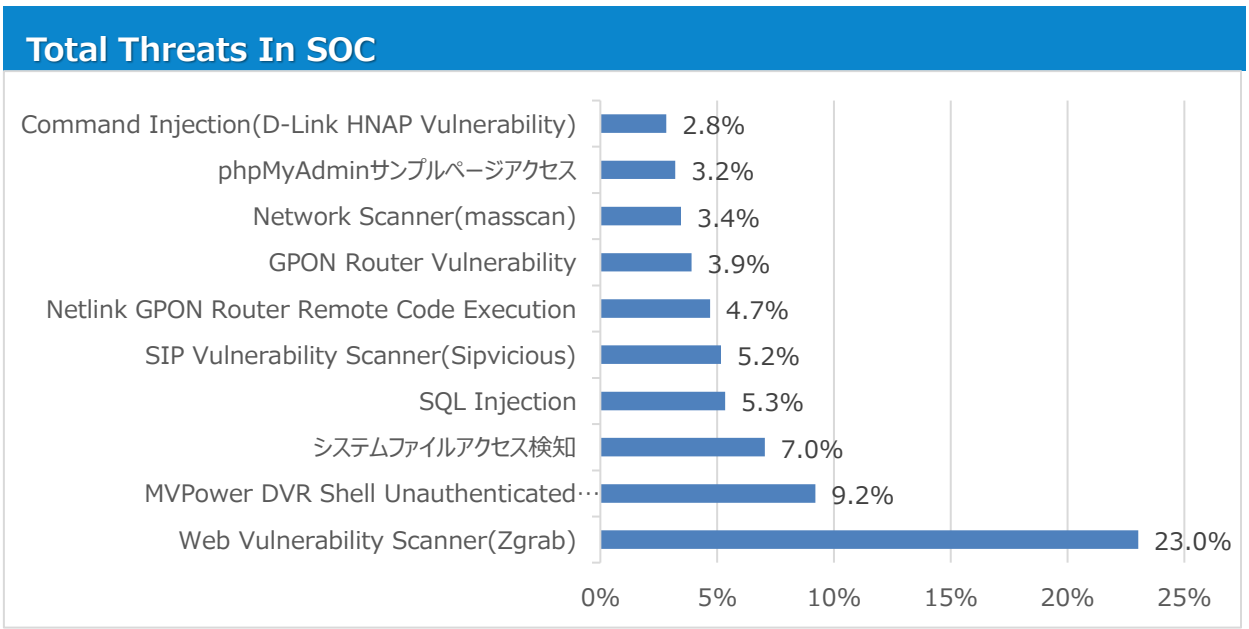


月次攻撃サービスの統計及び分析 - 2023年05月

02. 月次脆弱性攻撃TOP10

2023年05月の月次脆弱性TOP10を確認した結果、 SIP Vulnerability Scanner(Sipvicious), Network Scanner(masscan), Command Injection(D-Link HNAP Vulnerability)攻撃が新たにTOP10に登場し、全体的な攻撃件数が増加したことが確認できた。特に、Web Vulnerability Scanner(Zgrab)攻撃件数が1,000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	Web Vulnerability Scanner(Zgrab)	23.0%	▲1
2	MVPower DVR Shell Unauthenticated Command Execution	9.2%	▼1
3	システムファイルアクセス検知	7.0%	▲1
4	SQL Injection	5.3%	▲2
5	SIP Vulnerability Scanner(Sipvicious)	5.2%	NEW
6	Netlink GPON Router Remote Code Execution	4.7%	▲2
7	GPON Router Vulnerability	3.9%	-
8	Network Scanner(masscan)	3.4%	NEW
9	phpMyAdminサンプルページアクセス	3.2%	▼6
10	Command Injection(D-Link HNAP Vulnerability)	2.8%	NEW



月次攻撃サービスの統計及び分析 - 2023年05月

03. 月次ブラックリストIPアドレスTOP 10

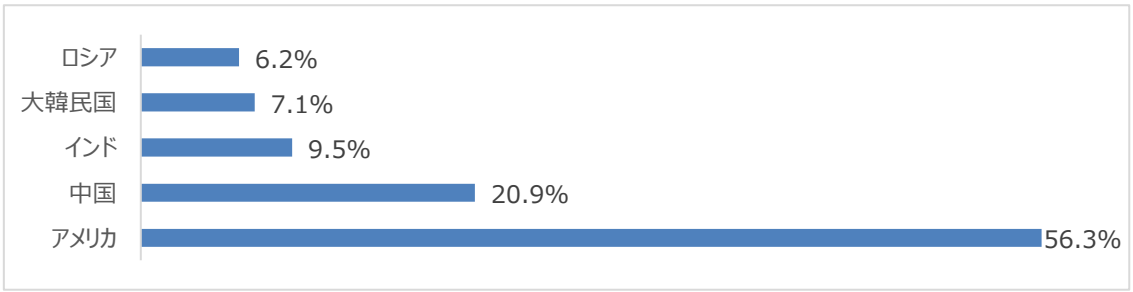
2023年05月についてTOP10を確認した結果、アメリカと中国、大韓民国の攻撃比率が増加し、一方インドとロシアの攻撃の比率は減少した。特にアメリカと中国の攻撃比率が合わせて約48%ぐらいで攻撃のほぼ半分ぐらいを占めていることが確認できた。

