CyberFortress Report

2021
MAR

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 - 2021年03月

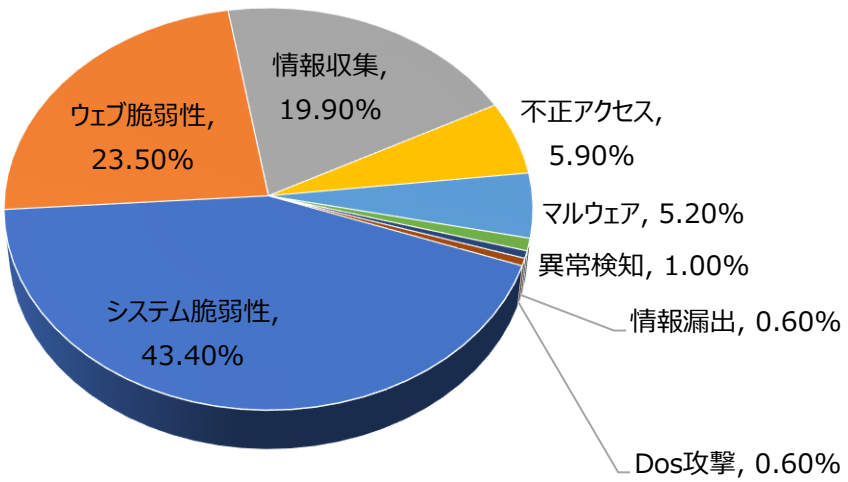
株式会社サイバーフォートレスでは攻撃サービス(ポート)情報を収集し、分析しています。
分析内容から、月次攻撃サービス（ポート）、月次攻撃サービスパターンのTOP10を確認し、過去データと比較し、攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てていただければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	43.4	-
ウェブ脆弱性(Web Vulnerability)	23.5	-
情報収集(Information Gathering)	19.9	-
不正アクセス(Unauthorized access)	5.9	-
マルウェア(Malware)	5.2	-
異常検知(Anomaly Detection)	1.0	-
情報漏洩(Information Exposure)	0.6	-
Dos攻撃(Denial of service attack)	0.6	-

[表1-1] 月次攻撃類型

2021年03月の月次攻撃の類型を確認した結果、 先月と同じ順位のことが確認できた。
先月と比べてシステム脆弱性(System Vulnerability)は増加し、ウェブ脆弱性(Web Vulnerability)と情報収集(Information Gathering)そして、不正アクセス(Unauthorized access)は、少し減少したのが確認できる-。これは検知名「Wordpressサンプルページアクセス」と「phpmyadminサンプルページアクセス」のイベント減少による影響だと判断できる。



