CyberFortress Report

2021
FEB

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02月

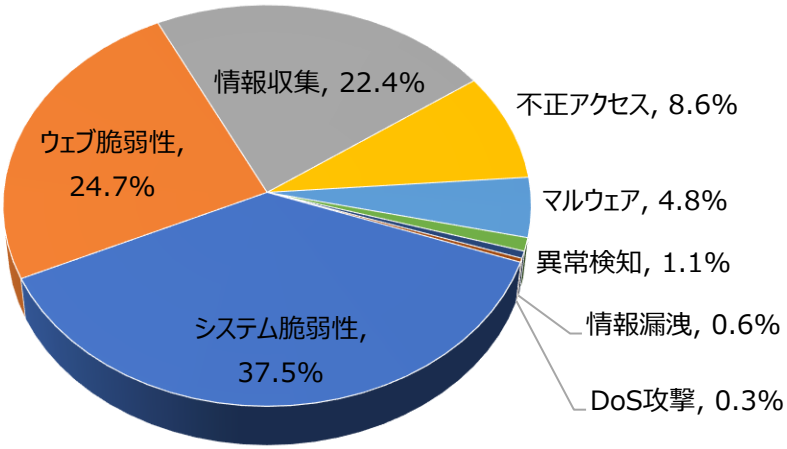
株式会社サイバーフォートレスでは攻撃サービス(ポート)情報を収集し、分析しています。
分析内容から、月次攻撃サービス（ポート）、月次攻撃サービスパターンのTOP10を確認し、過去データと比較し、攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てていただければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	37.5	-
ウェブ脆弱性(Web Vulnerability)	24.7	-
情報収集(Information Gathering)	22.4	-
不正アクセス(Unauthorized access)	8.6	-
マルウェア(Malware)	4.8	-
異常検知(Anomaly Detection)	1.1	-
情報漏洩(Information Exposure)	0.6	-
DoS攻撃(Denial of service attack)	0.3	-

[表1-1] 月次攻撃類型

2021年02月の月次攻撃の類型を確認した結果、 先月と同じ順位の結果が確認できた。システム脆弱性(System Vulnerability)が1位を占めていて、これは月次脆弱性のTop10の中でCommnad Injection関連の脆弱性が多い影響だと判断される。
そのあと、ウェブ脆弱性(Web Vulnerability)と情報収集(Information Gathering)順になっている。

