CyberFortress Report

2020
OCT

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10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

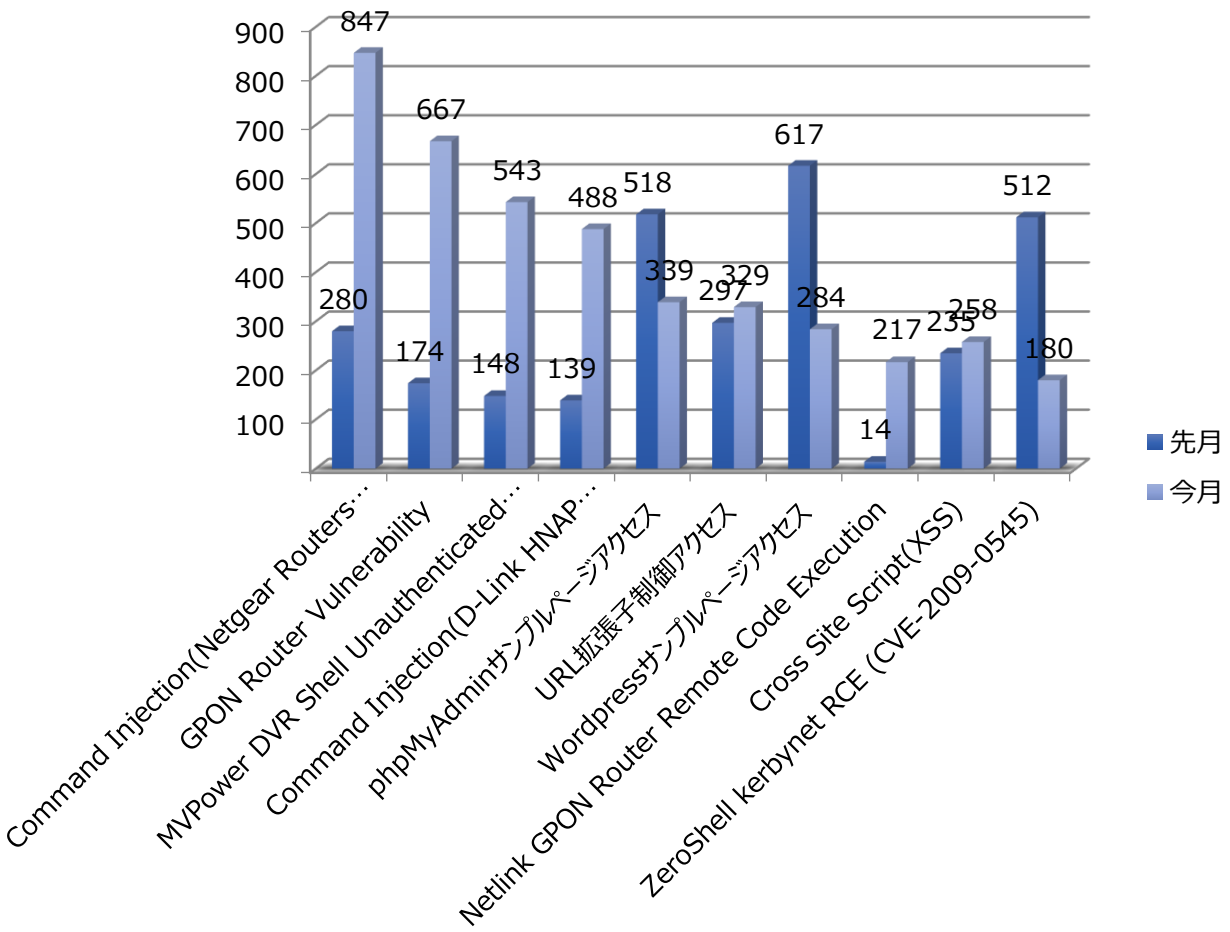
2020年10月、1ヶ月間収集された脆弱性攻撃のTOP10ではMVPower DVR Shell Unauthenticated Command Execution, Command Injection(D-Link HNAP Vulnerability), Netlink GPON Router Remote Code Executionの脆弱性を利用した攻撃が新たに順位に登場した。その他、Command Injection(Netgear Routers Vulnerability), GPON Router Vulnerability攻撃パターンが先月と比べて比率増加で上位の順位になった。

