SECURITY REPORT

2022

SEP

2022年9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9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。

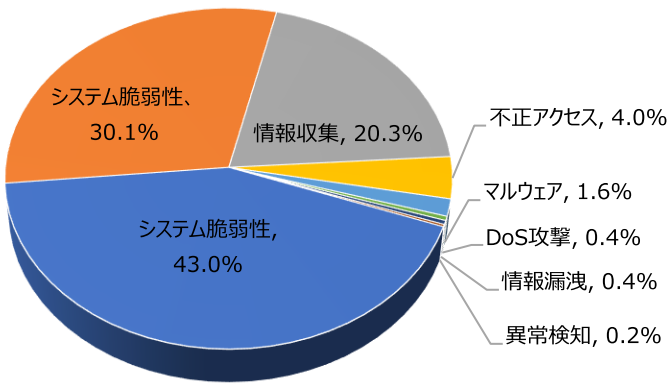
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	43.0%	▲1
Web脆弱性(Web Vulnerability)	30.1%	▼1
情報収集(Information Gathering)	20.3%	-
不正アクセス(Unauthorized access)	4.0%	-
マルウェア(Malware)	1.6%	-
DoS攻撃(Denial of service attack)	0.4%	-
情報漏洩(Information Exposure)	0.4%	-
異常検知(Anomaly Detection)	0.2%	-

2022年9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0.77倍ぐらい減少し、それぞれの攻撃パターン件数も減少していることが確認できた。

このうち、ウェブ脆弱性に関する攻撃は先月比べて約2,500件ほど減少し、これはThinkPHP Remote Code Execution Vulnerability攻撃件数の減少によるものだと確認できた。

また、システム脆弱性に関する攻撃は先月と比べて約200件ぐらい減少し、これはMVPower Command Injection(Netgear Routers Vulnerability)攻撃件数減少によるものだと確認できた。



