SECURITY REPORT

2024

DEC

2024年12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。

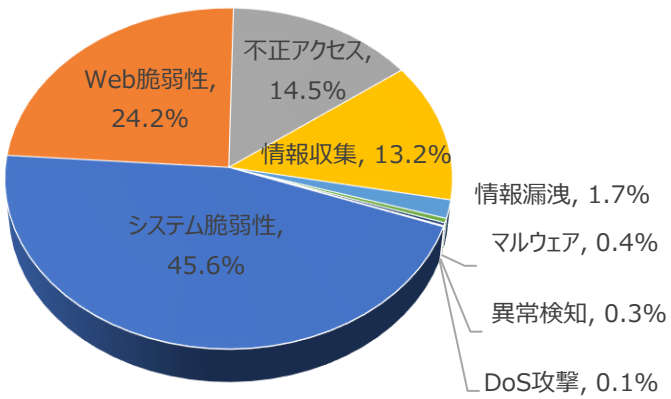
01. 月次攻撃類型

パターン	比率(%)	比較
システム脆弱性(System Vulnerability)	45.6%	-
Web脆弱性(Web Vulnerability)	24.2%	-
不正アクセス(Unauthorized access)	14.5%	▲1
情報収集(Information Gathering)	13.2%	▼1
マルウェア(Malware)	1.7%	▲2
情報漏洩(Information Exposure)	0.4%	▼1
異常検知(Anomaly Detection)	0.3%	▼1
DoS攻撃(Denial of service attack)	0.1%	-

2024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0.75倍ぐらい減少した。

そのうち、システム脆弱性に関する攻撃は先月比べて約4,345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、Web脆弱性に関する攻撃は先月と比べて約2,942件ぐらい減少し、これはPHPUnit, PHP-CGI Argument Injectionなどの攻撃件数減少によるものだと確認できた。

