CyberFortress Report

2020
JULY

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7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

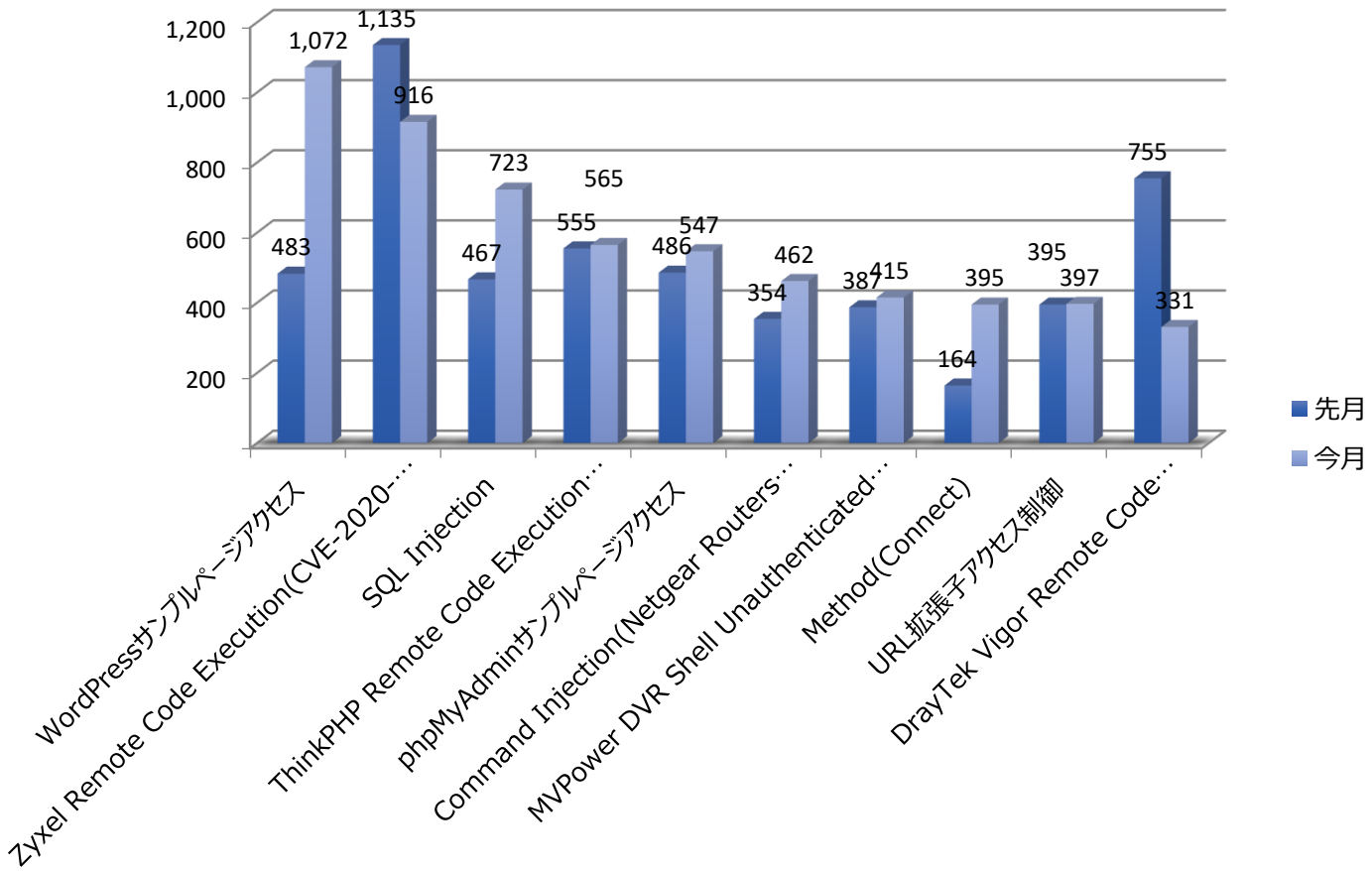
2020年7月の1ヶ月間で収取された脆弱性攻撃のTOP10では、WordPressサンプルページアクセス及びSQL InjectionのようなWEB攻撃が増えた。一方、DrayTek Vigor Remote Code Execution(CVE-2020-8515) RCE攻撃が幅広く減少した。

