SECURITY REPORT

2024

SEP

2024年09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 - 2024年08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。

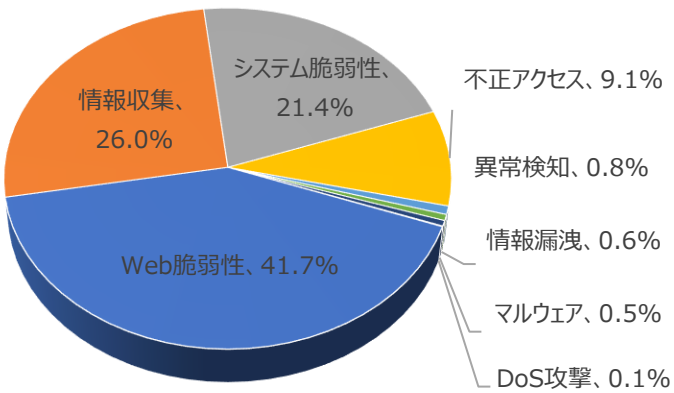
01. 月次攻撃類型

パターン	比率(%)	比較
Web脆弱性(Web Vulnerability)	41.7%	-
情報収集(Information Gathering)	26.0%	▲1
システム脆弱性(System Vulnerability)	21.4%	▼1
不正アクセス(Unauthorized access)	9.1%	-
異常検知(Anomaly Detection)	0.8%	▲2
情報漏洩(Information Exposure)	0.6%	-
マルウェア(Malware)	0.5%	▼2
DoS攻撃(Denial of service attack)	0.1%	-

2024年08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1.03倍ぐらい増加した。

そのうち、システム脆弱性に関する攻撃は先月比べて約490件ほど減少し、これはApache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)攻撃件数の減少によるものだと確認できた。

また、情報収集に関する攻撃は先月と比べて約641件ぐらい増加し、これはGit Repositoryページアクセス試み、Zgrabスキャンなどの攻撃件減増加によるものだと確認できた。

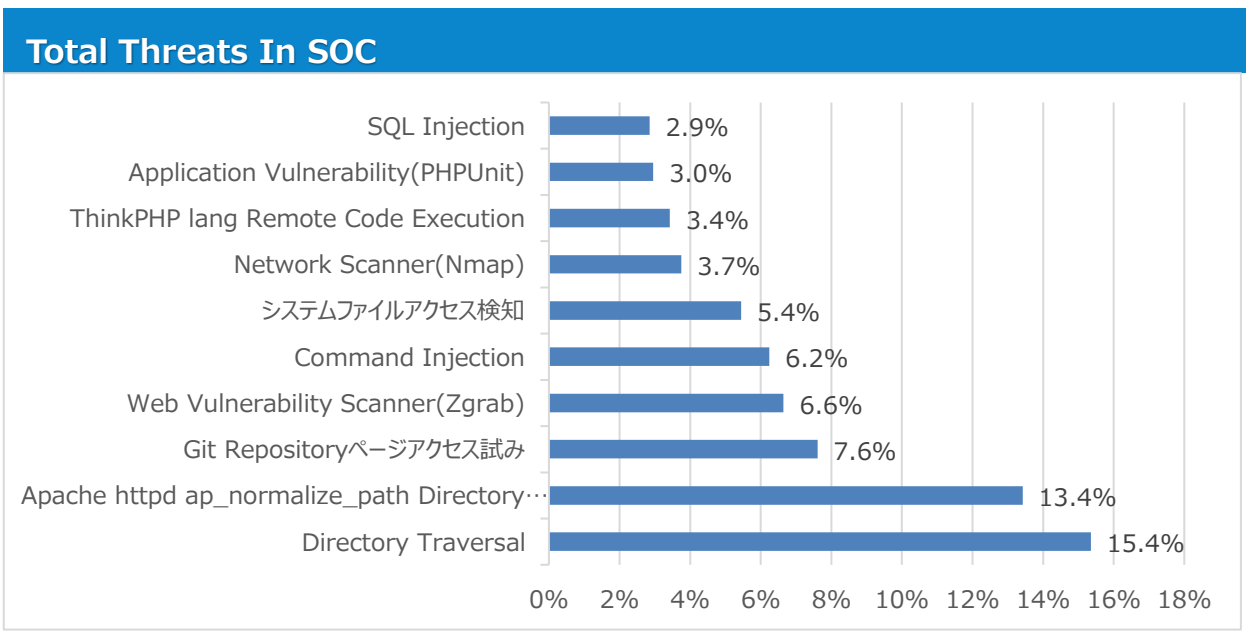


月次攻撃サービスの統計及び分析 - 2024年08月

02. 月次脆弱性攻撃TOP10

2024年08月の月次脆弱性TOP10を確認した結果、 Application Vulnerability(PHPUnit)攻撃が新たにTOP10に登場した。
全体的な攻撃件数は増加し、特にウェブスキャン攻撃件数は先月と比べて約703件ぐらい増加したことが確認できた。

