CyberFortress Report

2020
JUNE

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6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

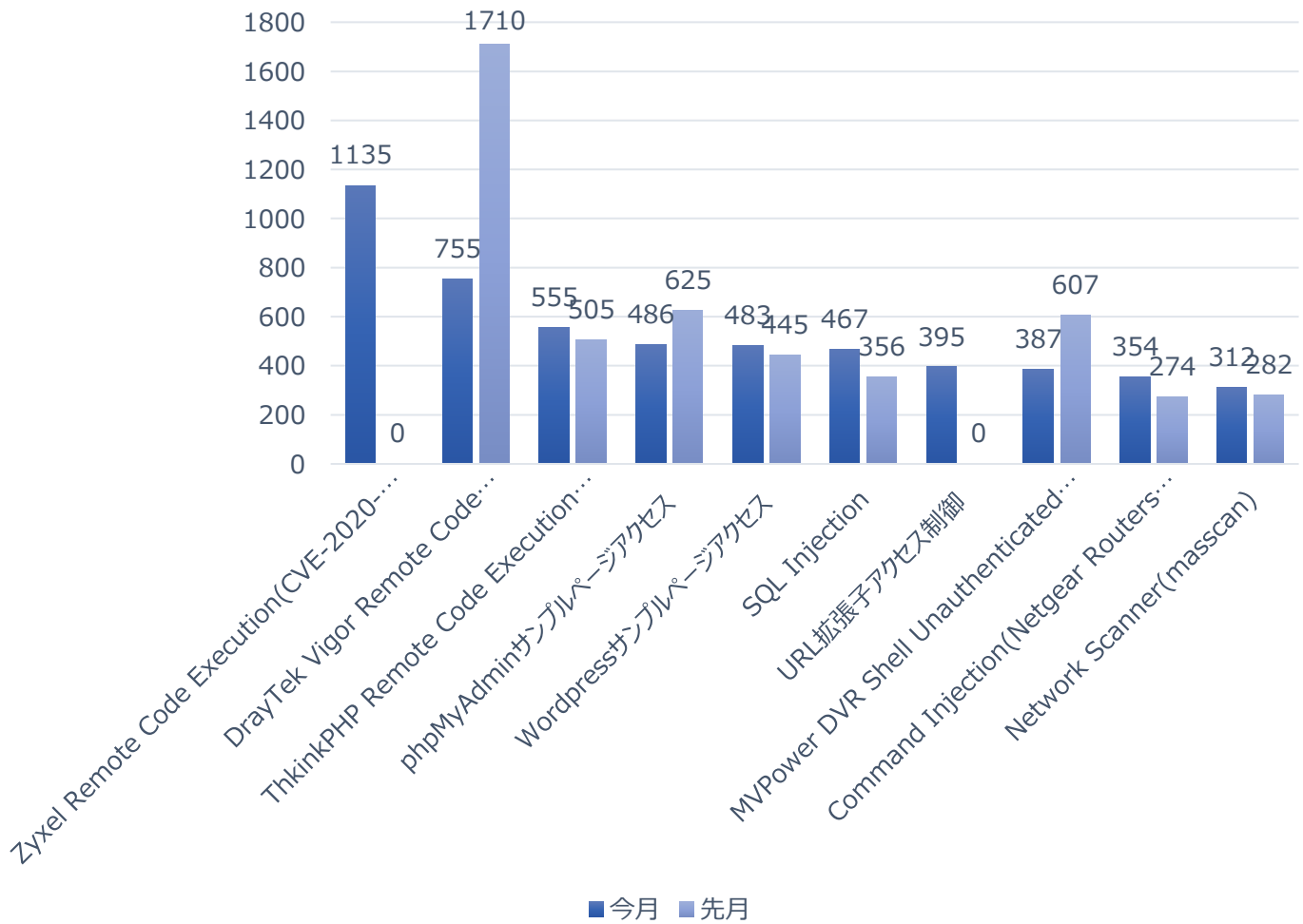
2020年6月の1ヶ月間で収取された脆弱性攻撃のTOP10では、Zyxel Remote Code Execution (CVE-2020-9054)の脆弱性を利用した攻撃及びDrayTek Vigor Remote Code Execution (CVE-2020-8515), ThinkPHP Remote Code Execution VulnerabilityのようなREC攻撃が増加している。

