CyberFortress Report

2021
MAY

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

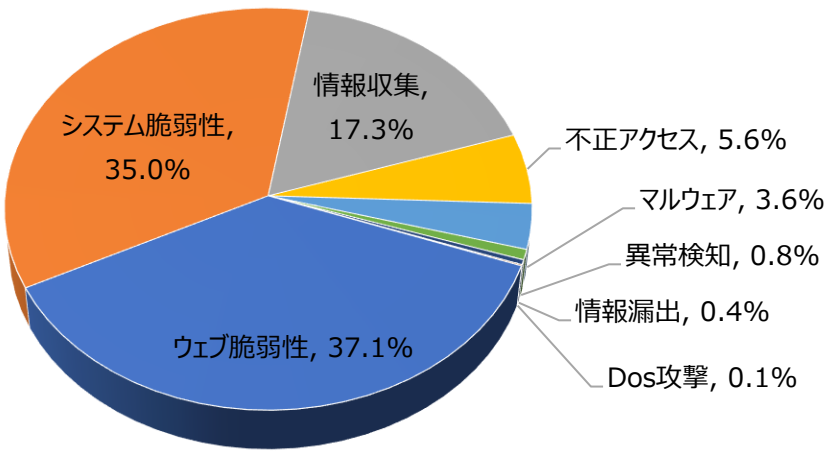
株式会社サイバーフォートレスでは攻撃情報を収集し、分析しています。
分析内容から、月次攻撃類型、脆弱性攻撃、ブラックリストのTOP10を確認し、過去データと比較し、攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てていただければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
ウェブ脆弱性(Web Vulnerability)	37.1	▲1
システム脆弱性(System Vulnerability)	35.0	▼1
情報収集(Information Gathering)	17.3	-
不正アクセス(Unauthorized access)	5.6	-
マルウェア(Malware)	3.6	-
異常検知(Anomaly Detection)	0.8	-
情報漏洩(Information Exposure)	0.4	-
Dos攻撃(Denial of service attack)	0.1	-

[表1-1] 月次攻撃類型

2021年5月の月次攻撃の類型を確認した結果、4月から増加したウェブ脆弱性(Web Vulnerability)の比率がシステム脆弱性(System Vulnerability)の比率を上回って1位になった。
先月と同じくPHPに関する攻撃が増加した影響と判断できる。その他の順位は先月と同一である。