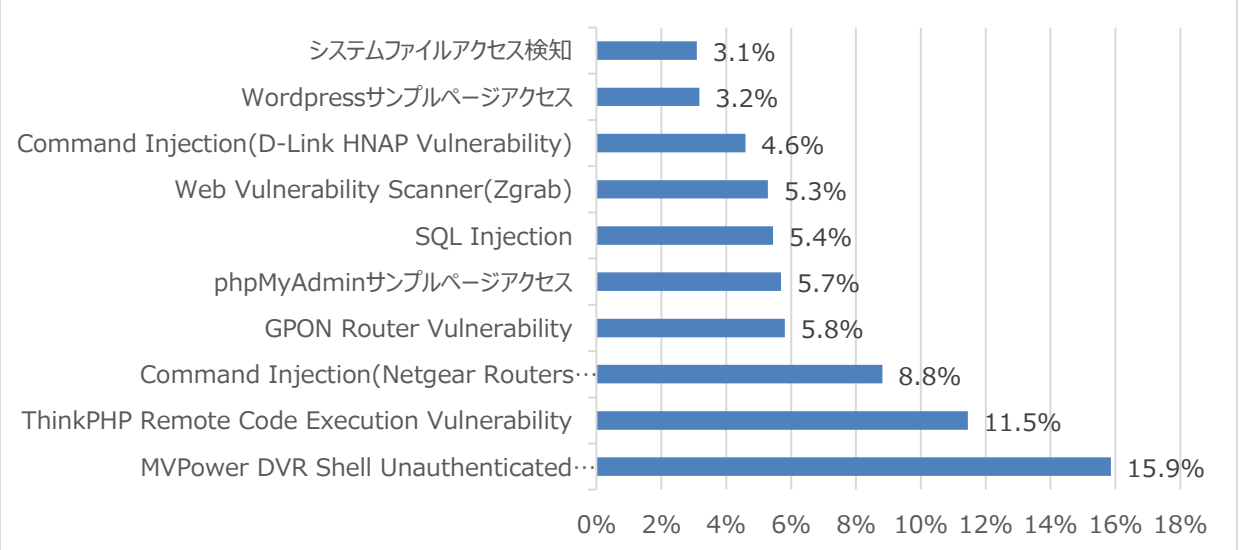
月次攻撃サービスの統計及び分析 - 2022年9月

02. 月次脆弱性攻撃TOP10

2022年9月の月次脆弱性TOP10を確認した結果、 phpMyAdminサンプルページアクセス攻撃が新たにTOP10に登場し、全体的な攻撃件数が減少したことが確認できた。特にThinkPHP Remote Code Execution Vulnerability攻撃が先月と比べて1300件ぐらい大幅に減少した。

順位	検知名	比率(%)	比較
1	MVPower DVR Shell Unauthenticated Command Execution	15.9%	▲1
2	ThinkPHP Remote Code Execution Vulnerability	11.5%	▼1
3	Command Injection (Netgear Routers Vulnerability)	8.8%	-
4	GPON Router Vulnerability	5.8%	▲2
5	phpMyAdminサンプルページアクセス	5.7%	NEW
6	SQL Injection	5.4%	▼1
7	Web Vulnerability Scanner(Zgrab)	5.3%	▼3
8	Command Injection (D-Link HNAP Vulnerability)	4.6%	▲1
9	WordPressサンプルページアクセス	3.2%	▼2
10	システムファイルアクセス検出	3.1%	▼2

Total Threats In SOC



月次攻撃サービスの統計及び分析 - 2022年9月

03. 月次ブラックリストIPアドレスTOP 10

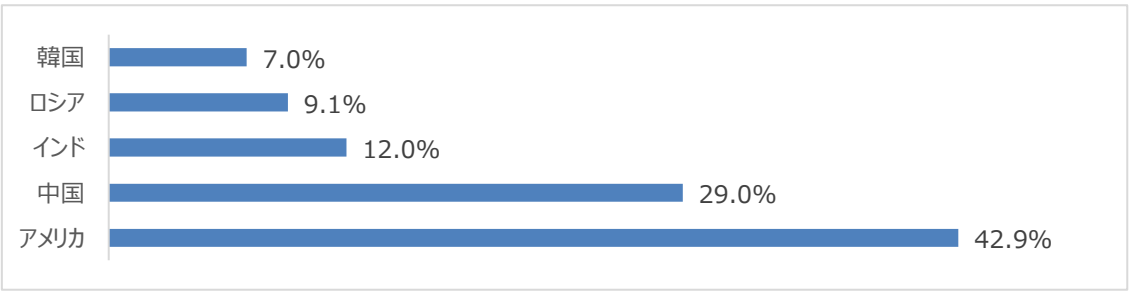
2022年9月についてTOP10を確認した結果、アメリカとインド、ロシアの攻撃比率が増加し、一方中国と韓国の攻撃の比率は減少した。アメリカと中国の攻撃比率の合計は全体に比べて約45%で、半分に少し足りないぐらい増加したことが確認できた。

※ 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	45.134.144.140	US	Directory Traversal
2	92.53.65.52	RU	Fortinet FortiOS Directory Traversal(CVE-2018-13379)
3	49.143.32.6	KR	MVPower DVR Shell Unauthenticated Command Execution
4	179.43.155.171	CH	Git Repositoryページアクセス検知
5	1.254.66.181	KR	Apache Log4j RCE(CVE-2021-44228)
6	65.49.27.187	US	Apache Log4j RCE(CVE-2021-44228)
7	141.98.11.92	LT	Vmware Server-side Template Injection RCE (CVE-2022-22594)
8	209.141.57.123	US	ThinkPHP Remote Code Execution Vulnerability
9	195.178.120.159	US	Command Injection(D-Link HNAP Vulnerability)
10	178.211.139.4	PL	Apache Log4j RCE(CVE-2021-44228)