順位	検知名	比率(%)	比較
1	Directory Traversal	15.4%	-
2	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	13.4%	-
3	Git Repositoryページアクセス試み	7.6%	▲5
4	Web Vulnerability Scanner(Zgrab)	6.6%	▼1
5	Command Injection	6.2%	▲1
6	システムファイルアクセス検知	5.4%	▼1
7	Network Scanner(Nmap)	3.7%	▼1
8	ThinkPHP lang Remote Code Execution	3.4%	▼1
9	Application Vulnerability(PHPUnit)	3.0%	NEW
10	SQL Injection	2.9%	▼1



月次攻撃サービスの統計及び分析 - 2024年08月

03. 月次ブラックリストIPアドレスTOP 10

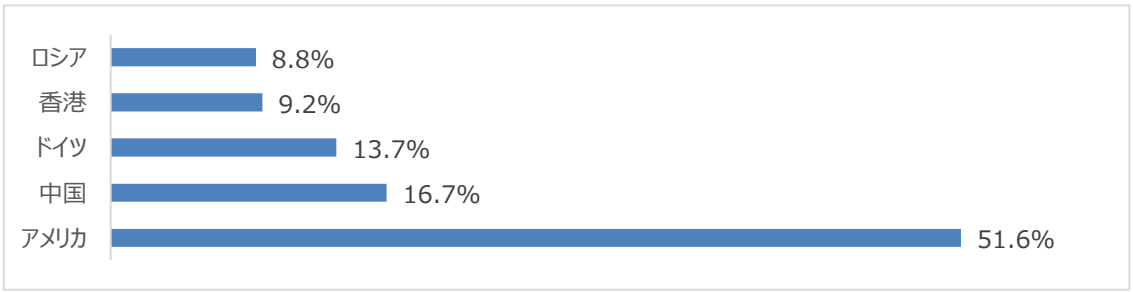
2024年08月についてTOP10を確認した結果、アメリカ、香港、ロシアの攻撃比率が増加し、特にアメリカの攻撃比率が51%を超えていることが確認できた。

※ 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	20.189.123.215	HK	Directory Traversal検知
2	94.156.64.214	BG	システムファイルアクセス
3	185.224.128.47	NL	Network Scanner(masscan)
4	27.210.152.236	CN	Directory Traversal検知
5	47.83.0.196	US	Directory Traversal検知
6	94.156.68.162	NL	システムファイルアクセス
7	51.158.205.47	FR	Network Scanner(masscan)
8	83.97.73.245	RU	etcpasswd Detect
9	154.213.185.140	SC	Command Injection
10	47.245.103.43	SG	Directory Traversal検知

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	20.189.123.215	HK
2	94.156.64.214	BG
3	185.224.128.47	NL
4	27.210.152.236	CN
5	47.83.0.196	US

Rank	Source IP	Country
6	94.156.68.162	NL
7	51.158.205.47	FR
8	83.97.73.245	RU
9	154.213.185.140	SC
10	47.245.103.43	SG

