CyberFortress Report

2020
DEC

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 - 2020年12月

株式会社サイバーフォートレスでは攻撃サービス(ポート)情報を収集し、分析しています。
分析内容から、月次攻撃サービス（ポート）、月次攻撃サービスパターンの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いただければと思います。

01. 月次脆弱性攻撃TOP 10

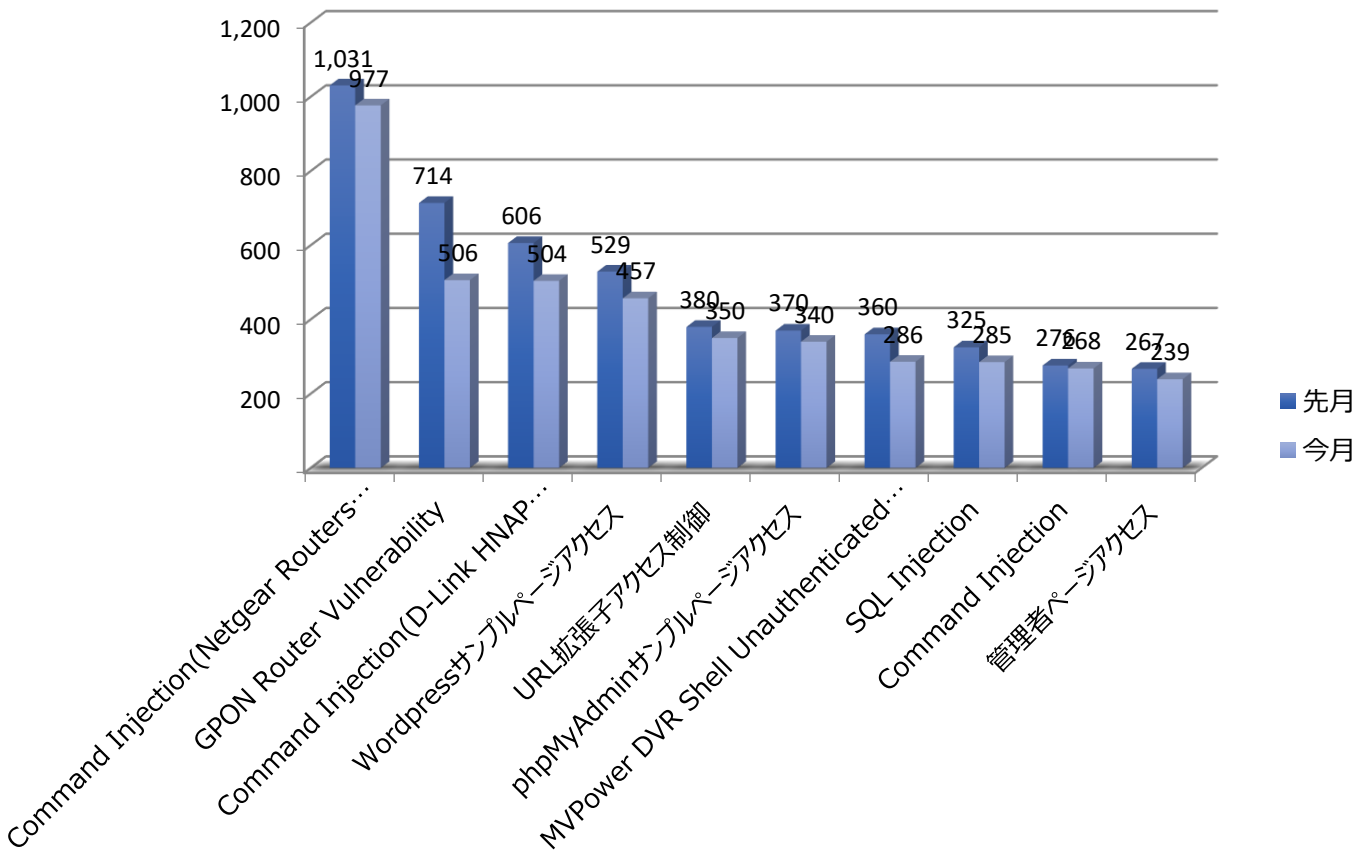
2020年12月、1ヶ月間収集された脆弱性攻撃のTOP10ではURL拡張子アクセス制御、管理者ページアクセス脆弱性を利用した攻撃が新たに登場した。
その他、GPON Router Vulnerability、Wordpressサンプルページアクセス、phpMyAdminサンプルページアクセス、 MVPower DVR Shell Unauthenticated Command Execution, Command Injection の順位が上昇したことが確認された。