順位	パターン	比率(%)	
1	Command Injection (Netgear Routers Vulnerability)	20.40%	▲6
2	GPON Router Vulnerability	16.06%	▲8
3	MVPower DVR Shell Unauthenticated Command Execution	13.08%	NEW
4	Command Injection(D-Link HNAP Vulnerability)	11.75%	NEW
5	phpMyAdmiサンプルページアクセス	8.16%	▼2
6	URL拡張子アクセス制御	7.92%	-
7	Wordpressサンプルページアクセス	6.84%	▼6
8	Netlink GPON Router Remote Code Execution	5.23%	NEW
9	Cross Site Script(XSS)	6.21%	-
10	ZeroShell kerbynet RCE (CVE-2009-0545)	4.34%	▼6

月次攻撃サービスの統計及び分析 - 2020年10月

02. 脆弱性攻撃毎のイベントの比較

2020年10月、1ヶ月間収集されたイベントを分析した結果、TOP10の中RCE(Remote Code Execution)の攻撃が六つもあり、先月と比べてRECの攻撃件数が大きく増えた。多数のBotNet攻撃によって発生したREC攻撃に判断されてセキュリティ担当者はTOP10に含まれてREC脆弱性攻撃に当該の機器が資産に含まれているか、最新セキュリティファームウェアがアップデートされているか確認が必要である。



月次攻撃サービスの統計及び分析 - 2020年10月

03. 月次攻撃サービス(ポート)TOP 10

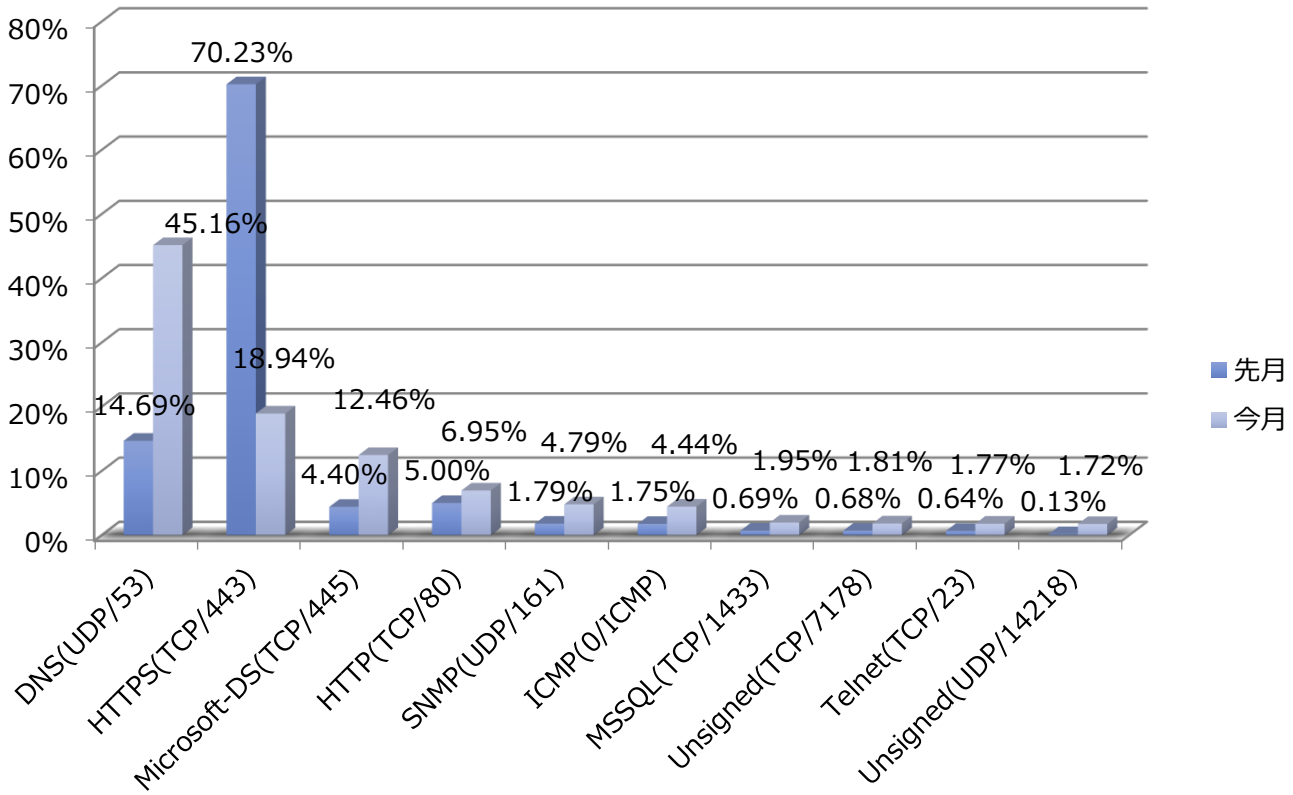
2020年10月の1ヶ月間で収取されたサービスポートのTOP10では、HTTPS(TCP/443)ポートを利用したイベントが先月と比べて幅広く減少し、その他、Microsoft-DS(TCP/445), MSSQL(TCP/1433), Unsigned(TCP/7178)ポートを利用したイベントが先月と比べて少し増加した。

