CyberFortress Report

2021
APR

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04月

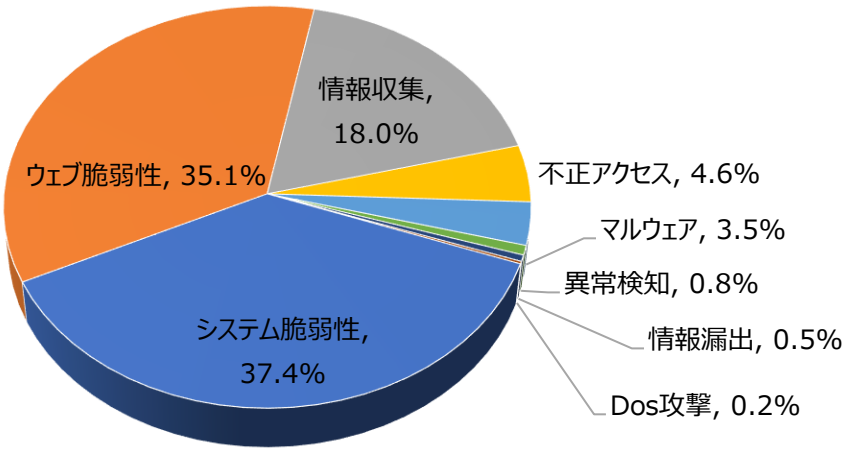
株式会社サイバーフォートレスでは攻撃情報を収集し、分析しています。
分析内容から、月次攻撃類型、脆弱性攻撃、ブラックリストのTOP10を確認し、過去データと比較し、攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てていただければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	37.4	-
ウェブ脆弱性(Web Vulnerability)	35.1	-
情報収集(Information Gathering)	18.0	-
不正アクセス(Unauthorized access)	4.6	-
マルウェア(Malware)	3.5	-
異常検知(Anomaly Detection)	0.8	-
情報漏洩(Information Exposure)	0.5	-
Dos攻撃(Denial of service attack)	0.2	-

[表1-1] 月次攻撃類型

2021年04月の月次攻撃の類型を確認した結果、 先月と同じ順位であることが確認できた。
先月、システム脆弱性(System Vulnerability)とウェブ脆弱性(Web Vulnerability)の比率はそれぞれ43%と23%で約20%の差があったが、今月は37%と35%と差がほぼなくなったことが確認できる。
これは月次脆弱性のTOP10に新たに登場したPHPに関する脆弱性攻撃の影響だと判断される。

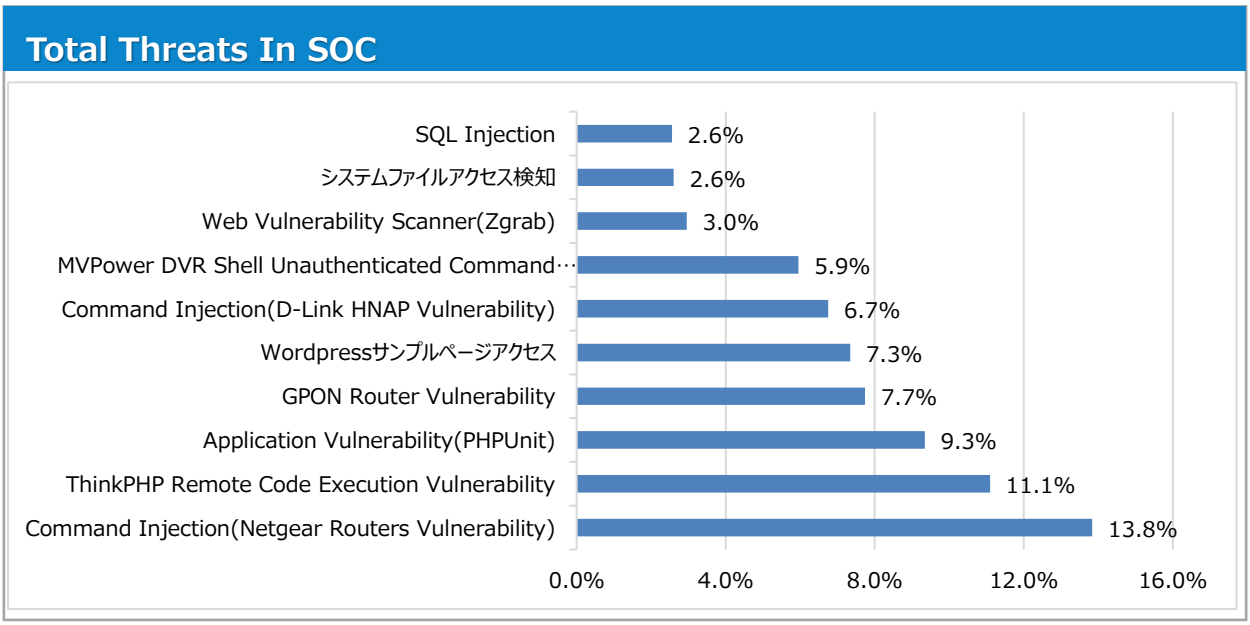


月次攻撃サービスの統計及び分析 - 2021年04月

02. 月次脆弱性攻撃TOP10

2021年04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)	13.8	-
2	ThinkPHP Remote Code Execution Vulnerability	11.1	NEW
3	Application Vulnerability (PHPUnit)	9.3	NEW
4	GPON Router Vulnerability	7.7	▼2
5	Wordpressサンプルページアクセス	7.3	▼1
6	Command Injection (D-Link HNAP Vulnerability)	6.7	▲2
7	MVPower DVR Shell Unauthenticated Command Execution	5.9	▼1
8	Web Vulnerability Scanner (Zgrab)	3.0	-
9	システムファイルアクセス検知	2.6	▲1
10	SQL Injection	2.6	▼4