順位	パターン	比率(%)	先月比較
1	Zyxel Remote Code Execution (CVE-2020-9054)	21.30%	NEW
2	DrayTek Vigor Remote Code Execution (CVE-2020-8515)	14.17%	▼1
3	ThinkPHP Remote Code Execution Vulnerability	10.41%	▲1
4	phpMyAdmiサンプルページアクセス	9.12%	▼2
5	WordPresサンプルページアクセス	9.06%	-
6	SQL Injection	8.76%	▲1
7	URL拡張子アクセス制御	7.41%	NEW
8	MVPower DVR Shell Unauthenticated Command Execution	7.26%	▼5
9	Command Injection (Netgear Routers Vulnerability)	6.64%	▲1
10	Network Scanner(masscan)	5.85%	▼1

月次攻撃サービスの統計及び分析 - 2020年6月

02. 脆弱性攻撃毎のイベントの比較

2020年6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6月

03. 月次攻撃サービス(ポート)TOP 10

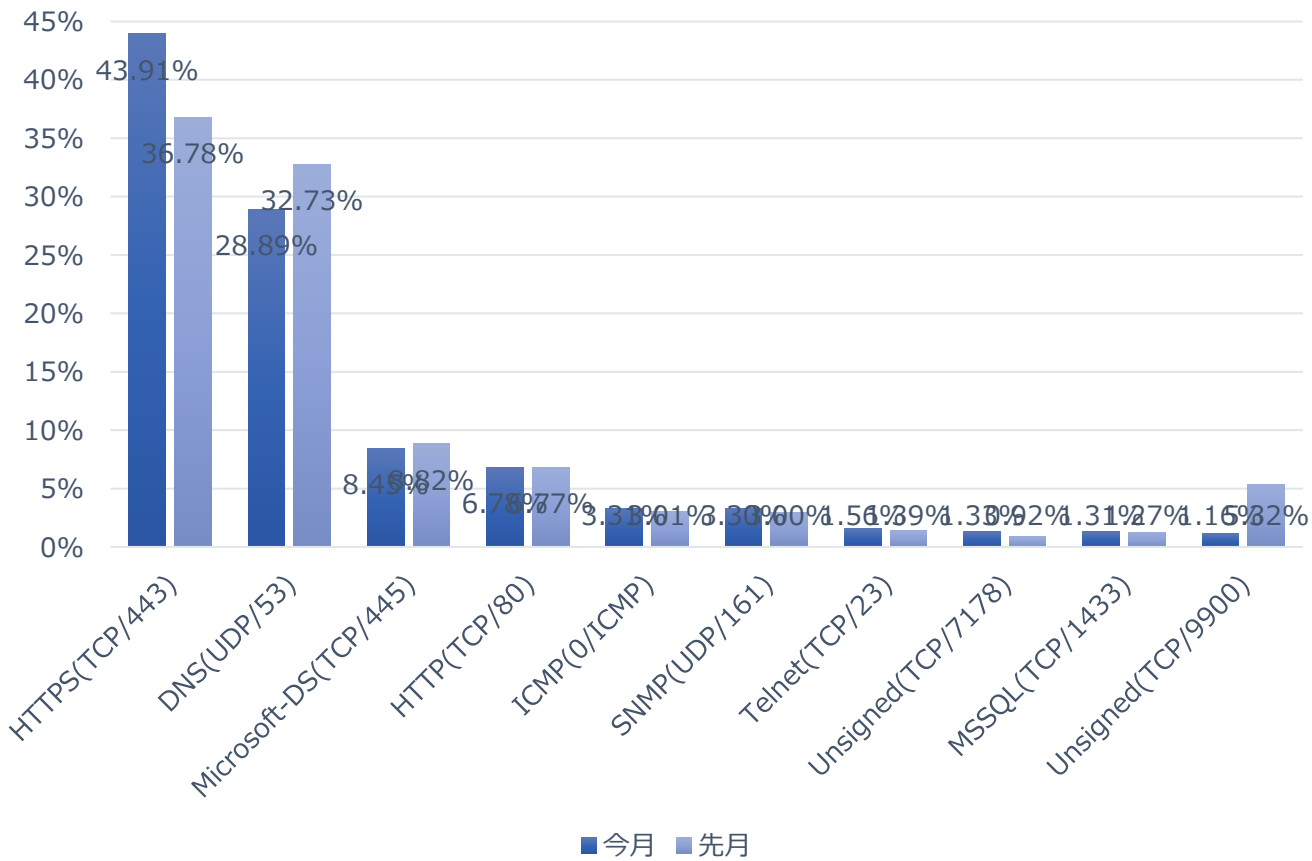
2020年6月の1ヶ月間で収取されたサービスポートのTOP10では、ICMP(0/ICMP), SNMP(UDP/161), Telnet(TCP/23), Unsigned(TCP/7178) ポートを利用したイベントが先月と比べて上昇し、Unsigned(TCP/9900)ポートは先月と比べて減少した。

