CyberFortress Report

2020
SEP

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9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

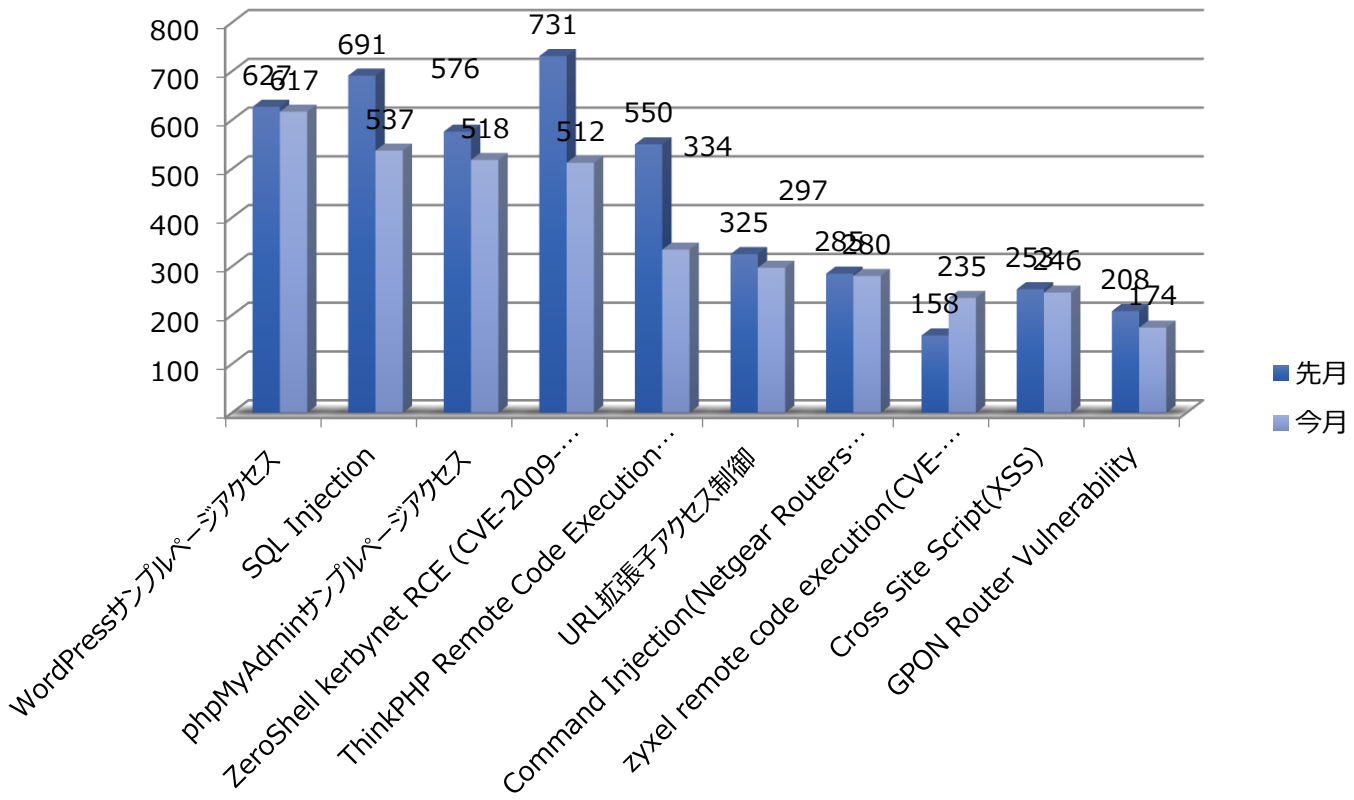
2020年9月、1ヶ月間収集された脆弱性攻撃のTOP10ではzyxel remote code execution(CVE-2020-9054), Cross Site Script(XSS), GPON Router Vulnerability 脆弱性を利用した攻撃が新たに順位に登場した。その他、WordPressサンプルページアクセス、SQL Injection, phpMyAdminサンプルページ攻撃のパターンが先月と比べて、上位に登場した。

順位	パターン	比率(%)	
1	WordPressサンプルページアクセス	16.45%	▲3
2	SQL Injection	14.32%	▲1
3	phpMyAdminサンプルページアクセス	13.81%	▲2
4	ZeroShell kerbynet RCE (CVE-2009-0545)	13.65%	▼2
5	ThinkPHP Remote Code Execution Vulnerability	8.91%	▲1
6	URL拡張子アクセス制御	7.92%	▲2
7	Command Injection (Netgear Routers Vulnerability)	7.47%	▲2
8	zyxel remote code execution (CVE-2020-9054)	6.27%	NEW
9	Cross Site Script(XSS)	6.56%	NEW
10	GPON Router Vulnerability	4.64%	NEW

