SECURITY REPORT

2024

NOV

2024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 - 2024年10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。

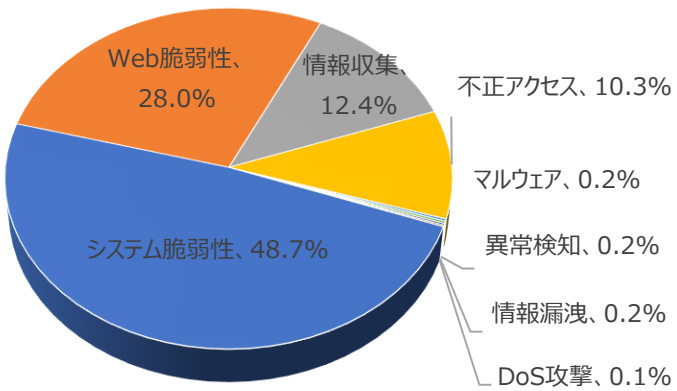
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	48.7%	▲3
Web脆弱性(Web Vulnerability)	28.0%	-
情報収集(Information Gathering)	12.4%	▼2
不正アクセス(Unauthorized access)	10.3%	▼1
マルウェア(Malware)	0.2%	▲2
異常検知(Anomaly Detection)	0.2%	▲1
情報漏洩(Information Exposure)	0.2%	▼1
DoS攻撃(Denial of service attack)	0.1%	-

2024年10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2.9倍ぐらい幅広く増加した。

システム脆弱性に関する攻撃は先月比べて約13,220件ほど増加し、これはApache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)攻撃件数の増加によるものだと確認できた。

また、Web脆弱性に関する攻撃は先月と比べて5,363件ほど増加し、これはPHPUnit, PHP-CGI Argument Injectionなどの攻撃件数の増加によるものだと確認できた。