順位	パターン	比率(%)	
1	Command Injection(Netgear Routers Vulnerability)	23.20%	-
2	GPON Router Vulnerability	12.01%	▲1
3	Command Injection(D-Link HNAP Vulnerability)	11.97%	▼1
4	Wordpressサンプルページアクセス	10.85%	▲2
5	URL拡張子アクセス制御	8.31%	NEW
6	phpMyAdminサンプルページアクセス	8.07%	▲1
7	MVPower DVR Shell Unauthenticated Command Execution	6.79%	▲1
8	SQL Injection	6.77%	▼3
9	Command Injection	6.36%	▲1
10	管理者ページアクセス	5.67%	NEW

月次攻撃サービスの統計及び分析 - 2020年12月

02. 脆弱性攻撃毎のイベントの比較

2020年12月、1ヶ月間収集されたイベントを分析した結果、TOP10の全体件数は先月と比べて減少したことが確認できたが、急激な件数の変化はないことで特異点はないと判断される。
新たに順位に登場したURL拡張子アクセス制御、管理者ページアクセスのイベントに対してセキュリティ機器対策として承認されたユーザーのみアクセスできるように対象することを推奨している。



月次攻撃サービスの統計及び分析 - 2020年12月

03. 月次攻撃サービス(ポート)TOP 10

2020年12月の1ヶ月間で収取されたサービスポートのTOP10では、 HTTP(TCP/80)イベントが先月と比べて上昇し、Microsoft-DS(TCP/445)イベントが先月と比べて減少している。その他、Telnet(TCP/23)ポートを利用したイベントが新たにTOP10に登場した。

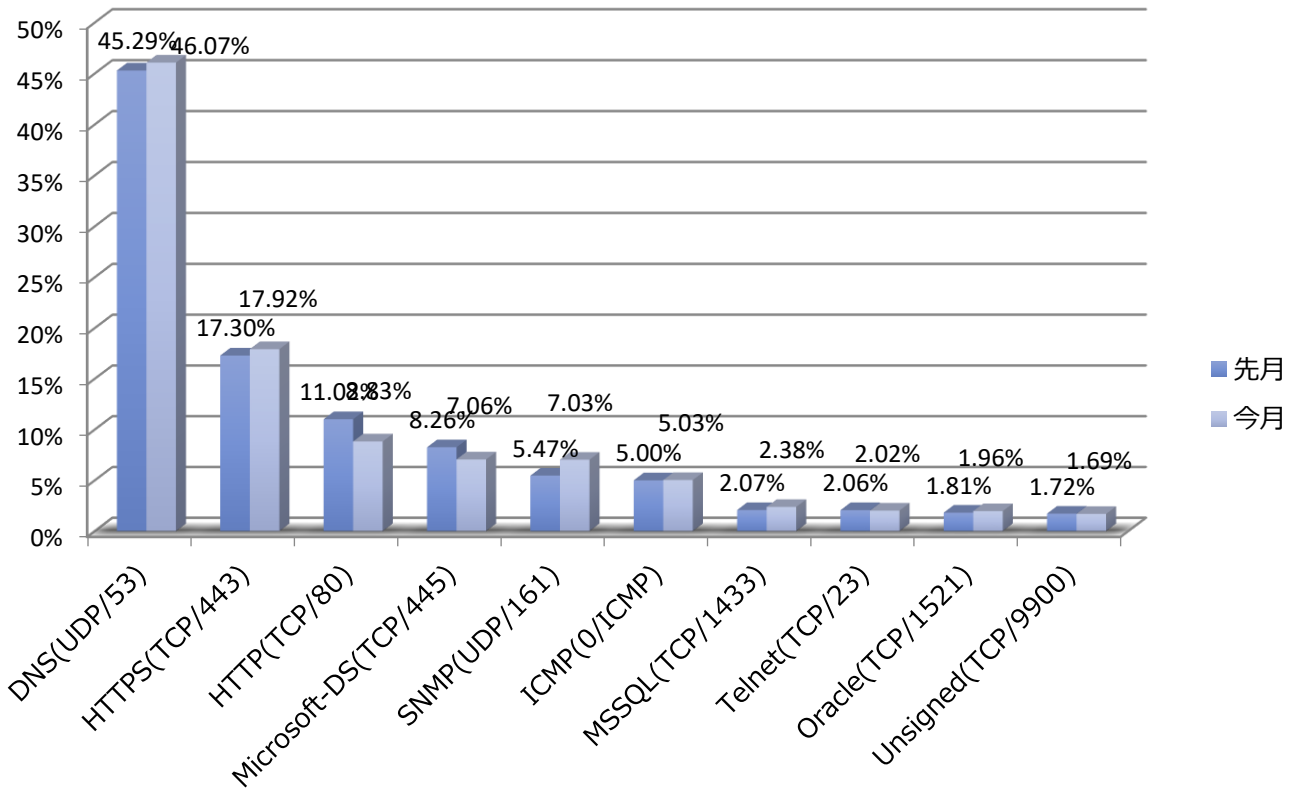
順位	サービス(ポート)	比率(%)	先月比較
1	DNS(UDP/53)	46.07%	-
2	HTTPS(TCP/443)	17.92%	-
3	HTTP(TCP/80)	8.83%	▲1
4	Microsoft-DS(TCP/445)	7.06%	▼1
5	SNMP(UDP/161)	7.03%	-
6	ICMP(0/ICMP)	5.03%	-
7	MSSQL(TCP/1433)	2.38%	-
8	Telnet(TCP/23)	2.02%	NEW
9	Oracle(TCP/1521)	1.96%	-
10	Unsigned(TCP/9900)	1.69%	-