月次攻撃サービスの統計及び分析 - 2021年04月

03. 月次ブラックリストIPアドレスTOP 10

2021年04月も先月と同じく中国の送信元のIPが約半分を占めていてシェアとして一番高い。その次、アメリカ、インド、アルバニア、ロシアが新たに順位に登場したことが確認できる。

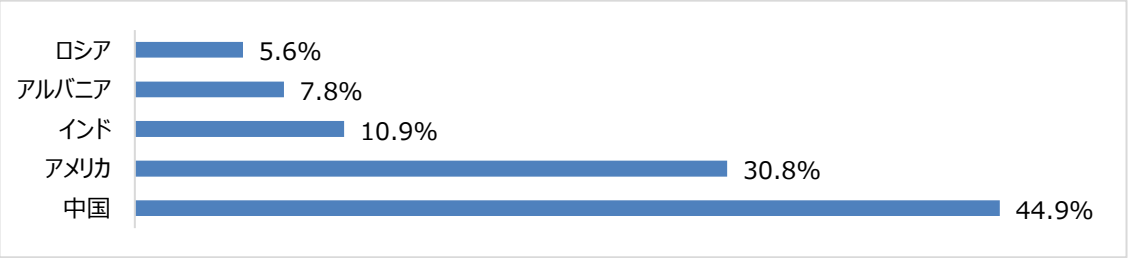
当該の送信元IPの危険性は独自調査で確認した結果である。

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	攻撃情報
1	45.146.165.157	RU	ThinkPHP Remote Code Execution Vulnerability
2	45.155.205.225	RU	ThinkPHP Remote Code Execution Vulnerability
3	205.185.122.102	US	Command Injection
4	45.146.165.165	RU	XML External ENTITY Injection
5	209.141.46.206	US	MVPower DVR Shell Unauthenticated Command Execution
6	31.210.20.175	US	Code Execution (Bash ShellShock)
7	107.189.8.176	US	Netlink GPON Router Remote Code Execution
8	18.237.5.42	US	Application Vulnerability (PHPUnit)
9	210.108.70.119	KR	Apache Struts2 Jakarta RCE (CVE-2017-5638)
10	185.204.1.210	FI	Application Vulnerability (PHPUnit)

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	45.146.165.157	RU
2	45.155.205.225	RU
3	205.185.122.102	US
4	45.146.165.165	RU
5	209.141.46.206	US

Rank	Source IP	Country
6	31.210.20.175	US
7	107.189.8.176	US
8	18.237.5.42	US
9	210.108.70.119	KR
10	185.204.1.210	FI

攻撃パターン毎の詳細分析結果

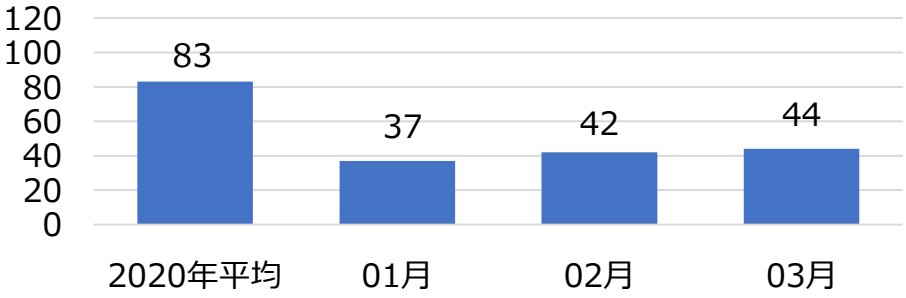
04月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
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。
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。
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。
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。
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)はウェブサーバの設定ページもしくは、許可メソッド、非認可ウェブページ、非許可ポートなど、脆弱なところの存在有無を確認するために使用する。
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。
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した値で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。

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03月の1か月間共有されたサイバー脅威検知ポリシーは44件である。
03月の1か月間MS Exchange(CVE-2021-26855), Dewmode Webshell, F5機器(CVE-2021-22986) 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

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.1.04918 MS, Exchange, CVE-2021-26855, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/owa/auth/"; fast_pattern:only; http_uri; content:"X-BEResource="; nocase; http_cookie; pcre:"/X-BEResource=[^¥x3b]*?([¥x5d¥x40¥x23]|:444)/Ci"; sid:104918;)	MS Exchangeの CVE-2021-26855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, Exchange, CVE-2021-26855
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.04919 MS, Exchange, CVE-2021-26855, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/ecp/"; fast_pattern:only; http_uri; content:"X-AnonResource-Backend="; nocase; http_cookie; pcre:"/X-AnonResource-Backend=[^¥x3b]*?([¥x5d¥x40¥x23]|:444)/Ci"; sid:104919;)	MS Exchangeの CVE-2021-26855脆弱性を悪用した管理者権限奪取を検知するポリシー	MS, Exchange, CVE-2021-26855
alert tcp $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"IGRSS.2.04930 Webshell, DEWMODE, Attempted User Privilege Gain"; flow:to_client,established; file_data; content:"Cleanup Shell"; fast_pattern:only; content:"?csrftoken="; nocase; content:"<th>file_id</th>"; distance:0; nocase; sid:204930;)	Dewmode Webshellのネットワーク通信を検知するポリシー	Webshell, DEWMODE
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.04939 WebApp, F5 iControl, CVE-2021-22986, Web Application Attack"; flow:to_server,established; content:"/mgmt/shared/authn/login"; fast_pattern:only; http_uri; content:"|22|loginReference|22|"; nocase; http_client_body; content:"|22|userReference|22|"; nocase; http_client_body; sid:1004939;)	F5機器 CVE-2021-22986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	WebApp, F5 iControl, CVE-2021-22986

月間重要検知ポリシー