順位	サービス(ポート)	比率(%)	先月比較
1	DNS(UDP/53)	45.16%	▲1
2	HTTPS(TCP/443)	18.94%	▼1
3	Microsoft-DS(TCP/445)	12.46%	▲1
4	HTTP(TCP/80)	6.95%	▼1
5	SNMP(UDP/161)	4.79%	-
6	ICMP(0/ICMP)	4.44%	-
7	MSSQL(TCP/1433)	1.95%	▲1
8	Unsigned(TCP/7178)	1.81%	▲2
9	Telnet(TCP/23)	1.77%	-
10	Unsigned(UDP/14218)	1.72%	NEW

月次攻撃サービスの統計及び分析 - 2020年10月

04. 攻撃サービス(ポート)毎のイベント比較

2020年10月、1ヶ月間収集されたイベントを分析した結果、Unsigned(UDP/14218)ポートが新たにTOP10順位に登場した。最近Well-Known Portに明示されていないサービスポートが使用された履歴の件数が持続的に増えている。不明なサービスポートの中、実際各企業で使用しているサービスポートも存在するが、ほとんどは使わないサービスポートである可能性が高い。定義されていないサービスポートは実際に使用有無を確認してポリシーでアクセス制御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10月

05. 月次攻撃サービスパターンTOP 10

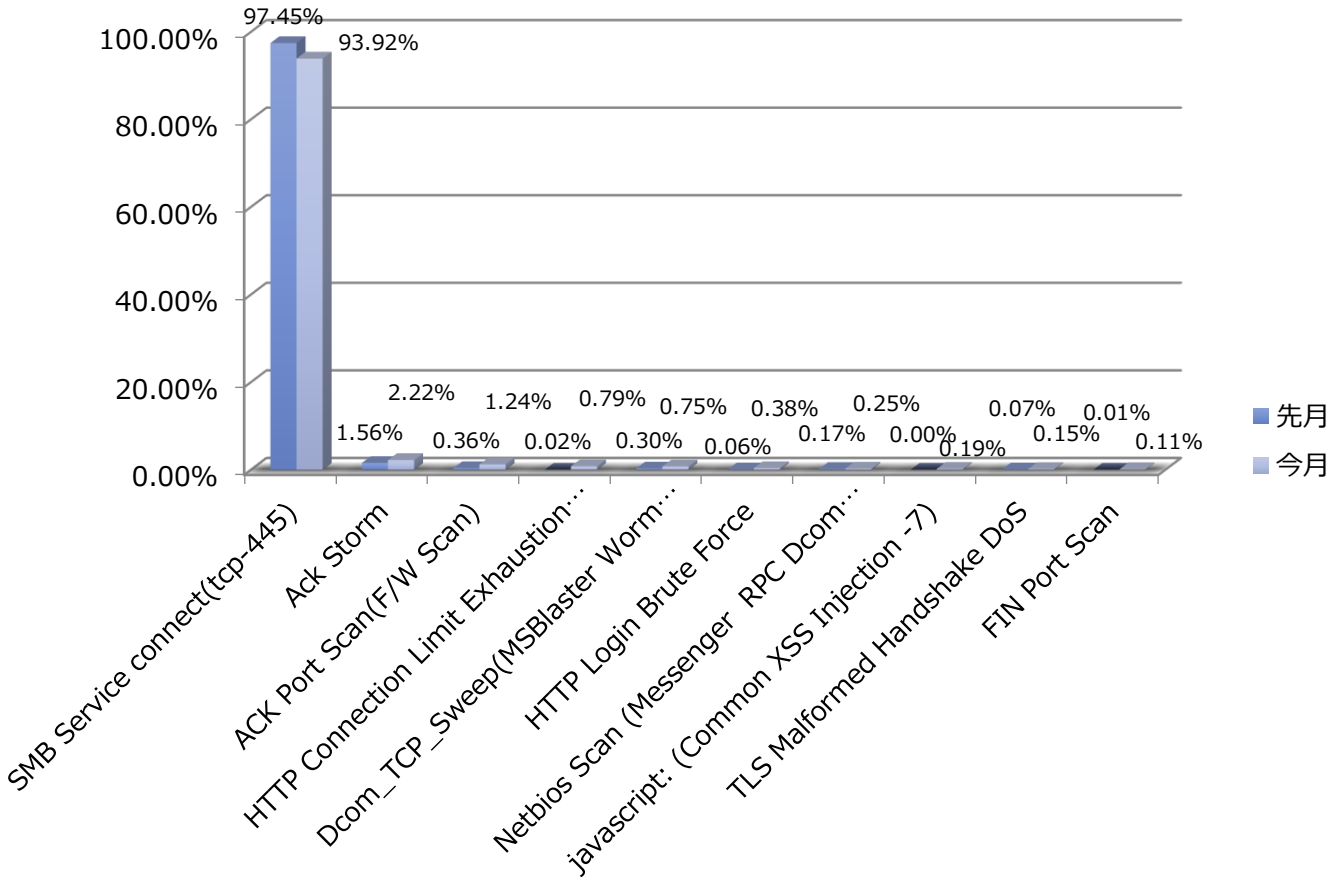
2020年10月の攻撃パターンTOP10では、HTTP Login Brute Forceイベントの順位が多少上昇し、その他、HTTP Connection Limit Exhaustion Attack(By Slowloris), javascript: (Common XSS Injection -7), FIN Port Scanイベントが新たに順位に登場した。

