CyberFortress Report

2021
JUN

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。

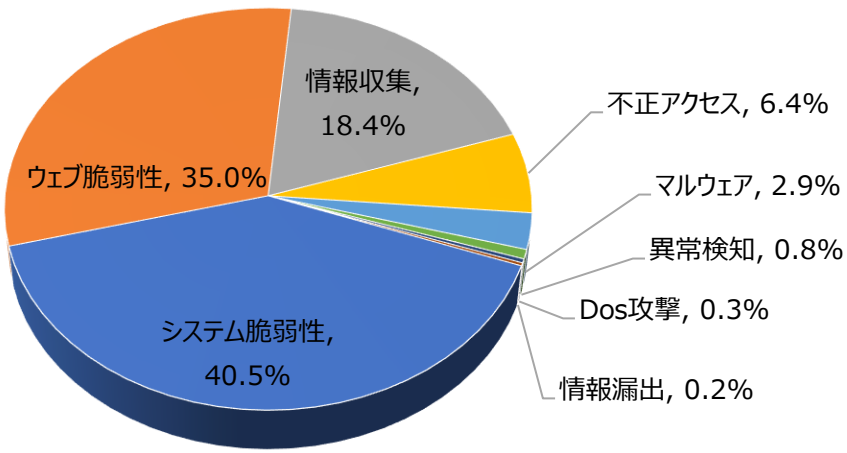
月次攻撃サービスの統計及び分析 - 2021年06月

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)	40.5	▲1
ウェブ脆弱性(Web Vulnerability)	30.5	▼1
情報収集(Information Gathering)	18.4	-
不正アクセス(Unauthorized access)	6.4	-
マルウェア(Malware)	2.9	-
異常検知(Anomaly Detection)	0.8	-
情報漏洩(Information Exposure)	0.3	-
Dos攻撃(Denial of service attack)	0.2	-

2021年06月の月次攻撃の類型を確認した結果、Gpon, Netgear, D-linkなどネットワーク機器に関するCommand Injection攻撃**が増加し**システム脆弱性(System Vulnerability)の比率が増加、ウェブ脆弱性(Web Vulnerability)を越えて1位になった。