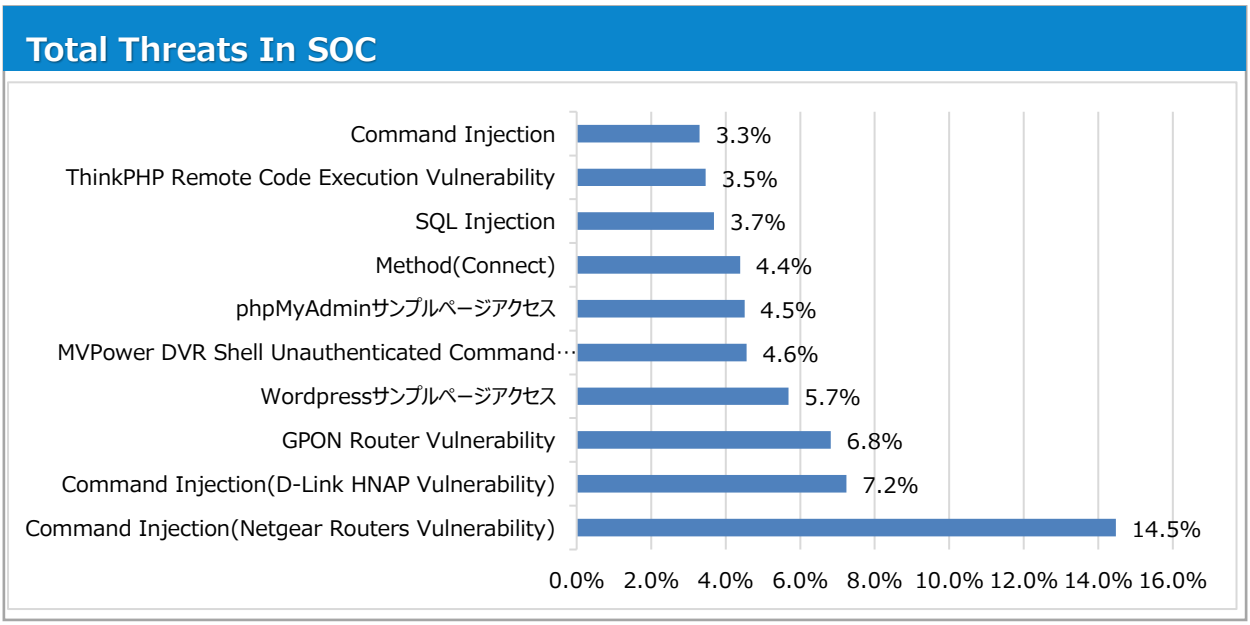


月次攻撃サービスの統計及び分析 - 2021年02月

02. 月次脆弱性攻撃TOP10

2021年02月の月次脆弱性攻撃TOP10を確認した結果、SQL Injection, ThinkPHP Remote Code Execution Vulnerability脆弱性が新たにTop10に登場した。
その他、GPON Router Vulnerability, phpMyAdminサンプルページアクセスの順位下落及びWordpressサンプルページアクセス脆弱性の急上昇が確認できた。

順位	検知名	比率(%)	比較
1	Command Injection (Netgear Routers Vulnerability)	14.5	-
2	Command Injection(D-Link HNAP Vulnerability)	7.2	▲1
3	GPON Router Vulnerability	6.8	▼1
4	Wordpressサンプルページアクセス	5.7	▲6
5	MVPower DVR Shell Unauthenticated Command Execution	4.6	▲2
6	phpMyAdminサンプルページアクセス	4.5	▼2
7	Method(Connect)	4.4	▲2
8	SQL Injection	3.7	NEW
9	ThinkPHP Remote Code Execution Vulnerability	3.5	NEW
10	Command Injection	3.3	▼2



月次攻撃サービスの統計及び分析 - 2021年02月

03. 月次ブラックリストIPアドレスTOP 10

2021年02月の基準で送信元IP TOP10は中国のIPが過半数以上を占めている。その次にロシア、インド、アメリカ、韓国の順になっている。

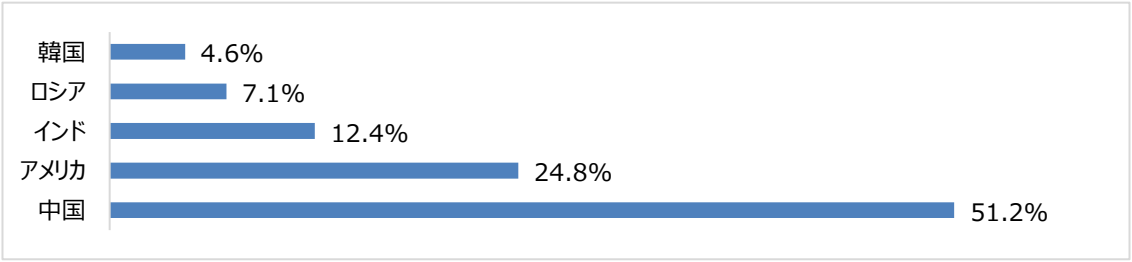
当該の送信元IPの危険性は独自観点での調査で確認した結果である。

下記の表を参考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	45.155.205.108	RU	ThinkPHP Remote Code Execution Vulnerability
2	89.248.170.31	GB	ThinkPHP Remote Code Execution Vulnerability
3	199.19.226.67	US	Web Scanner(ZmEu)
4	89.248.162.235	GB	Web Scanner(ZmEu)
5	43.229.62.95	AU	Network Scanner(masscan)
6	97.74.229.113	US	Admin (管理者) ページアクセス
7	103.78.208.100	ID	Network Scanner(masscan)
8	89.248.168.108	GB	Restriction Method(制限されたメソッド使用)
9	211.211.195.105	KR	XML External ENTITY Injection
10	72.251.228.101	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	45.155.205.108	RU
2	89.248.170.31	GB
3	199.19.226.67	US
4	89.248.162.235	GB
5	43.229.62.95	AU