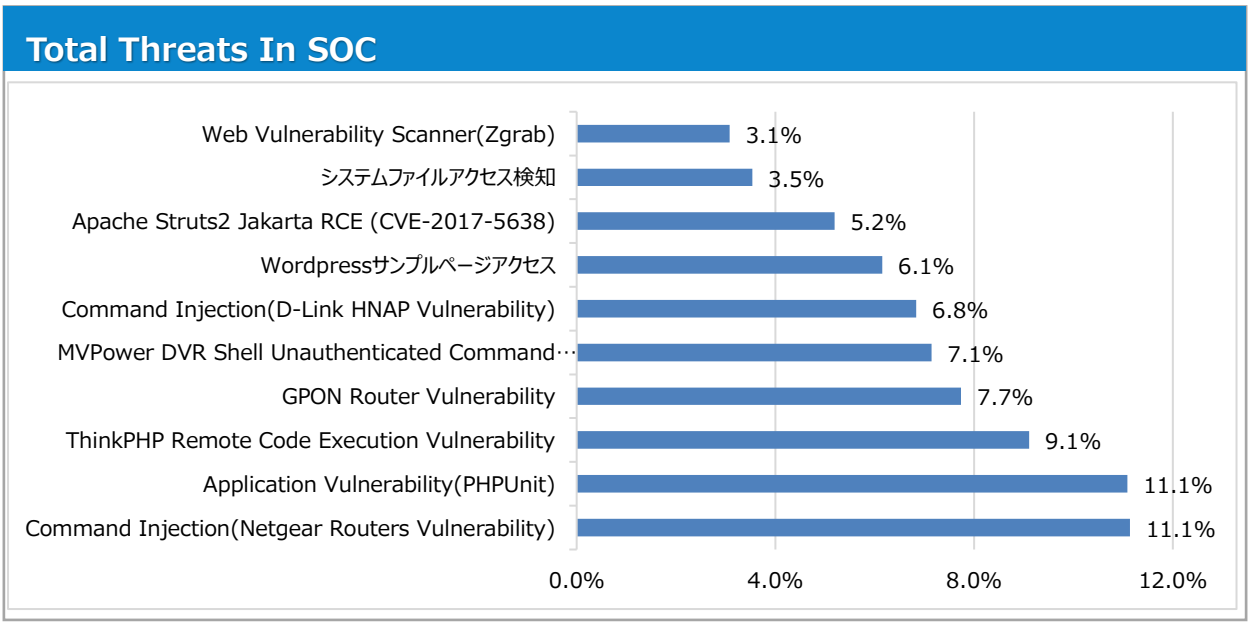


月次攻撃サービスの統計及び分析 - 2021年05月

02. 月次脆弱性攻撃TOP10

2021年05月の月次脆弱性攻撃TOP10を確認した結果、Apache Struts2 Jakarta RCE (CVE-2017-5638)脆弱性が新たにTOP10に登場し、先月と同じくウェブ脆弱性に関する攻撃が上位になっていることが確認できる。

順位	検知名	比率(%)	比較
1	Command Injection(Netgear Routers Vulnerability)	11.1	-
2	Application Vulnerability(PHPUnit)	11.1	▲1
3	ThinkPHP Remote Code Execution Vulnerability	9.1	▼1
4	GPON Router Vulnerability	7.7	-
5	MVPower DVR Shell Unauthenticated Command Execution	7.1	▲2
6	Command Injection(D-Link HNAP Vulnerability)	6.8	▲1
7	Wordpressサンプルページアクセス	6.1	▼2
8	Apache Struts2 Jakarta RCE (CVE-2017-5638)	5.2	NEW
9	システムファイルアクセス検知	3.5	-
10	Web Vulnerability Scanner(Zgrab)	3.1	▼2



月次攻撃サービスの統計及び分析 - 2021年05月

03. 月次ブラックリストIPアドレスTOP 10

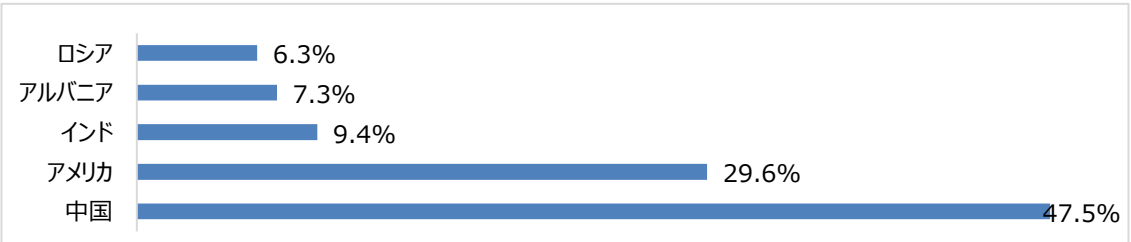
2021年05月も先月と同じく中国からの送信元IPが一番高くシェアし、比率の約半分を占めている。また、同じロシアからのIPも上位になっている。当該の送信元IPの危険性は独自調査で確認した結果である。

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	45.155.205.211	RU	Application Vulnerability(PHPUnit)
2	45.155.205.27	RU	Application Vulnerability(PHPUnit)
3	45.155.205.151	RU	Application Vulnerability(PHPUnit)
4	45.155.205.84	RU	Application Vulnerability(PHPUnit)
5	45.148.10.50	NL	Application Vulnerability(PHPUnit)
6	103.73.162.180	HK	Cross Site Script(XSS)
7	51.38.40.95	FR	Application Vulnerability(PHPUnit)
8	103.149.200.47	HK	Cross Site Script(XSS)
9	49.143.32.6	KR	Command Injection(Netgear Routers Vulnerability)
10	45.144.225.244	US	FCKeditor サンプルページアクセス