順位	サービス(ポート)	比率(%)	先月比較
1	HTTPS(TCP/443)	43.91%	-
2	DNS(UDP/53)	28.89%	-
3	Microsoft-DS(TCP/445)	8.45%	-
4	HTTP(TCP/80)	6.78%	-
5	ICMP(0/ICMP)	3.31%	▲1
6	SNMP(UDP/161)	3.30%	▲1
7	Telnet(TCP/23)	1.56%	▲1
8	Unsigned(TCP/7178)	1.33%	▲2
9	MSSQL(TCP/1433)	1.31%	-
10	Unsigned(TCP/9900)	1.16%	▼5

月次攻撃サービスの統計及び分析 - 2020年6月

04. 攻撃サービス(ポート)毎のイベント比較

2020年6月、1ヶ月間収集されたイベントを分析した結果、先月と比べて少し減少した。
ICMP(0/ICMP), SNMP(UDP/161), Telnet(TCP/23), Unsigned(TCP/7178)ポートを利用したイベントが先月比べて増加した。その中でICMPイベントはSniffing, ICMP Redirection, Spoofing攻撃に利用される可能性が高いプロトコルで、なるべくセキュリティ機器のICMP設定は無効化し、reply/request packetを介して情報が漏出されないように管理するのを推奨する。