順位	パターン	比率(%)	先月比較
1	SMB Service connect(tcp-445)	93.92%	-
2	Ack Storm	2.22%	-
3	ACK Port Scan(F/W Scan)	1.24%	-
4	HTTP Connection Limit Exhaustion Attack(By Slowloris)	0.79%	NEW
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	0.75%	▼1
6	HTTP Login Brute Force	0.38%	▲1
7	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	0.25%	▼2
8	javascript: (Common XSS Injection -7)	0.19%	NEW
9	TLS Malformed Handshake DoS	0.15%	▼3
10	FIN Port Scan	0.11%	NEW

月次攻撃サービスの統計及び分析 - 2020年10月

06. 攻撃パターン毎のイベント比較

2020年10月の攻撃パターンTOP10では、全体的にオープンされているサービスポートに対してのスキャニングが多く、SMBサービスポートに対してのアクセスが先月と同じく90%以上になっている。最近SMBv1のリモートコード実行脆弱性であるCVE-2020-1301，SMBv3のクライアント/サーバ情報露出の脆弱性であるCVE-2020-1206など、SMBに対して最新の脆弱性が発生している。全てMicroSoft社から緊急パッチを提供しているため、Windows Updateまたは、SMBポートを使用しない場合、無効設定が必要である。



攻撃パターン毎の詳細分析結果

10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。
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は既存の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。
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。
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。
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。
javascript: (Common XSS Injection -7)	javascript: (Common XSS Injection -7)脆弱性は攻撃者がウェブアプリケーションを使用して他の最終ユーザーにJavascriptのような不正データを送る際に発生する。 最終ユーザーはこのように不正コードが含まれているウェブサイトのリンクをクリックしたり、メールに含まれている内容を読んだり、BBSに投稿されているものをクリックすることだけでユーザー環境の設定事項を変更したり、クッキー(cook-ie)を変造して広告を見せたりすることができる。
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。
FIN Port Scan	この方法は一般的なTCP PortスキャンよりListenステータスのTCPポートを探すためにTCP FINパケットに対してホストの応答を観察しScanする。FINがListeningポートに送信された場合、応答がなく、Non-Lisitening ポートに送信された場合に応答する特性を利用した攻撃であり、実際にTCP連携を初期化せずに確認ができる。