順位	パターン	比率(%)	先月比較
1	WordPressサンプルページアクセス	18.41%	▲4
2	Zyxel Remote Code Execution (CVE-2020-9054)	15.73%	▼1
3	SQL Injection	12.42%	▲3
4	ThinkPHP Remote Code Execution Vulnerability	9.70%	▼1
5	phpMyAdminサンプルページアクセス	9.39%	▼1
6	Command Injection (Netgear Routers Vulnerability)	7.93%	▲3
7	MVPower DVR Shell Unauthenticated Command Execution	7.13%	▲1
8	Method(Connect)	6.78%	NEW
9	URL拡張子アクセス制御	6.82%	▼2
10	DrayTek Vigor Remote Code Execution (CVE-2020-8515)	5.68%	▼8

月次攻撃サービスの統計及び分析 - 2020年7月

02. 脆弱性攻撃毎のイベントの比較

2020年7月、1ヶ月間収集されたイベントを分析した結果、2020年新規脆弱性として発見されたZyxel Remote Code Execution(CVE-2020-9054)とDrayTek Vigor Remote Code Execution(CVE-2020-8515)を利用した攻撃が多数検知された。Zyxel Remote Code Execution(CVE-2020-9054)攻撃はZyxel NAS機器のweblogin.cgiファイルの脆弱性を利用してrec攻撃ができる新しい脆弱性である。
現在セキュリティアップデートがあり、当該の機器を使用している場合、最新アップデートが必要である。



月次攻撃サービスの統計及び分析 - 2020年7月

03. 月次攻撃サービス(ポート)TOP 10

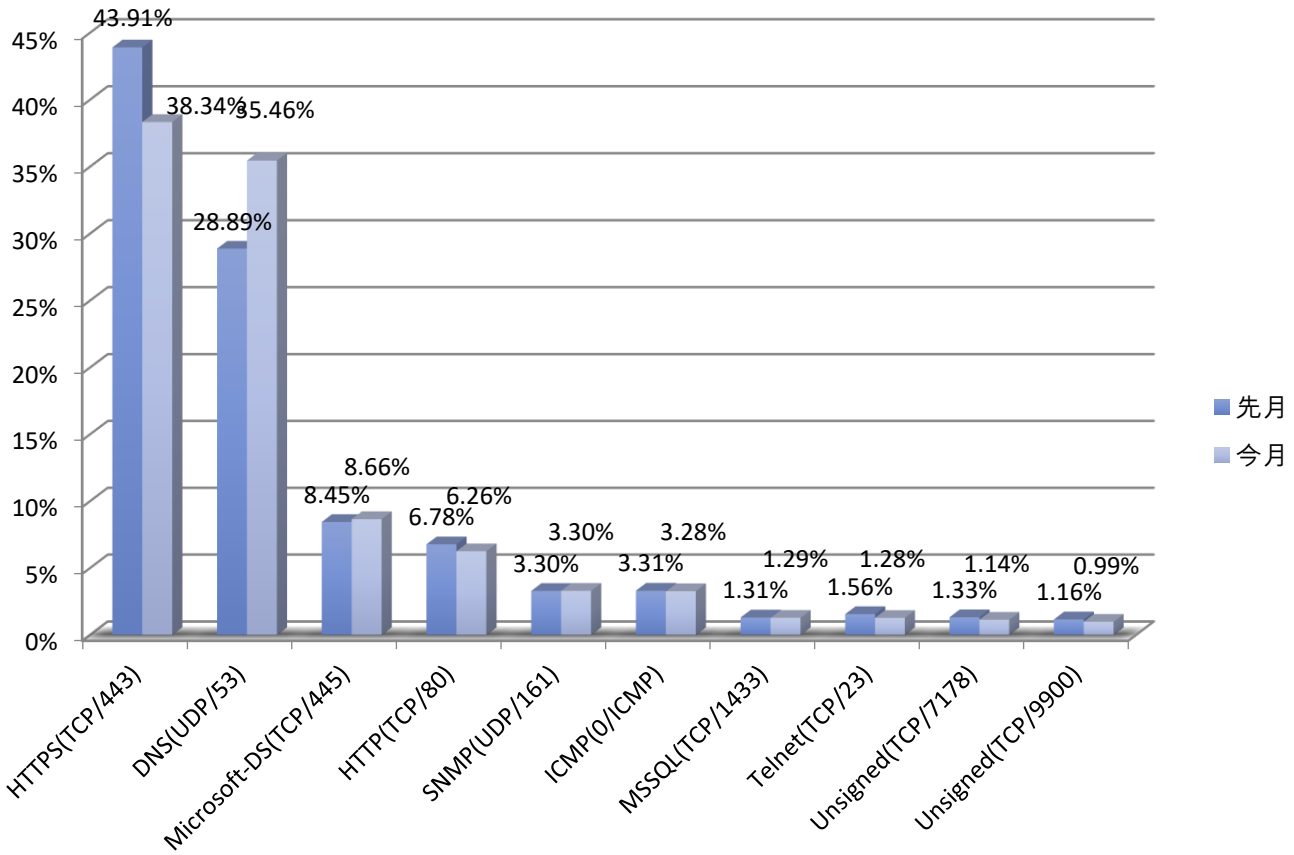
2020年7月の1ヶ月間で収取されたサービスポートのTOP10では、SNMP(UDP/161), MSSQL(TCP/1433) ポートを利用したイベントが先月比べて上昇し、ICMP(0/ICMP), Telnet(TCP/23), Unsigned(TCP/7178) は先月と比べて減少した。