月次攻撃サービスの統計及び分析 - 2020年12月

04. 攻撃サービス(ポート)毎のイベント比較

2020年12月、1ヶ月間収集されたイベントを分析した結果、 Telnet(TCP/23)ポートを利用したイベントが新たにTOP10に登場した。

Telnetは情報を送信する際、暗号化せずに送信するため、攻撃者が中間で情報を盗み、簡単に確認んすることができる。このような問題でTelnetサービスを利用するより暗号化して情報を送信するSSHサービスを利用するのを推奨する。サーバにTelnetサービスが有効であれば、使用有無を確認した後、使用しないのであればサービスを終了することを推奨する。



月次攻撃サービスの統計及び分析 - 2020年12月

05. 月次攻撃サービスパターンTOP 10

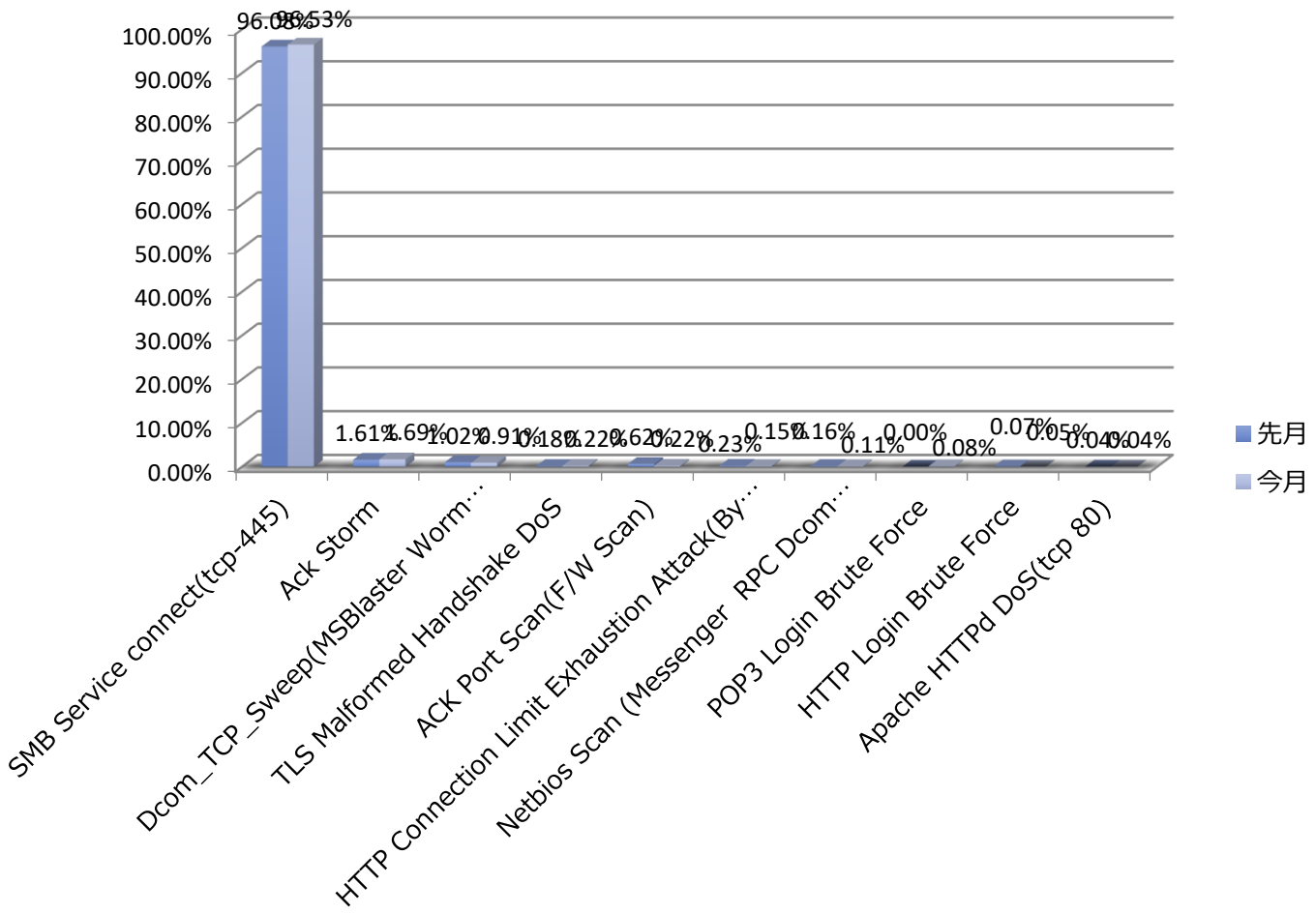
2020年12月の攻撃パターンTOP10では、 TLS Malformed Handshake DoSイベントの上昇とACK Port Scan(F/W Scan), HTTP Connection Limit Exhaustion Attack(By Slowloris), HTTP Login Brute Forceイベントの減少が確認できた。
その他、POP3 Login Bruteイベントが新たにTOP10に登場した。

順位	パターン	比率(%)	先月比較
1	SMB Service connect(tcp-445)	96.53%	-
2	Ack Storm	1.69%	-
3	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	0.91%	-
