SECURITY REPORT

2022

NOV

2022年11月
攻撃統計情報

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 - 2022年11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頂ければと思います。

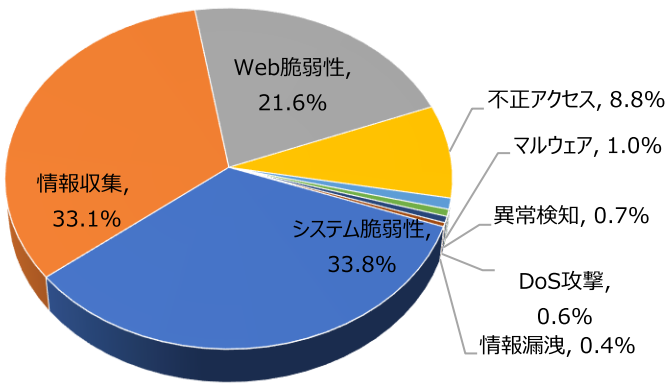
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	33.8%	-
情報収集(Information Gathering)	33.1%	▲1
Web脆弱性(Web Vulnerability)	21.6%	▼1
不正アクセス(Unauthorized access)	8.8%	-
マルウェア(Malware)	1.0%	-
異常検知(Anomaly Detection)	0.7%	-
DoS攻撃(Denial of service attack)	0.6%	-
情報漏洩(Information Exposure)	0.4%	-

2022年11月の攻撃類型を確認した結果、全体の攻撃合計が先月と比べて約1.02倍ぐらい増加しし、あまり変わりはなかった。

そのうち、システム脆弱性に関する攻撃は先月比べて約850件ほど減少し、これはMVPower DVR Shell Unauthenticated Command Execution攻撃件数の減少によるものだと確認できた。

また、情報収集関する攻撃は先月と比べて約880件ぐらい増加し、これはWeb Vulnerability Scanner(Zgrab)攻撃件数増加によるものだと確認できた。

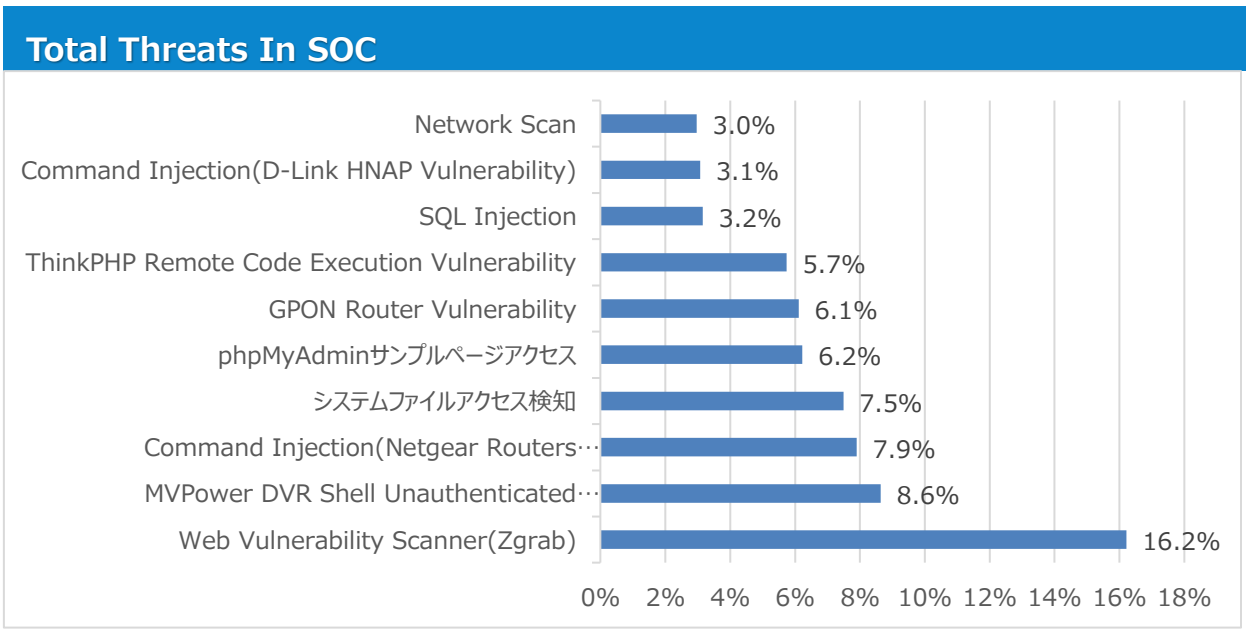


月次攻撃サービスの統計及び分析 - 2022年11月

02. 月次脆弱性攻撃TOP10

2022年11月の月次脆弱性TOP10を確認した結果、Network Scan攻撃が新たにTOP10に登場し、全体的な攻撃件数が増加したことが確認できた。特にWeb Vulnerability Scanner(Zgrab)攻撃が先月と比べて770件ぐらい大幅に増加した。