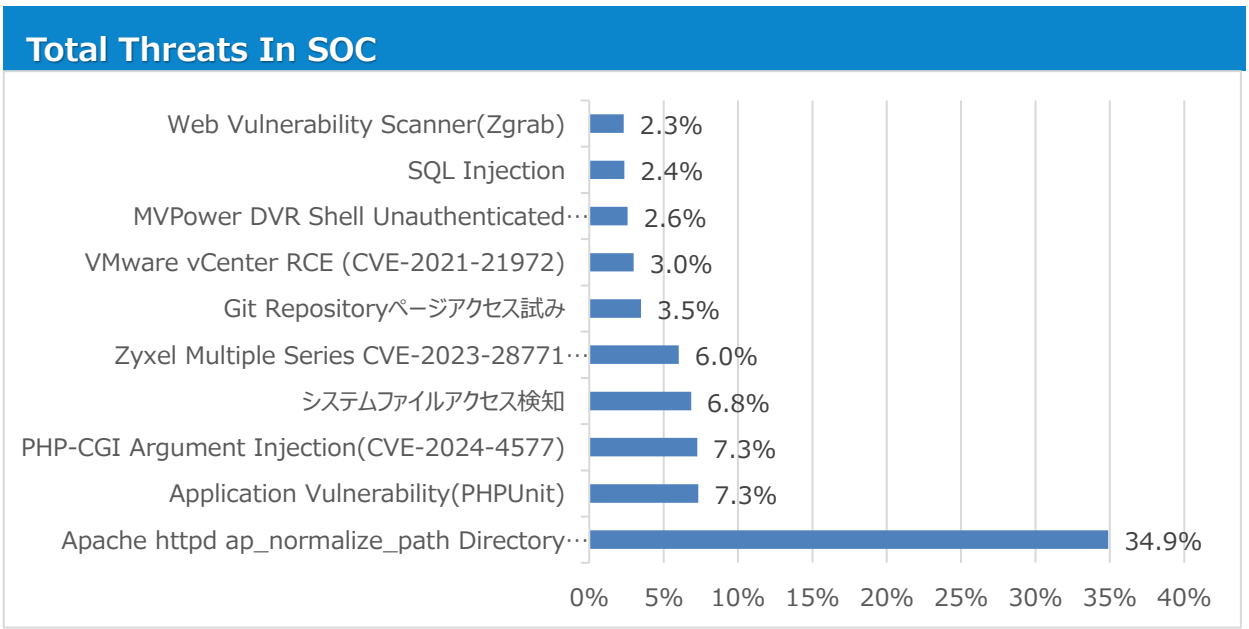


月次攻撃サービスの統計及び分析 - 2024年10月

02. 月次脆弱性攻撃TOP10

2024年10月の月次脆弱性TOP10を確認した結果、多数のシステム脆弱性攻撃が新たにTOP10に登場した。全体的な攻撃件数は増加し、これはシステム脆弱性の攻撃件数は先月と比べて約13,220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	Apache httpd ap_normalize_path Directory Traversal(CVE-2021-41773)	34.9%	▲4
2	Application Vulnerability(PHPUnit)	7.3%	NEW
3	PHP-CGI Argument Injection(CVE-2024-4577)	7.3%	NEW
4	システムファイルアクセス検知	6.8%	▼3
5	Zyxel Multiple Series CVE-2023-28771 Command Injection	6.0%	NEW
6	Git Repositoryページアクセス試み	3.5%	▼2
7	VMware vCenter RCE (CVE-2021-21972)	3.0%	NEW
8	MVPower DVR Shell Unauthenticated Command Execution	2.6%	NEW
9	SQL Injection	2.4%	▼2
10	Web Vulnerability Scanner(Zgrab)	2.3%	▼9



月次攻撃サービスの統計及び分析 - 2024年10月

03. 月次ブラックリストIPアドレスTOP 10

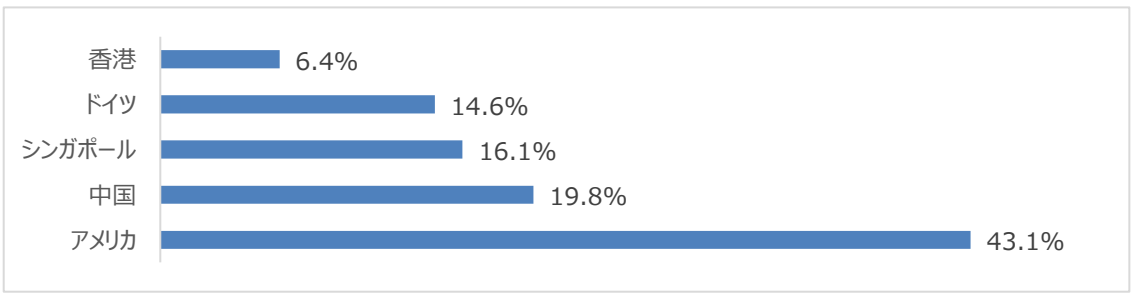
2024年10月についてTOP10を確認した結果、中国、シンガポールの攻撃比率が増加し、特にアメリカの攻撃比率が43%を超えていることが確認できた。

※ 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	47.251.99.88	US	PHP-CGI Argument Injection(CVE-2024-4577)
2	147.139.144.147	ID	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
3	8.216.124.0	JP	PHP-CGI Argument Injection(CVE-2024-4577)
4	121.141.64.236	KR	Application Vulnerability(PHPUnit)
5	8.213.33.170	SA	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
6	8.221.136.235	JP	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
7	8.217.10.15	HK	ThinkPHP Remote Code Execution Vulnerability
8	117.186.238.82	CH	ThinkPHP Remote Code Execution Vulnerability
9	47.251.110.228	US	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
10	8.218.12.181	HK	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)

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	47.251.99.88	US
2	147.139.144.147	ID
3	8.216.124.0	JP
4	121.141.64.236	KR
5	8.213.33.170	SA

Rank	Source IP	Country
6	8.221.136.235	JP
7	8.217.10.15	HK
8	117.186.238.82	CH
9	47.251.110.228	US
10	8.218.12.181	HK