4	TLS Malformed Handshake DoS	0.22%	▲2
5	ACK Port Scan(F/W Scan)	0.22%	▼1
6	HTTP Connection Limit Exhaustion Attack(By Slowloris)	0.15%	▼1
7	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	0.11%	-
8	POP3 Login Brute Force	0.08%	NEW
9	HTTP Login Brute Force	0.05%	▼1
10	Apache HTTPd DoS(tcp 80)	0.04%	-

月次攻撃サービスの統計及び分析 - 2020年12月

06. 攻撃パターン毎のイベント比較

2020年12月の攻撃パターンTOP10では、POP3 Login Brute Forceイベントが今月のTOP10に新たに登場した。Brute Forceイベントは既に知られている攻撃で、それに対しての攻撃予防方法も知られているが、いまだに良く使用されている攻撃である。これを予防するためにはユーザー及びRootアカウントに対しての周期的なパスワードの変更、複雑なパスワード使用、そしてユーザーの注意及びセキュリティの認識が重要である。これに対してセキュリティ担当者は周期的な管理を推奨する。



攻撃パターン毎の詳細分析結果

11月に発生した攻撃パターンTOP10の詳細分析を紹介する。
詳細分析結果を参考にし、同じ攻撃パターンを検知している場合、当該のシステムの脆弱性を事前に処置することを推奨する。

