CyberFortress Report

2021
JAN

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01月

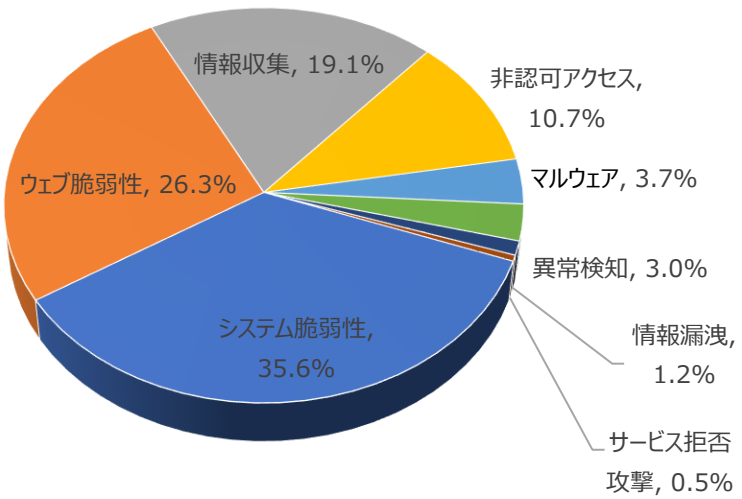
株式会社サイバーフォートレスでは攻撃サービス(ポート)情報を収集し、分析しています。
分析内容から、月次攻撃サービス（ポート）、月次攻撃サービスパターンのTOP10を確認し、過去データと比較し、攻撃トレンドへの対策を考えます。
セキュリティ担当者または、システム管理者はこのようなデータ分析を活用してサイバー脅威の予測に役立てていただければと思います。

01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	35.6	-
ウェブ脆弱性(Web Vulnerability)	26.3	-
情報収集(Information Gathering)	19.1	-
不正アクセス(Unauthorized access)	10.7	▲1
マルウエア(Malware)	3.7	▼1
異常検知(Anomaly Detection)	3.0	-
情報漏洩(Information Exposure)	1.2	-
DoS攻撃(Denial of service attack)	0.5	-

[表1-1] 月次攻撃類型

2021年01月の月次攻撃の類型を確認した結果、システム脆弱性(System Vulnerability)が月次攻撃の類型の中で一番大きく比率を占めている。その次はウェブ脆弱性と情報収集になっている。
先月と比べると不正アクセスが多くなっており、マルウェアについては、減少している。。これは脆弱性「Tomcat admin(管理者)ページの認証バイパス試し」と「システムファイルアクセス検知」の増加による影響だと判断される。