順位	サービス(ポート)	比率(%)	先月比較
1	HTTPS(TCP/443)	38.34%	-
2	DNS(UDP/53)	35.46%	-
3	Microsoft-DS(TCP/445)	8.66%	-
4	HTTP(TCP/80)	6.26%	-
5	SNMP(UDP/161)	3.30%	▲1
6	ICMP(0/ICMP)	3.28%	▼1
7	MSSQL(TCP/1433)	1.29%	▲2
8	Telnet(TCP/23)	1.28%	▼1
9	Unsigned(TCP/7178)	1.14%	▼1
10	Unsigned(TCP/9900)	0.99%	-

月次攻撃サービスの統計及び分析 - 2020年7月

04. 攻撃サービス(ポート)毎のイベント比較

2020年7月、1ヶ月間収集されたイベントを分析した結果、HTTPSおよびDNSサービスポートが持続的に高く占めていて、攻撃サービスのTOP10の下位のサービスポートのほとんどがWell-Known Portに明示されていないサービスポートで確認された。不明なサービスポートの中、実際に各企業で使用しているサービスポートも存在するが、使用していないサービスポートの可能性が高いため、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、ファイアウォールのポリシー設定などでアクセスを制御する方を推奨する。



月次攻撃サービスの統計及び分析 - 2020年7月

05. 月次攻撃サービスパターンTOP 10

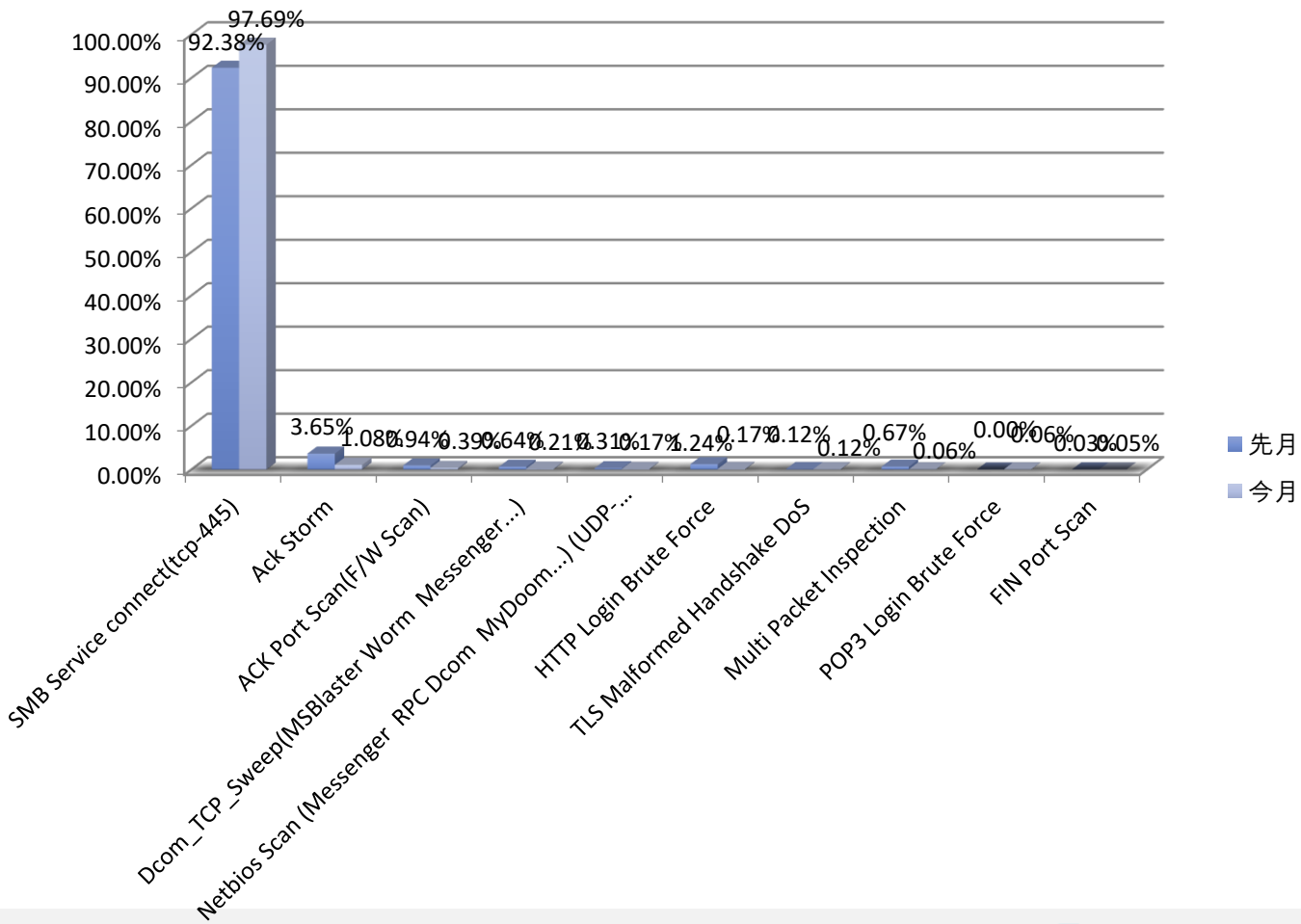
2020年7月の攻撃パターンTOP10では、ACK Port Scan(F/W Scan), Dcom_TCP_Sweep(MSBlaster Worm Messenger...), Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)のイベント順位が多少上昇し、HTTP Login Brute Force, Multi Packet Inspectionイベントの順位が下落したと判断される。その他POP3 Login Brute Forceイベントが新しく登場された。

順位	パターン	比率(%)	先月比較
1	SMB Service connect(tcp-445)	97.69%	-
2	Ack Storm	1.08%	-
3	ACK Port Scan(F/W Scan)	0.39%	▲1
4	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	0.21%	▲2
5	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	0.17%	▲2
6	HTTP Login Brute Force	0.17%	▼3
7	TLS Malformed Handshake DoS	0.12%	▲1