攻撃パターン	詳細分析結果
SMB Service connect(tcp-445)	Microsoft Windowsは他のパソコンとファイル及びプリンタの資源を共有するために、SMBプロトコルを使用する。Windowsの古いバージョン(つまり、95, 98, Me, NT)からのSMB共有はTCPポートの137, 139とUDPポート138からNetBIOS over TCP/IPを通じて直接SMB操作が可能であり、推測できるパスワードを使用していたりパスワードを設定せずファイル共有を行う場合、悪意的な攻撃により2次的な攻撃も行われる可能性がある。
Ack Storm	攻撃者が対象サーバに大量のTCP/IPのACKパケットを送信することで、対象サーバに不要なLoadが発生し、正常なサービスを遅延させる攻撃方法で、TCP/IPのプロトコルの穴を利用して攻撃する方法である。当該の攻撃はSessionを結んだPacketに対してHijackingをするために使用されることもある。
Dcom_TCP_Sweep (MSBlaster Worm Messenger...)	W32.Blaster.WormワームはDCOM RPC Buffer Overflow脆弱性を利用して感染させるワームの種類で、当該のワームはTCP/135ポートの使用有無を確認し、脆弱性が発見された場合、システムを感染させる。感染したシステムはTCP/4444ポートを有効化し、C&Cサーバから不正ファイルをダウンロードしてレジストリに登録する。このような過程で感染したシステムのトラフィックが増加する。
TLS Malformed Handshake DoS	TLS Malformed Handshake DoS攻撃は不正的に変造されたTLSパケットを利用したDOS攻撃の種類です。不正的に変造されたTLS ClientがHandshakeをする過程で発生する。リモートの攻撃者が不正TLSのパケットに影響されるシステムに送ることで負荷を発生させる。
ACK Port Scan (F/W Scan)	ACK Port Scan(FW Scan)とはファイアウォールのポリシーから不要に許可している脆弱なポートをスキャンする攻撃である。攻撃者は特定のパケットをサーバに送り、その応答のパケットを分析してファイアウォール上で許可されているポートの情報を収集することができる。
HTTP Connection Limit Exhaustion Attack(By Slowloris)	SlowlorisはDoS攻撃(大量のパケットを送信)とは違ってウェブサーバに異常なHTTP Requestを送信することでTCPの繋がりを維持する攻撃ツールである。攻撃対象のウェブサーバはConnection資源枯渇の状態になり、ユーザーの要請に応答ができなくなりサービスサービス拒否状態になる。
Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	NetBiosはUDP137ポートでお互いの情報を確認し、TCP139でセッションを組んだ後、TCP138で情報を交換する。攻撃者はUDP137ポートを利用した攻撃対象のシステムとセッションを組んで、対象のシステムから共有しているディレクトリ及びネットワーク情報をスキャンすることができる。
POP3 Login Brute Force	POP3(110/TCP)にアクセスし、攻撃者が前もって作成したIDとパスワードリストを利用した手作業もしくはプログラムを介して持続的なログインを試す。攻撃者はシステムユーザーのアカウントを獲得し、アクセス権限を獲得することができる。
HTTP Login Brute Force	この攻撃はHTTP WEBサービスポート(TCP/80)にアクセスして特定のID(root, guestなど)のパスワードをクラッキングするツールキットを利用する。繰り返し任意の文字列を入れて確認する方法で、パスワードが推測しやすいもの、もしくはリスト型に登録されている場合、簡単にクラッキングされる。これはアカウントとパスワードは最低限6桁以上で、単純なパターンは使わずに、HTTPポート(TCP/80)に送信されるデータはFilteringして予防できる。
Apache HTTPd DoS(tcp 80)	ApacheはUNIXやLinux, MS WindowsなどのOSから動作するオープンソースのウェブサーバである。 ap_get_mime_headers_core()に存在する脆弱性で、万が一ヘッダーが空白もしくはtabで始まる場合、Apacheは必要なメモリを割り当てる。 リモートの攻撃者が悪意を持って作成されたパケットを送信してサーバが大量のメモリを割り当てるようにしてApacheが動作されないようにする。