攻撃パターン毎の詳細分析結果

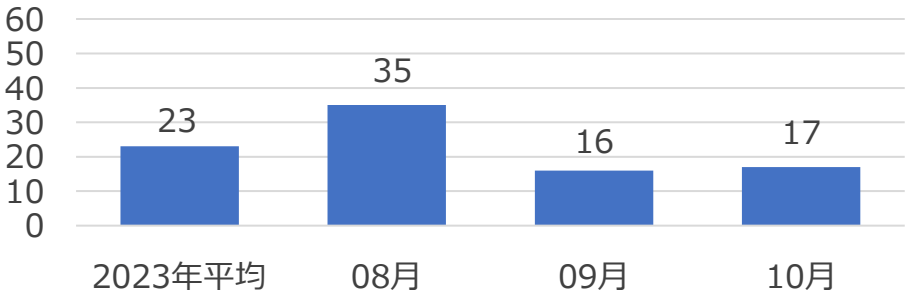
10月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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?<phpの文字列から始まるHTTP POSTデータで任意のPHPコードが実行できる。
PHP-CGI Argument Injection(CVE-2024-4577)	CVE-2024-4577脆弱性はPHPのCGIモードからWindowsの「Best-Fit」機能が間違ったエンコードが行われて発生するリモートコード実行(RCE)脆弱性である。WindowsのOSからPHPがCGIモードで実行されたり、XAMPPのような開発環境でデフォルト設定でPHPバイナリが漏出された場合脆弱である。この脆弱性を悪用すると攻撃者は改ざんされたURLぱらめーたで任意のこーどが実行できる。今まで確認されたことは、特定のシステムロケール(中国語の繁体字及び簡体字、日本語)を使用する場合エクスプロイトができることが確認されたが、他のロケールも場合によっては影響を受ける可能性があるため、パッチバージョンでアップデートすることを推奨する。
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。
Zyxel Multiple Series CVE-2023-28771 Command Injection	台湾の通信機器業者のZyxel社のファイアウォール・VPN機器に存在する一部ファイアウォールバージョンの不適切なエラーメッセージを修理で認証されていない攻撃者が改ざんされたパケットを影響を受ける危機に送信し、一部のOSコマンドがリモートで実行できる。
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。
VMware vCenter RCE (CVE-2021-21972)	vSphere Client(HTML5)にはvCenter Servereプラグインのリモートコード実行脆弱性が含まれている。ポート443に対するネットワークアクセス権限がある悪意を持っている攻撃者がこの問題を悪用してvCenter Serverをホスティングする基本OSに無制限の権限でコマンドが実行できる。これはVMware vCenter Server(7.0 U1c以前の7.x、6.7 U3l以前の6.7及び6.5、U3n以前6の.5)及びVMware Cloud Foundation(4.2以前の4.x及び3.10.1.2以前の3.x)に影響を及ぼす。
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。
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。

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17件である。10月1か月間Window(CVE-2024-38112), SolarWinds(CVE-2024-28986), Ivanti(CVE-2024-9380)Cicada3301ランサムウェアなどに対する検知ポリシーが配布された。



3か月間件数

6,529
全体配布量

17
今月配布量

16
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 $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.2.06551 os-windows,microsoft,mshtml,cve-2024-38112, Attempted User Privilege Gain"; flow:to_client,established; file_data; content:"[InternetShortcut]"; depth:250; fast_pattern; nocase; content:"mhtml|3A|"; distance:0; nocase; content:"x-usc|3A|"; distance:0; nocase; pcre:"/^¥s*URL¥s*=¥s*mhtml¥x3a¥s*http/im"; sid:206551;)	Mircrosoft Windows MSHTMLの脆弱性であるCVE-2024-38112を悪用したスプーフィング試みを検知するポリシー	os-windows,microsoft,mshtml,cve-2024-38112
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06552 server-webapp,solarwinds,WebHelpDesk,cve-2024-28986, Attempted User Privilege Gain"; flow:to_server,established; content:"/helpdesk/WebObjects/Helpdesk.woa/ajax/"; fast_pattern:only; http_uri; content:"WOIsmapCoords"; nocase; http_client_body; content:"takeValueForKey"; distance:0; nocase; http_client_body; content:"javaClass"; distance:0; nocase; http_client_body; sid:206552;)	SolarWinds Web Help Deskの脆弱性であるCVE-2024-28986を悪用した逆直列化試みを検知するポリシー	server-webapp,solarwinds,WebHelpDesk,cve-2024-28986
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.06553 malware-other,ransomware,Cicada3301, A Network Trojan was detected"; flow:to_server,established; file_data; content:"C|3A 5C|Users|5C|Public|5C|psexec0.exe4d5a90"; sid:806553;)	Cicada3301 Ransomwareダウンロード試みを検知するポリシー	malware-other,ransomware,Cicada3301
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06566 server-webapp,Ivanti,CSA,cve-2024-34102, Web Application Attack"; flow:to_server,established; content:"/gsb/reports.php"; fast_pattern:only; http_uri; content:"TW"; nocase; http_client_body; pcre:"/(^|&)TW(¥x5f|%(25)?5f)ID=[^&]*?([¥x60¥x3b¥x7c¥x23]|%(25)?(60|3b|7c|23|26|0a)|([¥x3c¥x3e¥x24]|%(25)?(3c|3e|24))(¥x28|%(25)?28))/Pim"; sid:1006566;)	Ivanti Cloud Services Appliance脆弱性であるCVE-2024-9380を悪用したコマンドインジェクション試みを検知するポリシー	server-webapp,Ivanti,CSA,cve-2024-34102