順位	検知名	比率(%)	比較
1	Web Vulnerability Scanner(Zgrab)	16.2%	▲2
2	MVPower DVR Shell Unauthenticated Command Execution	8.6%	▼1
3	Command Injection(Netgear Routers Vulnerability)	7.9%	▼1
4	システムファイルアクセス検知	7.5%	▲5
5	phpMyAdminサンプルページアクセス	6.2%	▼1
6	GPON Router Vulnerability	6.1%	▼1
7	ThinkPHP Remote Code Execution Vulnerability	5.7%	-
8	SQL Injection	3.2%	▼2
9	Command Injection(D-Link HNAP Vulnerability)	3.1%	▼1
10	Network Scan	3.0%	NEW



月次攻撃サービスの統計及び分析 - 2022年11月

03. 月次ブラックリストIPアドレスTOP 10

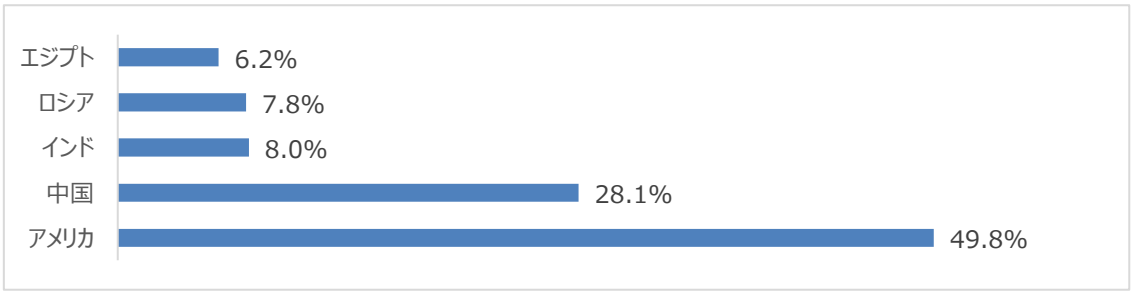
2022年11月についてTOP10を確認した結果、アメリカの攻撃比率が増加し、一方中国とインド、ロシア、エジプトの攻撃の比率は減少した。アメリカと中国の攻撃比率の合計は全体に比べて約78%で、半分以上上回って、アメリカは先月比べて約8%大幅く増加したことが確認できた。

※ 下記の表を参考にしたファイウォールやセキュリティ機器からの遮断を推奨します。

順位	ブックリストIP	国	攻撃情報
1	152.89.196.23	GB	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
2	152.89.196.211	GB	Application Vulnerability(PHPUnit)
3	185.7.214.218	RU	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
4	204.48.24.100	US	Apache Log4j RCE(CVE-2021-44228)
5	49.143.32.6	KR	GPON Router Vulnerability
6	193.142.146.35	DE	Command Injection(D-Link HNAP Vulnerability)
7	82.99.217.202	IR	Apache Log4j RCE(CVE-2021-44228)
8	123.157.222.168	CN	phpMyAdminサンプルページアクセス
9	195.178.120.33	US	Netgear Command Injection(CVE-2016-6277)
10	45.134.144.203	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	Rank	Source IP	Country
1	152.89.196.23	GB	6	193.142.146.35	DE
2	152.89.196.211	GB	7	82.99.217.202	IR
3	185.7.214.218	RU	8	123.157.222.168	CN
4	204.48.24.100	US	9	195.178.120.33	US
5	49.143.32.6	KR	10	45.134.144.203	US