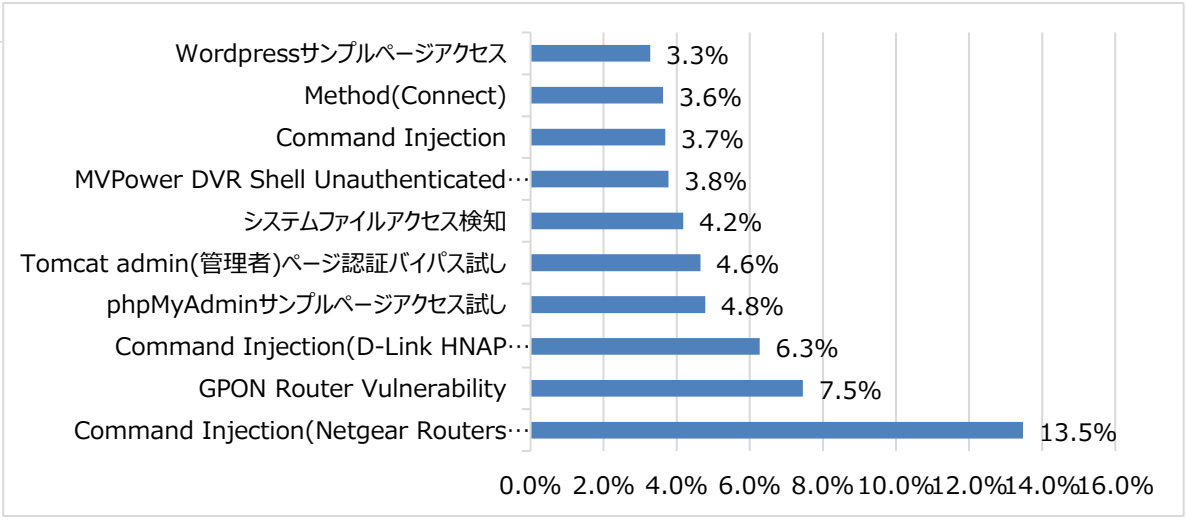
月次攻撃サービスの統計及び分析 - 2021年01月

02. 月次脆弱性攻撃TOP10

2021年01月の月次脆弱性攻撃TOP10を確認した結果、Tomcat admin(管理者)ページ認証バイパス試しとシステムファイルアクセス検知、Method(Connect)脆弱性が新たにTOP10に登場した。
その他、MVPower DVR Shell Unauthenticated Command Execution, Command Injectionの順位の上昇とWordpressサンプルページアクセスの順位の急落が確認できた。

順位	検知名	比率(%)	比較
1	Command Injection (Netgear Routers Vulnerability)	13.5	-
2	GPON Router Vulnerability	7.5	-
3	Command Injection(D-Link HNAP Vulnerability)	6.3	-
4	phpMyAdmin サンプルページアクセス	4.8	-
5	Tomcat admin(管理者)ページ 認証バイパス試し	4.6	NEW
6	システムファイルアクセス検知	4.2	NEW
7	MVPower DVR Shell Unauthenticated Command Execution	3.8	▲1
8	Command Injection	3.7	▲1
9	Method(Connect)	3.6	NEW
10	Wordpressサンプルページアクセス	3.3	▼6

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2021年01月

03. 月次ブラックリストIPアドレスTOP 10

2021年01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。その次にアメリカ、インド、ロシア、韓国の順になっている。

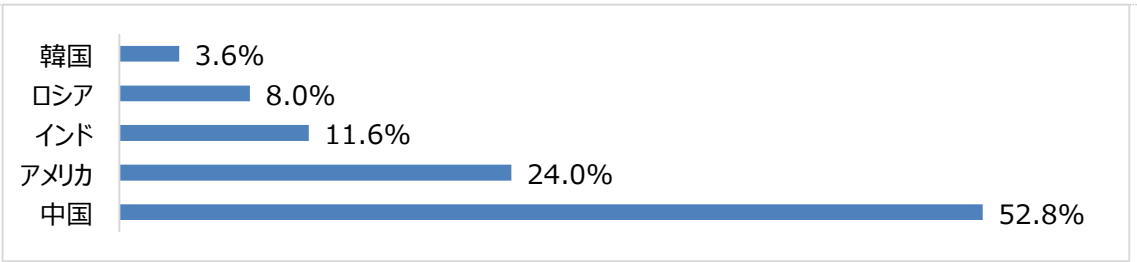
当該の送信元IPの危険性はIGLOO_CTI情報，OSINT情報から確認した結果である。（IGLOOは弊社パートナー会社）

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	91.241.19.84	RU	4/114	ThinkPHP Remote Code Execution Vulnerability
2	45.155.205.108	RU	14/114	ThinkPHP Remote Code Execution Vulnerability
3	45.146.164.15	RU	7/114	ThinkPHP Remote Code Execution Vulnerability
4	85.214.44.193	DE	8/114	Code Execution(Bash ShellShock)
5	185.234.217.183	IE	12/114	etcpasswd Detect
6	149.129.139.48	SG	8/114	ZeroShell kerbynet RCE (CVE-2009-0545)
7	209.141.50.5	US	9/114	Web Scanner(ZmEu)
8	185.234.219.28	IE	14/114	etcpasswd Detect
9	137.116.133.111	SG	10/114	ZeroShell kerbynet RCE (CVE-2009-0545)
10	208.91.198.220	US	0/114	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	91.241.19.84	RU
2	45.155.205.108	RU
3	45.146.164.15	RU
4	85.214.44.193	DE
5	185.234.217.183	IE