※ 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	152.89.196.54	NL	Application Vulnerability(PHPUnit)
2	95.214.55.244	PL	Apache Log4j RCE(CVE-2021-44228)
3	109.237.97.180	GB	システムファイルアクセス検知
4	109.237.98.226	GB	システムファイルアクセス検知
5	79.124.59.170	BG	Network Scanner(masscan)
6	51.159.93.171	FR	SIP Vulnerability Scanner(Sipvicious)
7	80.66.77.239	TF	DVR(Digital Video Recorder) Login Bypass (CVE-2018-9995, CVE-2018-10676)
8	192.142.226.5	TH	etcpasswd Detect
9	152.89.196.222	NL	ThinkPHP Remote Code Execution Vulnerability
10	69.174.102.18	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
1	152.89.196.54	NL
2	95.214.55.244	PL
3	109.237.97.180	GB
4	109.237.98.226	GB
5	79.124.59.170	BG

Rank	Source IP	Country
6	51.159.93.171	FR
7	80.66.77.239	TF
8	192.142.226.5	TH
9	152.89.196.222	NL
10	69.174.102.18	US

攻撃パターン毎の詳細分析結果

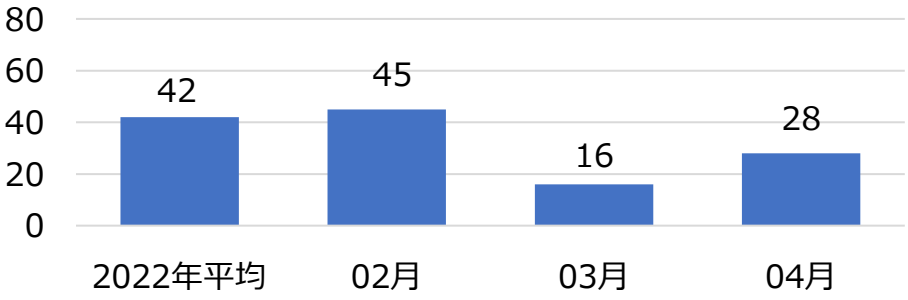
05月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

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。
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。
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。
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	Netlink GPON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。
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。
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。
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。
Command Injection (D-Link HNAP Vulnerability)	D-Link製品を設置する際に使用されるHNAP(Home Network Administration Protocol)に関 するスクリプトに存在する脆弱性で認証を迂回してサービス中止、バックドアインストールなどのコマンドの実 行が可能になる。

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、2023年04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28件である。04月1か月の間、Chinotto, Qakbot MalwareとSophos Firewall(CVE-2022-3236), PaperCut MF(CVE-2023-27350)などに対する検知ポリシーが配布された。



3か月間件数

6,149
全体配布量

28
今月配布量

16
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.06158 Malware, CNC, Chinotto, A Network Trojan was detected"; flow:to_server,established; content:"/js/20170805.hwp"; fast_pattern:only; http_uri; sid:806158;)	Chinotto Malwareのネットワーク通信を検知するポリシー	Malware, CNC, Chinotto
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.1.06159 SERVER-WEBAPP, Sophos, Sophos Firewall, CVE-2022-3236, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/controller"; fast_pattern:only; http_uri; content:"_discriminator"; http_client_body; pcre:"/(¥x22|%(25)?22)_discriminator(¥x22|%(25)?22)[¥s+]*:[¥s+]*(¥x7b|%(25)?7b)((?!(?<!¥x5c)¥x7d).)*?[¥x60¥x3b¥x7c¥x23]/Pim"; sid:106159;)	Sophos FirewallのCVE-2022-3236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	SERVER-WEBAPP, Sophos, Sophos Firewall, CVE-2022-3236
alert tcp $EXTERNAL_NET any -> $HOME_NET [$HTTP_PORTS,9191,9192] (msg:"IGRSS.10.06175 SERVER-WEBAPP, PaperCut, MF, CVE-2023-27350, Web Application Attack"; flow:to_server,established; content:"service="; nocase; content:"configEditor"; distance:0; nocase; content:"quickFindForm"; within:18; nocase; content:"|24|TextField="; nocase; content:"print"; distance:0; nocase; content:"script"; within:11; nocase; content:"sandboxed"; within:14; nocase; pcre:"/(^|[&¥r¥n])¥x24TextField=[^&]*?print(¥x2e|%(25)?2e)script(¥x2e|%(25)?2e)sandboxed/i"; sid:1006175;)	PaperCut MFの脆弱性であるCVE-2023-27350を悪用したサンドボックス設定試みを検知するポリシー	SERVER-WEBAPP, PaperCut, MF, CVE-2023-27350
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.06177 Malware, Dropper, Qakbot, A Network Trojan was detected"; flow:to_server,established; flowbits:isset,file.onenote.embedded; file_data; content:"CreateObject|28 22|Wscript.Shell|22 29|"; fast_pattern; nocase; content:"RegWrite"; distance:0; nocase; sid:806177;)	Qakbot のネットワーク通信を検知するポリシー	Malware, Dropper, Qakbot