8	Multi Packet Inspection	0.06%	▼3
9	POP3 Login Brute Force	0.06%	NEW
10	FIN Port Scan	0.05%	-

月次攻撃サービスの統計及び分析 - 2020年7月

06. 攻撃パターン毎のイベント比較

2020年7月の攻撃パターンTOP10では、SMB Service connect(tcp-445)を利用した攻撃パターンがイベント全体の97%を占めている。従って、SMBポートに対しての格別な注意が必要だと判断される。
内部ネットワークからはSMBサービスが使用されているか確認後、ファイアウォールのポリシーを介して外部からのSMBアクセスを遮断し、内部はアンチウィルスプログラムとファイアウォールの機能を利用して他のクライアントPCから不正コード及び不要なアクセスができないように設定することを推奨する。



攻撃パターン毎の詳細分析結果

7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にたいして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。
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。
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。
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。
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。
Multi Packet Inspection	特定のIPSから発生できるルールで、IPSに設定されている自動パターン学習の防御機能によって検知される。IPSに設定されているサイズ(Bytes)より大きいパケットが同じパターンで繰り返しIPSに送信され、そのパケットがIPSに設定されているPPS以上であれば、指定されている時間の間、アクセスを遮断する。
POP3 Login Brute Force	POP3(110/tcp)にアクセスし、攻撃者がすでに作成したIDとパスワードを利用して、手作業もしくはツールなどで繰り返しログインを試す。攻撃者はシステムユーザーのアカウントを獲得することができ、アクセス権限を奪うことができる。
FIN Port Scan	この方法は一般的なTCP Portスキャンより早い方法で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てScanする。FINがListeningポートに送信された際、応答がなく、Non-Lisitening ポートに送信された際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。