Rank	Source IP	Country
6	149.129.139.48	SG
7	209.141.50.5	US
8	185.234.219.28	IE
9	137.116.133.111	SG
10	208.91.198.220	US

攻撃パターン毎の詳細分析結果

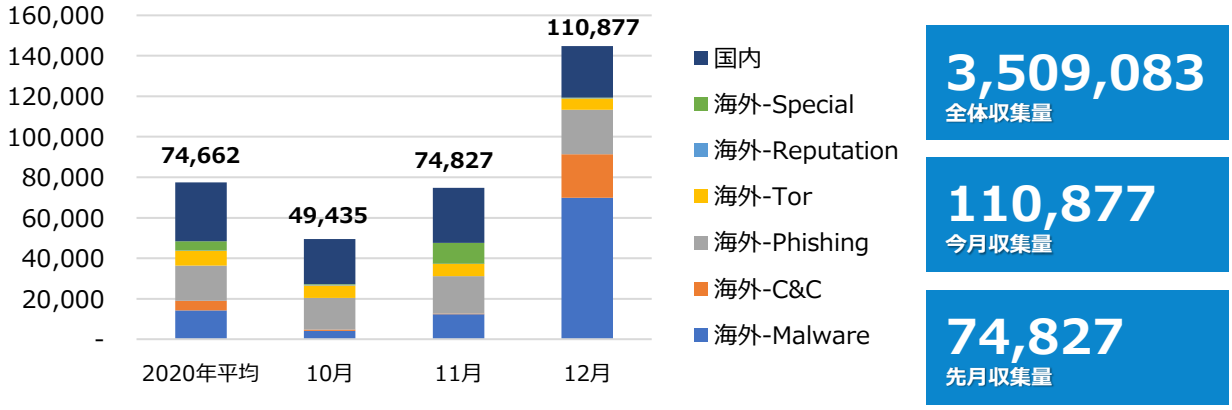
01月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

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。
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。
Tomcat admin(管理者)ページ認証」バイパス試し	WASの一つであるTomcatをインストール後、デフォルトパスでアクセスできる管理者ページ(e.g http://localhost:8080/manager, http://localhost:8080/manager/htmlなど)にアクセスして認証ヘッダーにデフォルトのID, PWをBase64にエンコードしてアクセスする攻撃で、認証のバイパスに成功した場合、ウェブシェルのアップロード、サーバシェルの権限獲得、exploitによるroot権限の取得ができる。
システム ファイル アクセス検知	攻撃者はシステム情報を獲得するためにDirectory Traversalの脆弱性を利用して「/etc/passwd」や「*.conf /.env」のようなアカウント、環境変数などの設定情報が入っている重要システムファイルにアクセスを試みる。
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。
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。
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。
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。

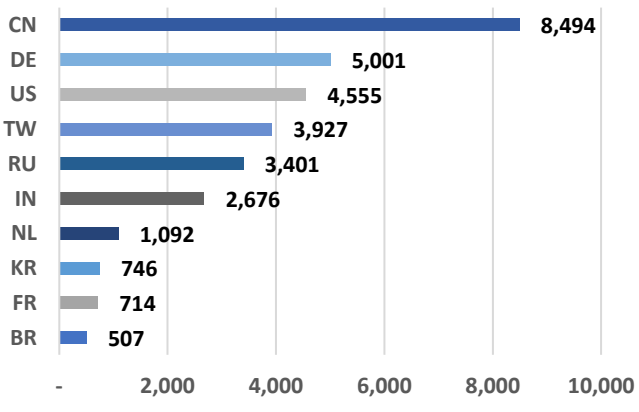
侵害指標(IOC)