攻撃パターン毎の詳細分析結果

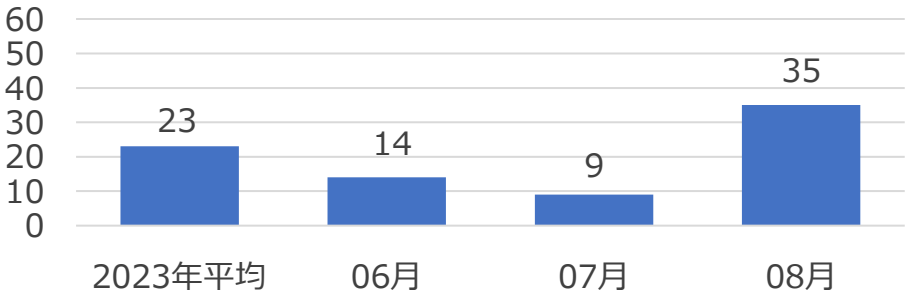
08月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
Directory Traversal	ホームページの表示もしくはダウンロードページのURLを使用せず、Webサーバ上のhomeディレクトリ外の任意のディレクトリ上のファイル(/etc/passwdファイルなど)を参照またはダウンロードすることが出来る。内部情報については、システム情報を含む/etc/pass/shadow、/etc/hosts/hostsなどの主要ファイルをダウンロードすることが可能であり、システム侵入や内部データ漏洩などの二次的な攻 撃に悪用される可能性がある。
Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	Apache httpdにDirectory Traversal脆弱性が存在する。当該の脆弱性は「ap_normalize_path」関数でURIぱすに対する不適切な有効性検証から発生する。リモートの攻撃者は悪意的に改ざんされたHTTPリクエストを送信して攻撃できる。攻撃に成功すると情報が漏洩される。
Git Repository ページアクセス試み	ソースコードのバージョン管理のためにGit Repository(/.git/)をホスティングする場合、存在するそーそコード及び重要情報を確認するためにconfigやHEADなどのデフォルトパスの存在有無及びレポジトリのパスをスキャンする攻撃である。
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	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。
システムファイル アクセス検知	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。
Network Scanner(Nmap)	代表的なNetwork Scanツールで、IP ScanとPort Scanの機能がある。ネットワーク脆弱性診断ツールとして活用されるが攻撃者から悪用されて攻撃ツールとして使用される。 .
ThinkPHP lang Remote Code Execution	ThinThinkPHP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。
Application Vulnerability(PHPUnit)	PHPUnitはユニット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 る脆弱性を利用してリモートで任意のコードが実行できる。攻撃者は
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。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年08の月の1か月間で共有されたサイバー脅威検知ポリシーは35件である。08月1か月間Zyxel NAS326(CVE-2024-29972), Ivanti vTM(CVE-2024-7593), Apache OFBiz(CVE-2024-36104), Versa Director(CVE-2024-39717)などに対する検知ポリシーが配布された。



3か月間件数

6、496
全体配布量

35
今月配布量

9
先月配布量

月間配布件数

検知ポリシー	説明	タグ
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06511 server-webapp,zyxel,nas326,cve-2024-29972, Web Application Attack"; flow:to_server,established; content:"/desktop,/cgi-bin/remote_help-cgi"; fast_pattern:only; http_uri; content:"sshd_tdc"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?type((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?sshd_tdc/Psim"; sid:1006511;)	Zyxel NAS326の脆弱性であるCVE-2024-29972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	server-webapp,zyxel,nas326,cve-2024-29972
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.1.06517 server-webapp,ivanti,vtm,cve-2024-7593, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"/apps/zxtm/wizard.fcgi"; fast_pattern:only; http_uri; content:"error="; nocase; http_uri; pcre:"/[?&]error=(?!0?(&|$))/Ui"; sid:106517;)	Ivanti vTM(Virtual Traffic Manager)の脆弱性あるCVE-2024-7593を悪用した認証バイパス攻撃を検知するポリシー	server-webapp,ivanti,vtm,cve-2024-7593
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06518 server-webapp,OFBiz,cve-2024-32113,cve-2024-36104, Web Application Attack"; flow:to_server,established; content:"/webtools/control/"; fast_pattern:only; content:"/webtools/control/"; nocase; http_raw_uri; pcre:"/^[^¥x3f]*?((¥x2e|%(25)?2e){2}([¥x2f¥x5c]|%(25)?(2f|5c))|(¥x3b|%(25)?3b))/Ii"; sid:1006518;)	Apache OFBizの脆弱性であるCVE-2024-32113, CVE-2024-36104を悪用してDirectory Traversal攻撃を検知するポリシー	server-webapp,OFBiz,cve-2024-32113,cve-2024-36104
alert tcp $EXTERNAL_NET any -> $HOME_NET [4566,4570] (msg:"IGRSS.1.06530 server-webapp,versa,director,cve-2024-39717, Attempted Administrator Privilege Gain"; flow:to_server,established; content:"PK|03 04|"; content:"CapturePassTransformer"; distance:0; sid:106530;)	Versa Directorの脆弱性であるCVE-2024-39717を悪用したファイルアップロード攻撃を検知するポリシー	server-webapp,versa,director,cve-2024-39717