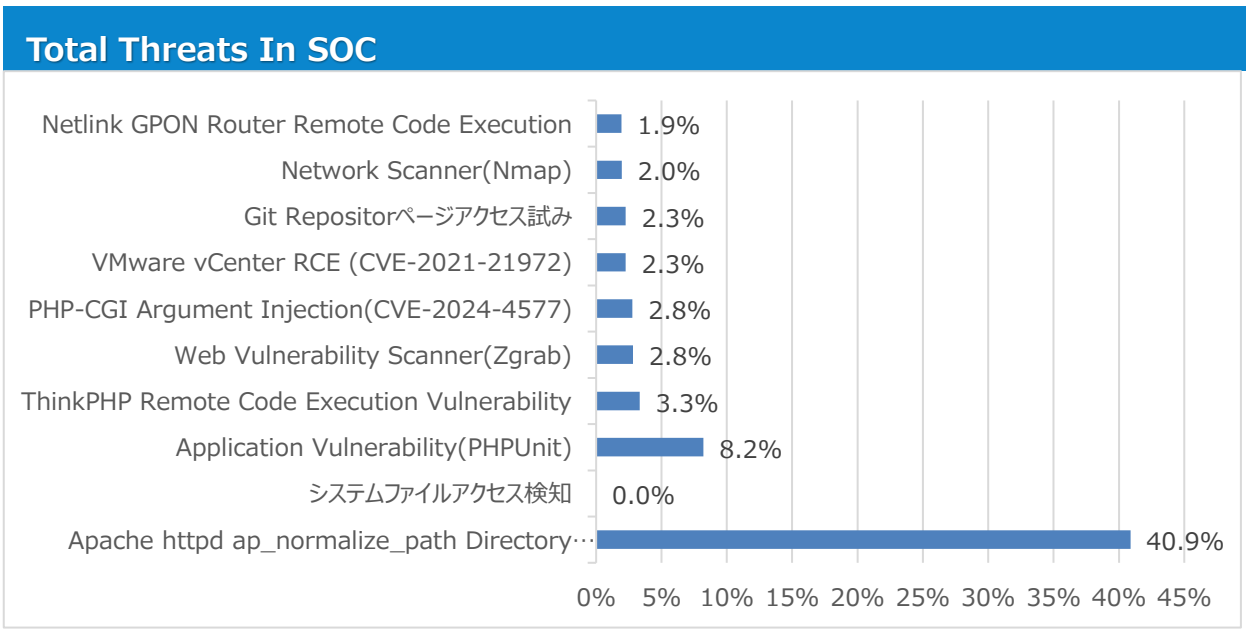


月次攻撃サービスの統計及び分析 - 2024年11月

02. 月次脆弱性攻撃TOP10

2024年11月の月次脆弱性TOP10を確認した結果、多数の新たな攻撃がTOP10に登場した。
全体的な攻撃件数は減少し、特にシステム脆弱性の攻撃件数が先月と比べて約7,491件ぐらい減少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)	40.9%	-
2	システムファイルアクセス検知	13.1%	▲2
3	Application Vulnerability(PHPUnit)	8.2%	▼1
4	ThinkPHP Remote Code Execution Vulnerability	3.3%	NEW
5	Web Vulnerability Scanner(Zgrab)	2.8%	▲5
6	PHP-CGI Argument Injection(CVE-2024-4577)	2.8%	▼3
7	VMware vCenter RCE (CVE-2021-21972)	2.3%	-
8	Git Repositorページアクセス試み	2.3%	▼2
9	Network Scanner(Nmap)	2.0%	NEW
10	Netlink GPON Router Remote Code Execution	1.9%	NEW



月次攻撃サービスの統計及び分析 - 2024年11月

03. 月次ブラックリストIPアドレスTOP 10

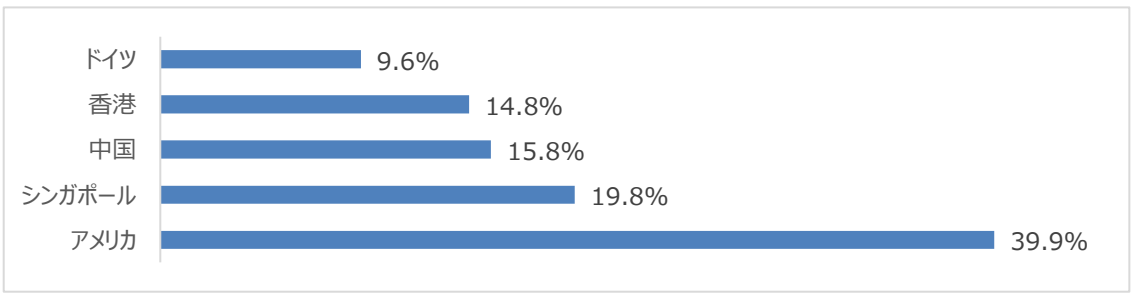
2024年11月についてTOP10を確認した結果、中国とシンガポールの攻撃比率が増加し、特にアメリカの攻撃比率が約39.9%を超えていることが確認できた。

※ 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	223.100.248.31	CN	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
2	47.236.167.8	SG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
3	47.245.119.234	SG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
4	47.251.103.74	US	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
5	47.236.136.217	SG	Application Vulnerability(PHPUnit)
6	47.236.252.254	SG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
7	8.219.144.149	SG	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
8	203.81.86.34	MM	Apache httpd ap_normalize_path Directory Traversal (CVE-2021-41773)
9	47.236.150.50	SG	PHP-CGI Argument Injection(CVE-2024-4577)
10	47.237.6.119	SG	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	Rank	Source IP	Country
1	223.100.248.31	CN	6	47.236.252.254	SG
2	47.236.167.8	SG	7	8.219.144.149	SG
3	47.245.119.234	SG	8	203.81.86.34	MM
4	47.251.103.74	US	9	47.236.150.50	SG
5	47.236.136.217	SG	10	47.237.6.119	SG

攻撃パターン毎の詳細分析結果

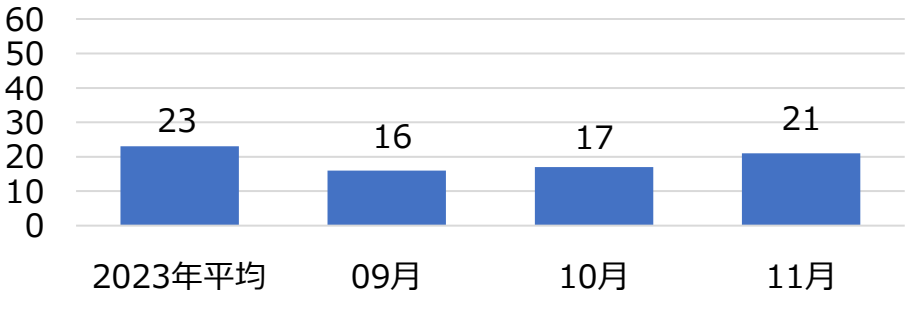
11月に発生した脆弱性パターンのうち、TOP10を中心に攻撃パターン詳細分析結果を表記しています。
詳細分析結果を参考にして、同じ攻撃パターンを検知している場合は当該システムの脆弱性を事前に対処されることを推奨いたします。