Rank	Source IP	Country
6	97.74.229.113	US
7	103.78.208.100	ID
8	89.248.168.108	GB
9	211.211.195.105	KR
10	72.251.228.101	US

攻撃パターン毎の詳細分析結果

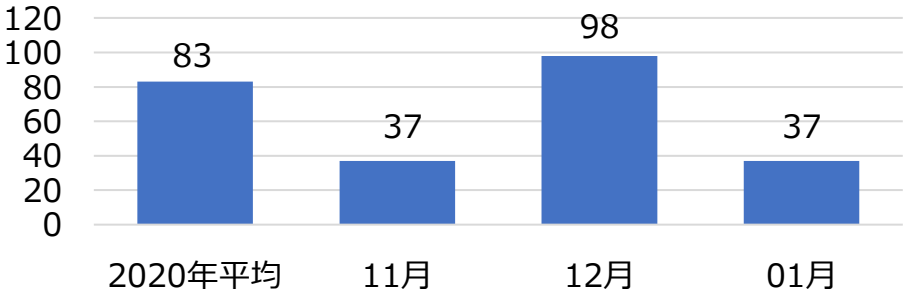
2月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
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。
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。
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。
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。
Method(Connect)	Connect Methodを利用してHTTP TLS(Transport Layer Security)トンネリングは内部にアクセスをする。このため、Connect Methodを使用していて、脆弱性が存在する場合、中間経由地として使用される可能性がある。
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。
ThinkPHP Remote Code Execution Vulnerability	ThinkPHPの脆弱な文字フィルタリングによって不適切なコントローラクラスが呼び出されてリモートコード実行攻撃が可能な脆弱性である。¥think¥*クラスを呼び出して脆弱なオブジェクトを通じて攻撃者は任意のPHPコード及びシステムコマンドが実行できる。
Command Injection	システムコマンドが含まれている入力値が適切な検証プロセスを通らない場合、入力されたコマンドが実行しうる。この脆弱性が存在する場合、攻撃者がシステムに直接コマンド送信できるため、ファイルの閲覧、ダウンロード、実行などで追加被害が発生する可能性がある。

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01月の1か月間共有されたサイバー脅威検知ポリシーは37件である。
01月の1か月間Fireeye Red Team Tool, Solarwindsハッキングインシデントに関する検知ポリシー及び Apache Struts(CVE-2020-17530), MS Windows SMB(CVE-2020-17096)脆弱性に関する検知ポリシーが配布された。



3か月間の配布件数

4,819
全体配布量

37
今月配布量

98
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 -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.04820 SolarWinds, Orion API, CVE-2020-10148, Web Application Attack"; flow:to_server,established; content:"i18n.ashx"; fast_pattern:only; http_uri; content:"&v="; nocase; http_uri; sid:1004820;)	SolarWinds Orion APIのCVE-2020-10148 脆弱性を悪用したウェブアプリケーション認証バイパス攻撃を検知するポリシー	SolarWinds, Orion API, CVE-2020-10148
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.04831 Cisco, Jabber, CVE-2020-26085, Attempted User Privilege Gain"; flow:to_server,established; content:"/CLIENT_REQUEST"; fast_pattern:only; http_uri; content:"onanimationstart"; nocase; http_client_body; sid:204831;)	Cisco JabberのCVE-2020-26085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	Cisco, Jabber, CVE-2020-26085
alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.04837 Webshell, BumbleBee, A Network Trojan was detected"; flow:to_client,established; file_data; content:"<%if(Ntody(Request.QueryString[|22|parameter|22|])==|22|"; fast_pattern:only; sid:804837;)	BumbleBee Webshellのネットワーク通信を検知するポリシー	Webshell, BumbleBee
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.04844 Malware, Trickbot, A Network Trojan was detected"; flow:to_server,established; file_data; content:"|2C E7 6A B3 CE 43 A8 23 3F 8B BF 86 1B 6B 78 4D DA 8C 38 2B A4 F5 26 27 0B 1E 6D DF 70 85 8B FC|"; fast_pattern:only; sid:804844;)	Trickbot Malwareのネットワーク通信を検知するポリシー	Malware, Trickbot

月間重要検知ポリシー