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	45.134.144.140	US	6	65.49.27.187	US
2	92.53.65.52	RU	7	141.98.11.92	LT
3	49.143.32.6	KR	8	209.141.57.123	US
4	179.43.155.171	CH	9	195.178.120.159	US
5	1.254.66.181	KR	10	178.211.139.4	PL

攻撃パターン毎の詳細分析結果

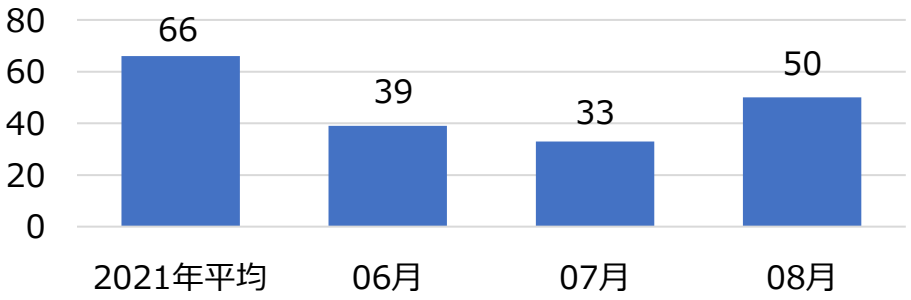
9月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。
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。
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。
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。
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。
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。
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。
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。

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7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50件である。
8月1か月の間、VMware Workspace ONE Access(CVE-2022-31659)、Realtek(CVE-2022-27255), Cmdshell php Webshellなどに対する検知ポリシーが配布された。



3か月間件数

5,890
全体配布量

50
今月配布量

33
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 5432 -> $HOME_NET any (msg:"IGRSS.1.05886 VMware, Workspace One Access, CVE-2022-31659, Attempted Administrator Privilege Gain"; flow:to_client,established; content:"|44|"; content:"|3B|CREATE/*"; distance:0; nocase; content:"|3B|COPY/*"; distance:0; nocase; content:"*/PROGRAM/*"; distance:0; nocase; sid:105886;)	VMware Workspace ONE AccessのCVE-2022-31659脆弱性を悪用した権限上昇攻撃を検知するポリシー	VMware Workspace ONE Access CVE-2022-31659
alert tcp any any -> any $HTTP_PORTS (msg:"IGRSS.2.05887 Zimbra, Collanoration, CVE-2022-27924, Attempted User Privilege Gain"; flow:to_server,established; content:"/home/"; fast_pattern:only; http_uri; pcre:"/¥x2f(service|zimbra)¥x2fhome¥x2f[^¥x2f¥x3f¥x26]*?[¥r¥n]/Ui"; sid:205887;)	Zimbra CollaborationのCVE-2022-27924脆弱性を悪用したコマンド挿入攻撃を検知するポリシー	Zimbra, Collanoration CVE-2022-27924
alert udp $EXTERNAL_NET any -> $HOME_NET any (msg:"IGRSS.1.05906 Realtek, eCos SDK, CVE-2022-27255, Attempted Administrator Privilege Gain"; flow:to_server; content:"INVITE "; depth:7; content:"m=audio "; fast_pattern; nocase; isdataat:128,relative; content:!"|0D|"; within:128; content:!"|0A|"; within:128; pcre:"/m=audio¥x20[^¥x20¥r¥n]*¥x20[^¥r¥n]{128}/i"; sid:105906;)	Realtek eCos SDKの CVE-2022-27255 脆弱性を悪用したバッファオーバーフロー攻撃を検知するポリシー	Realtek, eCos SDK CVE-2022-27255
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.8.05920 Webshell, php, CmdShell, A Network Trojan was detected"; flow:to_server,established; file_data; content:"<?"; content:"system($_GET['cmd'])"; fast_pattern:only; sid:805920;)	CmdShell PHP Webshellの ネットワーク通信を検知するポリシー	Webshell, php, CmdShell