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	45.155.205.211	RU
2	45.155.205.27	RU
3	45.155.205.151	RU
4	45.155.205.84	RU
5	45.148.10.50	NL

Rank	Source IP	Country
6	103.73.162.180	HK
7	51.38.40.95	FR
8	103.149.200.47	HK
9	49.143.32.6	KR
10	45.144.225.244	US

攻撃パターン毎の詳細分析結果

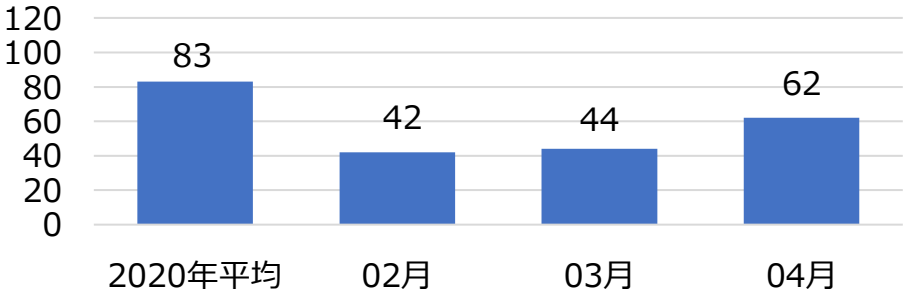
05月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
Application Vulnerability(PHPUnit)	PHPUnitは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でリモートから任意のコードが実行できる。 攻撃者は「<?php」文字列に始まるHTTP POSTデータを通じて任意の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。
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。
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。
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。
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。
Apache Struts2 Jakarta RCE (CVE-2017-5638)	Apache Struts2のJakartaプラグインを利用してファイルアップロードを処理する際、攻撃者はHTTP RequestヘッダーのContent-Type値にOGNL(Object Graph Navigation Language)表現式を利用てリモートコードが実行できる。
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。
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04月の1か月間共有されたサイバー脅威検知ポリシーは62件である。
04月の1か月間PAS Webshell, CtitX Exploit kit, SLIGHTPULSE, HARDPLUSE Malware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 $HOME_NET $HTTP_PORTS -> $EXTERNAL_NET any (msg:"IGRSS.8.04943 Webshell, PAS, A Network Trojan was detected"; flow:to_client,established; file_data; content:"<form action=|22 22| method=|22|post|22|><input type=|22|text|22| name=|22|"; depth:55; content:"|22| value=|22 22|/><input type=|22|submit|22| value=|22|>|3B 22|/></form>"; within:54; distance:5; fast_pattern; isdataat:!1,relative; pcre:"/<form action=¥x22¥x22 method=¥x22post¥x22><input type=¥x22text¥x22 name=¥x22[a-z_]{5}¥x22/"; sid:804943;)	PAS Webshellの ネットワーク通信を検知するポリシー	Webshell, PAS
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"IGRSS.8.04951 Exploit kit, CritX, A Network Trojan was detected"; flow:to_server,established; content:"/load"; http_uri; content:".php"; distance:0; http_uri; pcre:"/¥/load(?:(?:db|rh|silver|msie|flash|fla[0-9]{4,5}))¥.php/U"; flowbits:set,file.exploit_kit.pe; sid:804951;)	CtitX Exploit kitの ネットワーク通信を検知するポリシー	Exploit kit, CritX
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.04989 Malware, SLIGHTPULSE, A Network Trojan was detected"; flow:to_server,established; content:"/meeting_testjs.cgi"; fast_pattern:only; http_uri; content:"POST"; http_method; pcre:"/(^|&)(name|img|cert)=/Pim"; sid:804989;)	SLIGHTPULSE Malwareの ネットワーク通信を検知するポリシー	Malware, SLIGHTPULSE
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.04993 Malware, HARDPULSE, A Network Trojan was detected"; flow:to_server,established; content:"/compcheckjava.cgi"; fast_pattern:only; http_uri; content:"hashid="; nocase; http_client_body; content:"checkcode="; nocase; http_client_body; sid:804993;)	HARDPLUSE Malwareの ネットワーク通信を検知するポリシー	Malware, HARDPULSE

月間重要検知ポリシー