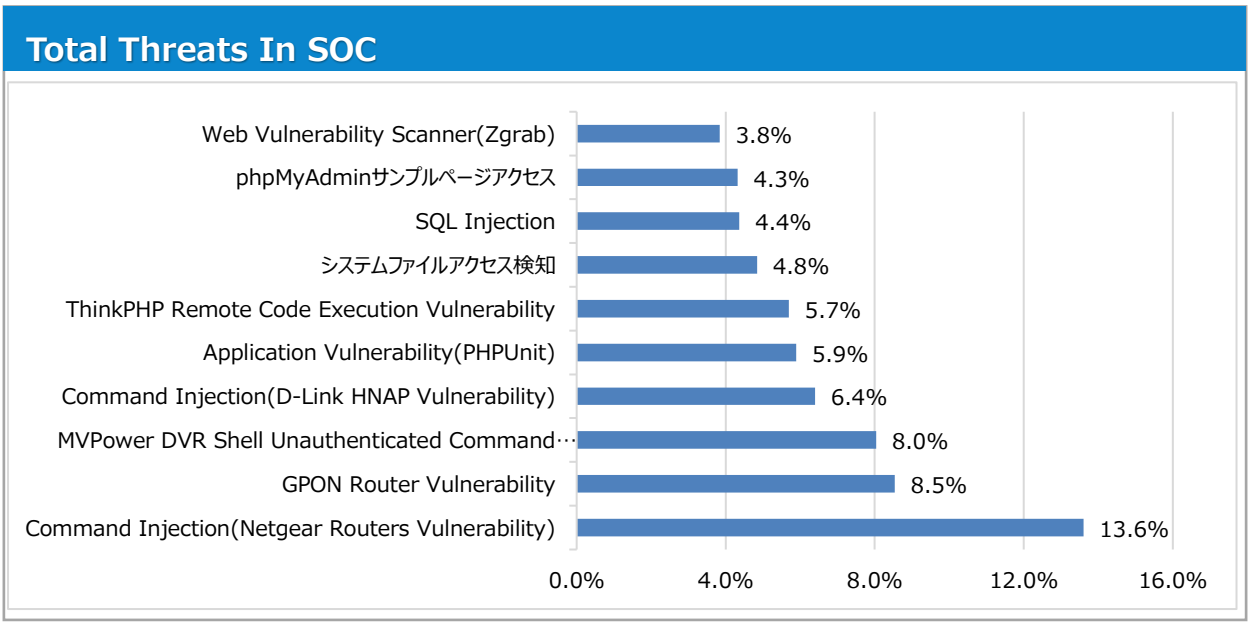


月次攻撃サービスの統計及び分析 - 2021年06月

02. 月次脆弱性攻撃TOP10

2021年06月の月次脆弱性攻撃TOP10を確認した結果、SQL injection、phpMyAdminサンプルページアクセス脆弱性が新たにTOP10に登場し、先月と比べてCommand Injectionに関する攻撃の順位が上昇した。

順位	検知名	比率(%)	比較
1	Command Injection(Netgear Routers Vulnerability)	13.6	-
2	GPON Router Vulnerability	8.5	▲2
3	MVPower DVR Shell Unauthenticated Command Execution	8.0	▲2
4	Command Injection(D-Link HNAP Vulnerability)	6.4	▲2
5	Application Vulnerability(PHPUnit)	5.9	▼3
6	ThinkPHP Remote Code Execution Vulnerability	5.7	▼3
7	システムファイルアクセス検知	4.8	▲2
8	SQL Injection	4.4	NEW
9	phpMyAdminサンプルページアクセス	4.3	NEW
10	Web Vulnerability Scanner(Zgrab)	3.8	-



月次攻撃サービスの統計及び分析 - 2021年06月

03. 月次ブラックリストIPアドレスTOP 10

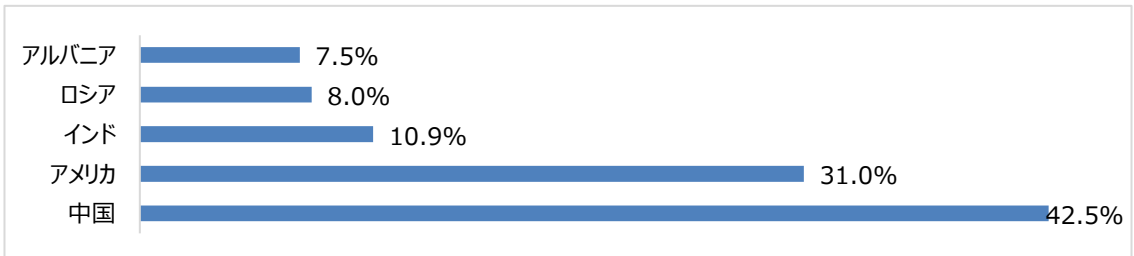
2021年06は月アメリカとインドからの攻撃が増加し順位が上がり、先月2位だったロシアの攻撃が比較的に減少し、5位になった。

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	45.146.164.125	RU	ThinkPHP Remote Code Execution Vulnerability
2	45.155.205.181	RU	ThinkPHP Remote Code Execution Vulnerability
3	209.141.33.232	US	MVPower DVR Shell Unauthenticated Command Execution
4	5.188.210.4	RU	FCKeditorサンプルページアクセス
5	210.108.70.119	KR	Apache Struts2 Jakarta RCE (CVE-2017-5638)
6	45.155.205.109	RU	ThinkCMF Remote Code Execution Vulnerability
7	185.53.90.19	BZ	Alcatel-Lucent OmniPCX MasterCGI Command Execution
8	199.116.118.198	US	etcpasswd Detect
9	51.159.7.190	FR	Web Scanner(ZmEu)
10	77.247.108.42	BZ	Network Scanner(masscan)