▶. グローバル月間脅威情報収集統計

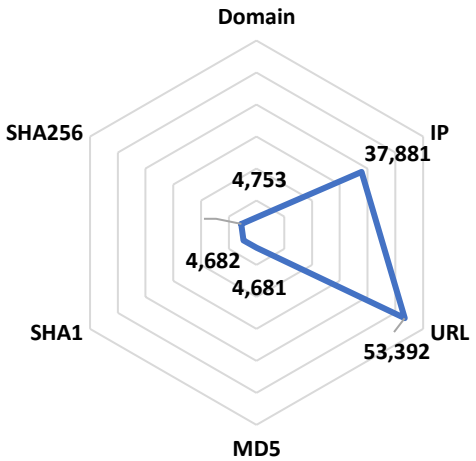
2020年12月の1か月間グローバルにデータを見ると4週間目に幅広く増加したことが確認でき、海外のOSINTデータの収集が高くなっている。
海外-Phishingデータの増加によるURL IoCが幅広く増加されたと判断できる。



此処3か月間のグローバル脅威情報収集件数



ブラックリストIP国別現況

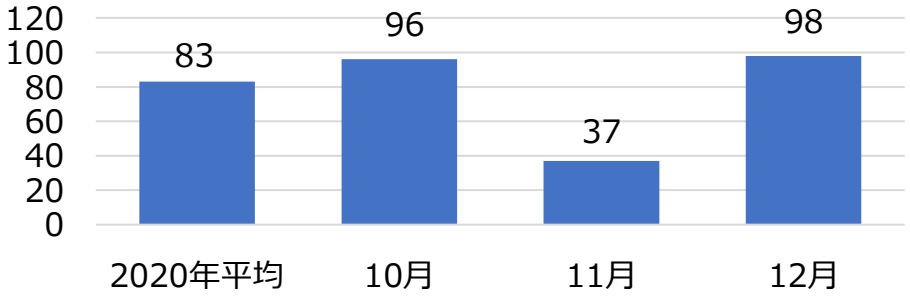


IoC毎、収集現況

検知ポリシー

▶. 月間サイバー脅威検知ポリシー統計

2020年12月の1か月間配布されたサイバー脅威検知ポリシーは98件である。
12月の1か月間Fireeye Red Team Tool, Solarwindsハッキング事項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か月間件数

4,802
全体配布量

98
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 any $HTTP_PORTS -> any any (msg:"IGRSI.20.04732 Fireeye, Red team tool, HTTP.BEACON, Large Scale Information Leak"; flow:to_server,established; content:"HTTP/1."; depth:7; content:"Connection: close"; content:"Content-Type: application/json¥; charset=utf-8"; content:"Content-Security-Policy: upgrade-insecure-requests"; content:"Strict-Transport-Security: max-age=10890000"; content:"Cache-Control: public, immutable, max-age=315360000"; content:"Accept-Ranges: bytes"; content:"X-Cache: HIT, HIT"; content:"X-Timer: S1593010188.776402,VS0,VE1"; content:"Vary: X-AbVariant, X-AltUrl, Accept-Encoding"; sid:2004732;)	Fireeye Red Team Tool漏出関連 HTTP.BEACON検知ポリシー	Fireeye, Red team tool, HTTP.BEACON
alert tcp $HOME_NET any -> any any (msg:"IGRSI.20.04765 Fireeye, Solarwinds, MSIL.SUNBURST, Large Scale Information Leak"; flow:to_server,established; content:"T "; offset:2; depth:3; content:"/swip/Events HTTP/1"; within:100; content:"Host: "; content:!".solarwinds.com"; within:100; sid:2004765;)	Fireeye Solarwinds攻撃関連 MSIL.SUNBURST検知ポリシー	Fireeye, Solarwinds, MSIL.SUNBURST
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.04818 Apache Struts, CVE-2020-17530, Attempted User Privilege Gain"; flow:to_server,established; content:"${"; http_uri; content:"java.lang.ProcessBuilder"; distance:0; nocase; http_uri; sid:204818;)	Apache Struts의 CVE-2020-17530脆弱性を悪用し、ユーザーの権限奪取試しを検知するポリシー	Apache Struts, CVE-2020-17530

月間重要検知ポリシー