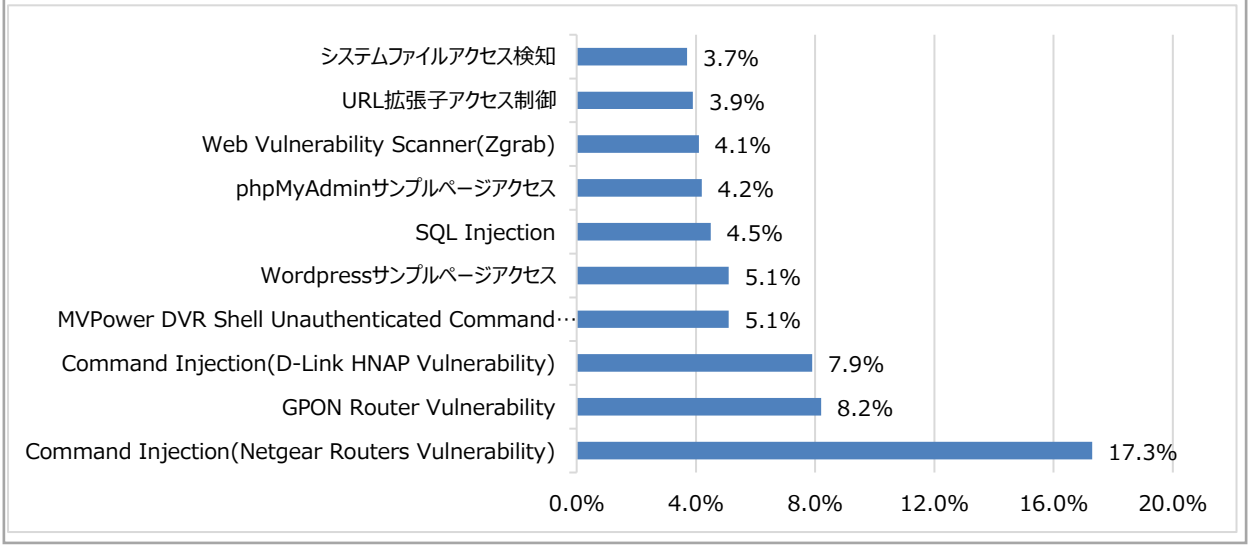
月次攻撃サービスの統計及び分析 - 2021年03月

02. 月次脆弱性攻撃TOP10

2021年03月の月次脆弱性攻撃TOP10を確認した結果、Web Vulnerability Scanner(Zgrab)、URL拡張子アクセス制御、システムファイルアクセス検知の脆弱性が新たにTOP10に登場した。
その他、Command Injectionに関する脆弱性が上位を占めていることが確認でき、SQL Injectionの場合、順位が少し上昇したことが確認できた。

順位	検知名	比率(%)	比較
1	Command Injection(Netgear Routers Vulnerability)	17.3	-
2	GPON Router Vulnerability	8.9	▲1
3	Command Injection(D-Link HNAP Vulnerability)	7.9	▼1
4	MVPower DVR Shell Unauthenticated Command Execution	5.1	▲1
5	Wordpressサンプルページアクセス	5.1	▼1
6	SQL Injection	4.5	▲2
7	phpMyAdminサンプルページアクセス	4.2	▼1
8	Web Vulnerability Scanner(Zgrab)	4.1	NEW
9	URL拡張子アクセス制御	3.9	NEW
10	システムファイルアクセス検知	3.7	NEW

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2021年03月

03. 月次ブラックリストIPアドレスTOP 10

2021年03月の基準で中国の送信元のIPが約半分を占めていてシェアとして一番高い。その後他に、アメリカ、インド、ロシア、韓国の順に確認できた。

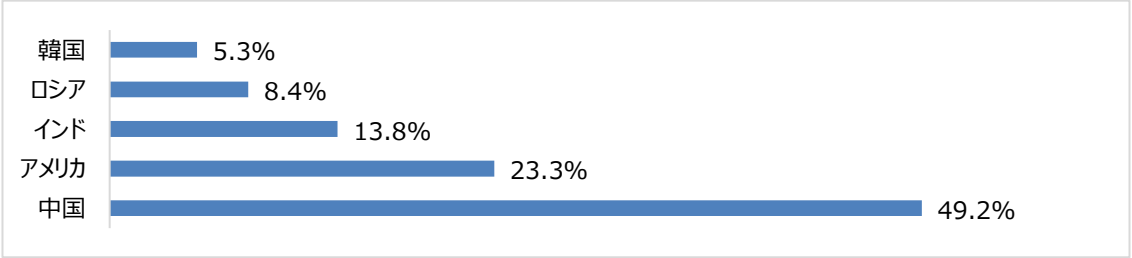
当該の送信元IPの危険性は独自調査で確認した結果である。

下記の表を参考にしてファイウォールやセキュリティ機器からの遮断を推奨する。

順位	ブックリストIP	国	IGLOO_CTI	攻撃情報
1	45.155.205.108	RU	9/114	ThinkPHP Remote Code Execution Vulnerability
2	45.155.205.225	RU	20/114	ThinkPHP Remote Code Execution Vulnerability
3	2.57.122.97	RO	19/114	Command Injection
4	89.248.168.108	GB	7/114	Netlink GPON Router Remote Code Execution
5	157.245.100.146	IN	3/114	MVPower DVR Shell Unauthenticated Command Execution
6	31.210.20.175	US	14/114	Code Execution(Bash ShellShock)
7	89.248.160.139	GB	8/114	Network Scan
8	89.248.165.7	GB	11/114	phpMyAdminサンプルページアクセス
9	97.74.229.113	US	3/114	Admin (管理者) ページアクセス
10	42.114.249.74	VN	4/114	SQL Injection

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	45.155.205.108	RU
2	45.155.205.225	RU
3	2.57.122.97	RO
4	89.248.168.108	GB
5	157.245.100.146	IN

Rank	Source IP	Country
6	31.210.20.175	US
7	89.248.160.139	GB
8	89.248.165.7	GB
9	97.74.229.113	US
10	42.114.249.74	VN