攻撃パターン	詳細分析結果
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。
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。
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。
ThinkPHP Remote Code Execution Vulnerability	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。
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。
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。
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。
Git Repository ページアクセス	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。
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。
Netlink GPON Router Remote Code Execution	NetlinkGPONルータで発見された脆弱性として、ターゲットアドレスの後に/boaform/admin/formPing文字列を入力して認証手順を通過する可能性がある。この脆弱 性を悪用し、認証されていない攻撃者が端末からリモートでコマンドを実行、悪意のあるファイルをアップロードするなどが可能になる。

検知ポリシー

▶ 月間サイバー脅威検知ポリシー統計

2024年11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52件である。
02月1か月の間、ConnectWise ScreenConnect(CVE-2024-1708、CVE-2024-1709)、Microsoft Outlook(CVE-2023-35636、CVE-2024-21413)などに対する検知ポリシーが配布された。



3か月間件数

6,550
全体配布量

21
今月配布量

17
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 any -> $HOME_NET 541 (msg:"IGRSS.2.06569 server-other,Fortinet,FGFM,cve-2024-23113, Attempted User Privilege Gain"; flow:to_server,established; content:"|34 E0 01 00|"; depth:4; fast_pattern; content:"reply 200"; distance:4; nocase; content:"request"; nocase; content:"="; distance:0; content:"auth"; distance:0; nocase; content:"%"; pcre:"/^((auth|mgmt)ip|fmg_fqdn)¥s*=[^¥r¥n]*?¥x25(?-i)[AacdEeFfGginopsuXx]/im"; sid:206569;)	Fortinet FGFMの脆弱性であるCVE-2024-23113を悪用したFormat string Injection試みを検知するポリシー	server-other,Fortinet,FGFM,cve-2024-23113
alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"IGRSS.8.06579 malware-other,ransomware,ransomhub, A Network Trojan was detected"; flow:to_server,established; file_data; content:"|4C 8D 47 01 4C 39 C3 73 2D 48 89 F0 48 89 D9 BF 01 00 00 00 48 8D 35 35 B4 23 00 4C 89 C3 E8 8D 1A B3 FF 48 8B 54 24 50 49 89 D8 48 89 C6 48 89 CB 48 8B 44 24 40|"; fast_pattern:only; sid:806579;)	RansomHubの変種Ransomwareのダウンロード試みを検知するポリシー	malware-other,ransomware,ransomhub
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.06585 server-webapp,paloalto,pan-os,cve-2024-9474, Web Application Attack"; flow:to_server,established; content:"/php/utils/createRemoteAppwebSession.php"; fast_pattern:only; http_uri; content:"user"; nocase; http_client_body; content:"Content-Disposition"; nocase; http_client_body; pcre:"/name¥s*=¥s*[¥x22¥x27]?user((?!^--).)*?[¥r¥n]{2,}((?!^--).)*?([¥x60¥x3b¥x7c¥x26¥x23]|[¥x3c¥x3e¥x24]¥x28)/Psim"; sid:1006585;)	Paloalto PAN-OSの脆弱性であるCVE-2024-9474を悪用したCommand Injection攻撃を検知するポリシー	server-webapp,paloalto,pan-os,cve-2024-9474
alert tcp any any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.06586 server-webapp,paloalto,pan-os,cve-2024-0012, Attempted User Privilege Gain"; flow:to_server,established; content:".js.map"; fast_pattern:only; http_uri; content:"X-PAN-AUTHCHECK:"; nocase; http_header; pcre:"/X-PAN-AUTHCHECK¥x3a¥s*off/Hi"; sid:206586;)	Paloalto PAN-OSの脆弱性であるCVE-2024-0012を悪用した認証バイパス攻撃を検知するポリシー	server-webapp,paloalto,pan-os,cve-2024-0012