月次攻撃サービスの統計及び分析 - 2020年6月

05. 月次攻撃サービスパターンTOP 10

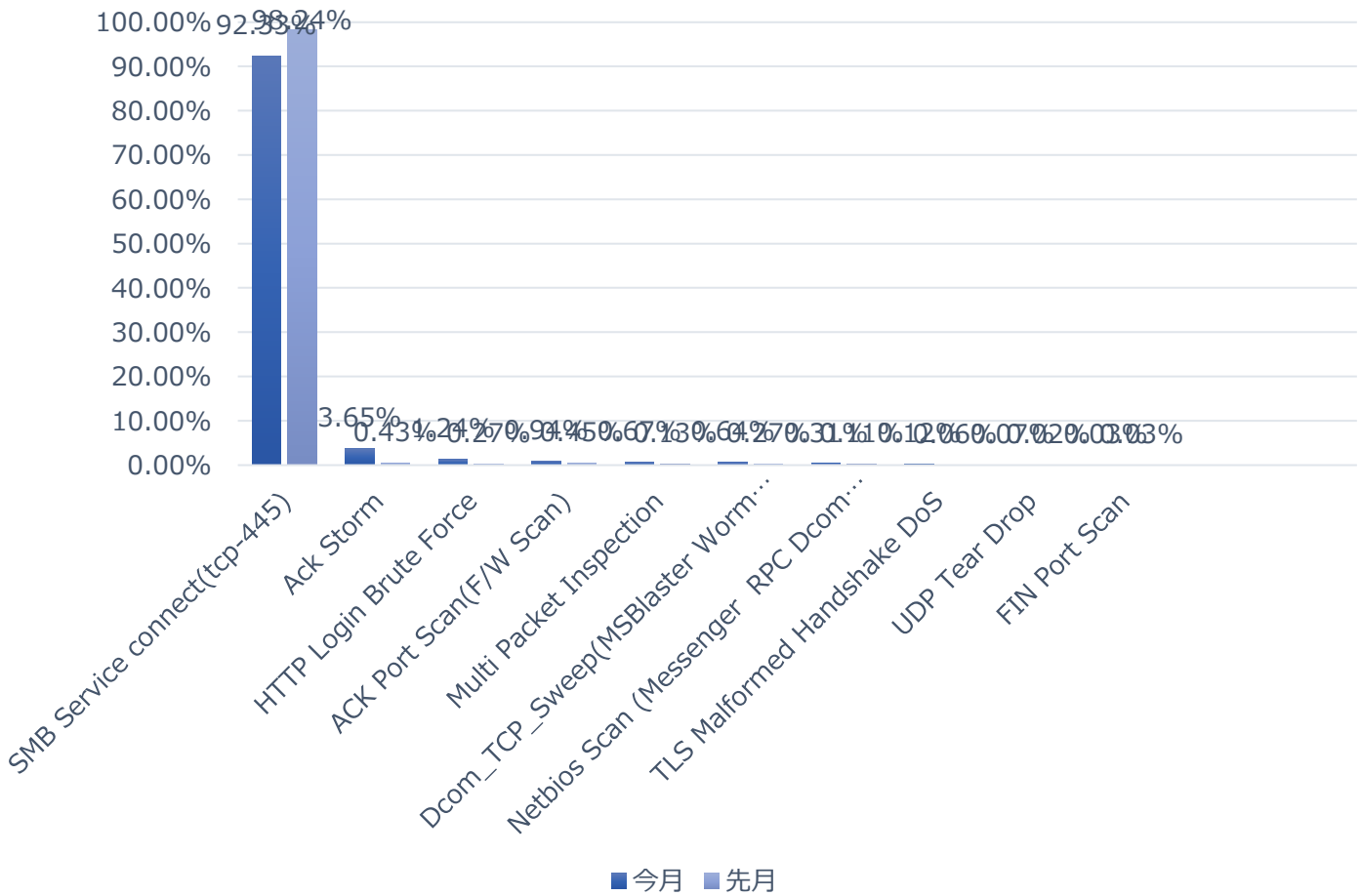
2020年6月の攻撃パターンTOP10では、Ack Storm, HTTP Login Brute Force, Multi Packet Inspection のイベントの順位が多少上昇し、ACK Port Scan(F/W Scan), Dcom_TCP_Sweep(MSBlaster Worm Messengr)のイベントの順位が下落したことが確認できた。その他、UDP Tear Drop, FIN Port Scanイベントが新しく確認できた。

順位	パターン	比率(%)	先月比較
1	SMB Service connect(tcp-445)	92.33%	-
2	Ack Storm	3.62%	▲1
3	HTTP Login Brute Force	1.23%	▲1
4	ACK Port Scan(F/W Scan)	0.93%	▼2
5	Multi Packet Inspection	0.67%	▲1
6	Dcom_TCP_Sweep (MSBlaster Worm Messenger)	0.64%	▼1
7	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	0.31%	-
8	TLS Malformed Handshake DoS	0.12%	-
9	UDP Tear Drop	0.07%	NEW
10	FIN Port Scan	0.03%	NEW

月次攻撃サービスの統計及び分析 - 2020年6月

06. 攻撃パターン毎のイベント比較

2020年6月の攻撃パターンTOP10では、先月と比べてSMB Service connect(tcp-445)の件数が幅広く下落したが、それでも1位の順位にある攻撃パターンでSMB及びNetbiosサービスポートに対して持続的なアクセス制御が必要である。UDP Tear Drop, FIN Port Scanパターンが新しく順位に入り、今月6月の順位の中の攻撃がほぼScan, Bute Forceのようなスキャニングイベントであることが確認できる。アクセスができる未使用ポートの把握及び各種機器及びサーバのパスワードの複雑性検証なでのセキュリティ処置を推奨する。



攻撃パターン毎の詳細分析結果

06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。
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。
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。
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。
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。
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。
UDP Tear Drop	正常のパケットを送信するたびに断片化が発生すると再構成時、正確に構成するためにoffset値を加えることになっている。当該のパターンはUDPを利用して正常のoffset値より大きい値を加えてその範囲を超えるoverflowを起こしてシステムの機能を麻痺させるDoS攻撃の一種である。
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。