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	45.146.164.125	RU
2	45.155.205.181	RU
3	209.141.33.232	US
4	5.188.210.4	RU
5	210.108.70.119	KR

Rank	Source IP	Country
6	45.155.205.109	RU
7	185.53.90.19	BZ
8	199.116.118.198	US
9	51.159.7.190	FR
10	77.247.108.42	BZ

攻撃パターン毎の詳細分析結果

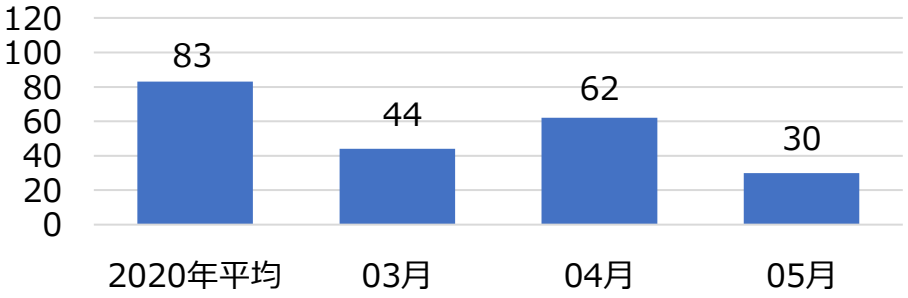
06月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
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 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。
Application Vulnerability(PHPUnit)	PHPUnitはユニットテストフレームワークで/phpunit/src/Util/PHP/eval-stdin.phpファイルに存在する脆弱性を利用してリモートで任意のコードが実行できる。攻撃者は<?phpの文字列から始まるHTTP POSTデータで任意のPHPコードが実行できる。
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。
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。

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05月の1か月間共有されたサイバー脅威検知ポリシーは30件である。
05月の1か月間Cryptomining, Cobolt Strike不正ソフトウェア使用及びMS Windows(CVE-2021-31166), MS Exchange(CVE-2020-0688)に関する検知ポリシーが配布された。



3か月間件数

4,997
全体配布量

30
今月配布量

62
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.16.05005 Malware, cryptomining, Misc Attack"; flow:to_server,established; content:"/owa/auth/win_"; fast_pattern:only; http_uri; content:".zip"; nocase; http_uri; sid:1605005;)	Cryptomining Malwareの ネットワーク通信を検知するポリシー	Malware, cryptomining
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05011 MS, Windows, CVE-2021-31166, Attempted User Privilege Gain"; flow:to_server,established; content:"Accept-Encoding:"; nocase; http_header; content:"Accept-Encoding: |0A|"; distance:0; nocase; http_header; sid:205011;)	MS Windowsの CVE-2021-31166の脆弱性を悪用した ユーザーの権限奪取試し を検知するポリシー	MS, Windows, CVE-2021-31166
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.05030 MS, Exchange, CVE-2020-0688, Attempted Administrator Privilege Gain"; flow:to_server,established; urilen:>500; content:"/ecp/"; nocase; http_uri; content:"__VIEWSTATE="; fast_pattern; nocase; http_uri; base64_decode:bytes 2000,offset 0,relative; base64_data; content:"ActivitySurrogateSelector"; within:2000; nocase; sid:105030;)	MS Exchangeの CVE-2020-0688脆弱性を悪用した 管理者権限奪取試し を検知するポリシー	MS, Exchange, CVE-2020-0688
alert udp $HOME_NET any -> any 53 (msg:"IGRSS.8.05034 Malware, Cobalt Strike, A Network Trojan was detected"; flow:to_server; content:"|03|aaa|05|stage"; nocase; content:"|00 00 10 00 01|"; distance:0; sid:805034;)	Cobalt StrikeのDNSに関する不正行為 を検知するポリシー	Malware, Cobalt Strike