攻撃パターン毎の詳細分析結果

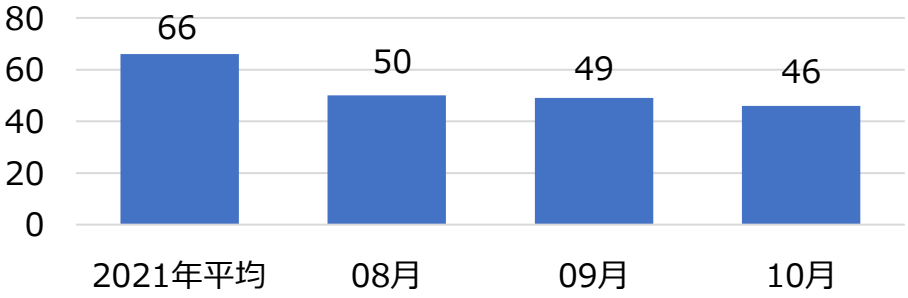
11月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
Web Vulnerability Scanner(Zgrab)	Web Vulnerability Scanner(Zgrab)は、Webサーバの設定ページや許可方法、許可されていないWebページ、ライセンスのないポートなど、脆弱性部分の存在を判断するために使用される。
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。
CommandInjection (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。
システムファイル アクセス検出	Directory Traversalの脆弱性などを利用し、「/etc/passwd」や「*.conf /.env」などの構成情報を含む主要なシステム ファイルにアクセスを計る。
phpMyAdmin サンプルページへ アクセス	phpMyAdminはMySQLをWebサーバで管理する目的にてPHPで作成されたオープンソースツールである。MySQLサーバを対象に脆弱性を見つけ、データベースの作成/削除、テーブルの作成/削除、フィールドの生成/削除、SQL文の実行など、権限を利用した管理機能実行による攻撃が可能となる。その脆弱性が存在する場合、phpMyAdminのscript/setup.phpファイルに `?` 引数を使用して任意の関数を挿入し、システム命令を実行できる。
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。 この脆弱性は家庭用ルータにて発見された。
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。
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。
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。
Network Scan	ネットワーク脆弱性スキャン攻撃は送信先の多数のシステムに対してシステムそのもののバグ、構成上の問題点などハッキング可能なシステムのセキュリティ脆弱性を調べるための攻撃で、一番頻繁に行われる攻撃である。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

SPIDER TM のポリシーにて、2022年10月の1か月間で共有されたサイバー脅威検知ポリシーは46件である。10月1か月の間、MS Windows(CVE-2022-34721), MS Exchange(CVE-2022-41040, CVE-2022-41082), MetaStealer Malware, OWASP Amassなどに対する検知ポリシーが配布された。



3か月間件数

5,985
全体配布量

46
今月配布量

49
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert udp $EXTERNAL_NET any -> $HOME_NET 500 (msg:"IGRSS.2.05976 Microsoft, Windows IKE, CVE-2022-34721, Attempted User Privilege Gain"; flow:to_server; content:"|84|"; depth:1; offset:16; content:"|00 08|"; within:2; distance:13; sid:205976;)	Microsoft Windows IKEのCVE-2022-34721脆弱性を悪用したリモートコマンド実行攻撃を検知するポリシー	Microsoft, Windows IKE, CVE-2022-34721
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.05986 Microsoft, Exchange, CVE-2022-41040, CVE-2022-41082, Attempted User Privilege Gain"; flow:to_server,established; content:"autodiscover.json"; fast_pattern; nocase; http_uri; content:"Powershell"; distance:0; nocase; http_uri; sid:205986;)	Microsoft ExchangeのCVE-2022-41040, CVE-2022-41082 脆弱性を悪用したリモートコマンド実行攻撃を検知するポリシー	Microsoft, Exchange, CVE-2022-41040, CVE-2022-41082
alert tcp $HOME_NET any -> $EXTERNAL_NET ![20,21,22,53,69,110,143,993] (msg:"IGRSS.8.05990 Malware, MetaStealer, A Network Trojan was detected"; flow:to_server,established; content:"GET /avast_update HTTP/1.1|0D 0A|"; depth:28; nocase; sid:805990;)	MetaStealer Malwareの ネットワーク通信を検知するポリシー	Malware, MetaStealer
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.12.06021 OWASP, Amass, Attempted Information Leak"; flow:to_server,established; content:"User-Agent: OWASP Amass"; fast_pattern:only; http_header; sid:1206021;)	OWASP AmassのデフォルトUser-Agentを検知するポリシー	OWASP, Amass