攻撃パターン毎の詳細分析結果

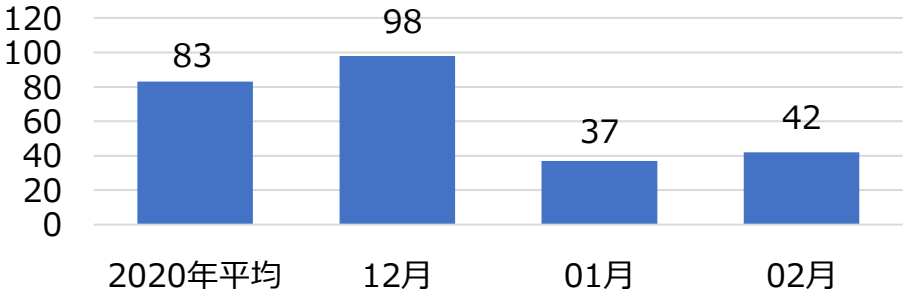
03月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

攻撃パターン	詳細分析結果
Command Injection(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通せる脆弱性である。 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。
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。 攻撃者は「Domain/HNAP1/GetDeviceSettings/」パスの後ろにコマンドを挿入し、「SOAPAction」フィールドを利用して実行を試みる。
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、リモート攻撃者がウェブ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。
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。
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。
phpMyAdmin サンプルページアクセス	phpMyAdminはウェブサーバーからMySQLを管理する目的でPHPで作成されているオープンソースツールで、この攻撃はMy-SQLサーバを対象に脆弱性を探してデータベースの作成/削除、テーブルの作成/削除、フィールドの作成/削除、SQL問い合わせ実行、実行権限管理機能などが実行できる脆弱性が存在している場合、phpMyAdminの「script/setup.php」ファイルに「?」因子を利用して任意の関数を挿入することでシステムコマンドが実行できる。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)はウェブーサバの設定ページもしくは、許可メソッド、非認可されたウェブページもしくは、非許可ポートなどの脆弱なところの存在有無を確認するために使用する。
URL拡張子アクセス制御	ウェブサーバの内部ファイルに対してアクセス権限が弱く設定されている場合、悪意的なユーザーの攻撃の対象になる。アクセス可能なウェブサーバから外部の公開のためのファイル及びディレクトリのアクセス権限が匿名のユーザーにも許可されているのであればシステムの重要ファイル(システムファイル、ライブラリ、パスワードファイルなど)は悪意的な攻撃対象になる。
システムファイルアクセス検知	攻撃者はシステムの情報の獲得のためにDirectory Traversal脆弱性を利用して/etc/passwdや*.conf /.envのようなアカウント、環境変数など、設定ファイルにアクセスを試す。

検知ポリシー

▶. 月間サイバー脅威検知ポリシー統計

SPIDER TM のポリシーで、2021年02月の1か月間共有されたサイバー脅威検知ポリシーは42件である。
02月の1か月間Windows(CVE-2021-1648), CISCO Routers(CVE-2021-1314), Citrix Gateway(CVE-2020-8195)脆弱性に関する検知ポリシーが配布された。



3か月間件数

4,870
全体配布量

42
今月配布量

37
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.2.04857 MS, Windows, CVE-2021-1648, Attempted User Privilege Gain"; flow:to_server,established; file_data; content:"|48 89 88 50 01 00 00 48 B9 42 42 42 42 42 42 42 42 48 8B 05 5B 46 00 00 48 89 90 50 02 00 00 48|"; fast_pattern:only; sid:204857;)	MS WindowsのCVE-2021-1648脆弱性を悪用したユーザー権限奪取を検知するポリシー	MS, Windows, CVE-2021-1648
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.04858 Cisco, routers, CVE-2021-1314, Web Application Attack"; flow:to_server,established; content:"name="; nocase; http_client_body; content:"USBimagefile"; within:20; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?USBimagefile¥d?((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/Psim"; sid:1004858;)	Cisco RV Routers의 CVE-2021-1314脆弱性を悪用したコマンド挿入攻撃を検知するポリシー	Cisco, routers, CVE-2021-1314
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.04860 Citrix, Gateway, CVE-2020-8195, Web Application Attack"; flow:to_server,established; content:"/rapi/filedownload"; fast_pattern:only; http_uri; content:"<clipermission></clipermission>"; nocase; http_client_body; sid:1004860;)	Citrix GatewayのCVE-2020-8195脆弱性を悪用した情報漏洩試しを検知するポリシ	Citrix, Gateway, CVE-2020-8195
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.2.04862 Adobe, Acrobat, CVE-2021-21017, Attempted User Privilege Gain"; flow:to_client,established; flowbits:isset,file.pdf; file_data; content:"Object.defineProperty("; content:"__iterator__"; within:75; fast_pattern; content:"get"; content:"__proto__"; content:"for"; sid:204862;)	Adobe AcrobatのCVE-2021-21017脆弱性を悪用したユーザー権限奪取試しを検知するポリシー	Adobe, Acrobat, CVE-2021-21017

月間重要検知ポリシー