月次攻撃サービスの統計及び分析 - 2020年9月

02. 脆弱性攻撃毎のイベントの比較

2020年9月、1ヶ月間収集されたイベントを分析した結果、先月とくらべてTOP10の全体の件数は減少したが、Wordpressサンプルページアクセス、SQL Injection, phpMyAdminサンプルページアクセスのようなウェブスキャナーを利用したウェブ脆弱性の攻撃が持続的に発生している。その為、管理者は基本、不要なウェブページの削除及びSQL Injection攻撃に備えたウェブページ管理が必要である。



月次攻撃サービスの統計及び分析 - 2020年9月

03. 月次攻撃サービス(ポート)TOP 10

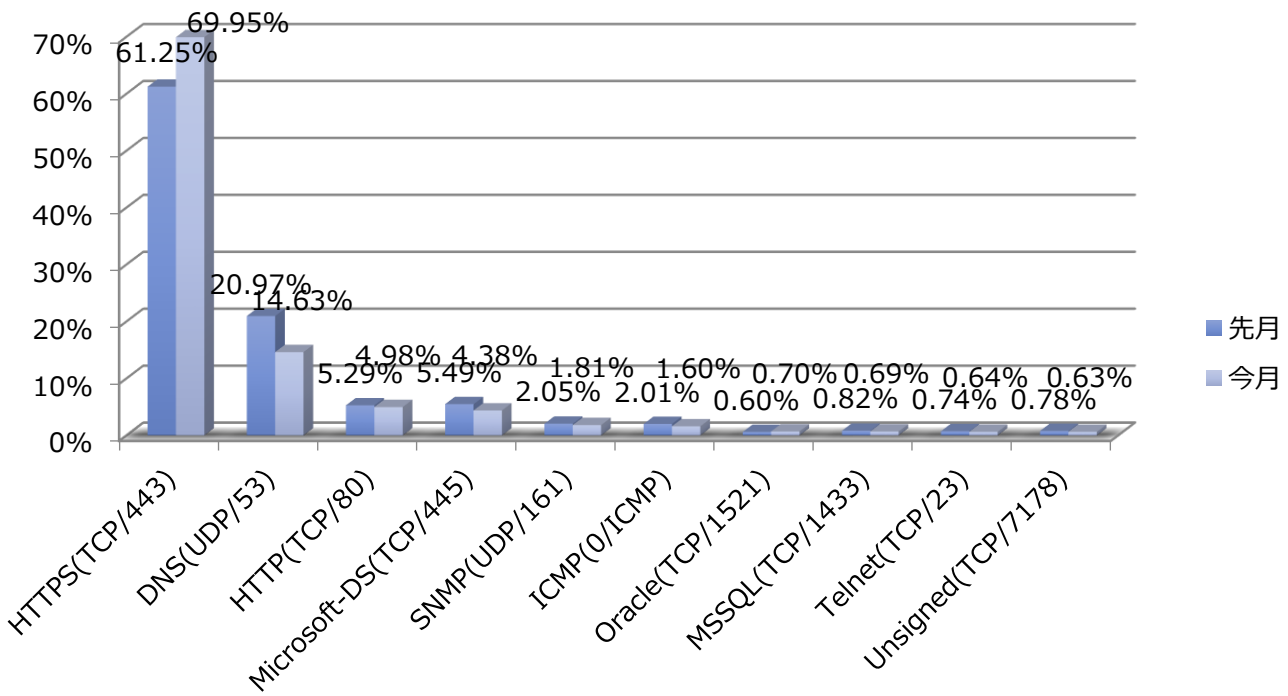
2020年9月の1ヶ月間で収取されたサービスポートのTOP10では、Oracle(TCP/1521)ポートを利用したイベントが先月と比べて1,000万件以上増加し、順位が3段階上がった、その他、Microsoft-DS(TCP/445), MSSQL(TCP/1433), Unsigned(TCP/7178)ポートを利用したイベントが先月と比べ小幅に減少した。

順位	サービス(ポート)	比率(%)	先月比較
1	HTTPS(TCP/443)	69.95%	-
2	DNS(UDP/53)	14.63%	-
3	HTTP(TCP/80)	4.98%	▲1
4	Microsoft-DS(TCP/445)	4.38%	▼1
5	SNMP(UDP/161)	1.81%	-
6	ICMP(0/ICMP)	1.60%	-
7	Oracle(TCP/1521)	0.70%	▲3
8	MSSQL(TCP/1433)	0.69%	▼1
9	Telnet(TCP/23)	0.64%	-
10	Unsigned(TCP/7178)	0.63%	▼2

月次攻撃サービスの統計及び分析 - 2020年9月

04. 攻撃サービス(ポート)毎のイベント比較

2020年9月、1ヶ月間収集されたイベントを分析した結果、先月TOP10に新たに登場したOracle(TCP/1521)ポートが今月1,000万件以上増加してイベント件数が持続的に増加している。攻撃者はOracle DBにアクセス成功時、SQL文を使用して内部システム情報を検索、挿入、修正などができるため、外部に漏出したらアクセスできないようにアクセス制御及び集中監視が必要である。



月次攻撃サービスの統計及び分析 - 2020年9月

05. 月次攻撃サービスパターンTOP 10

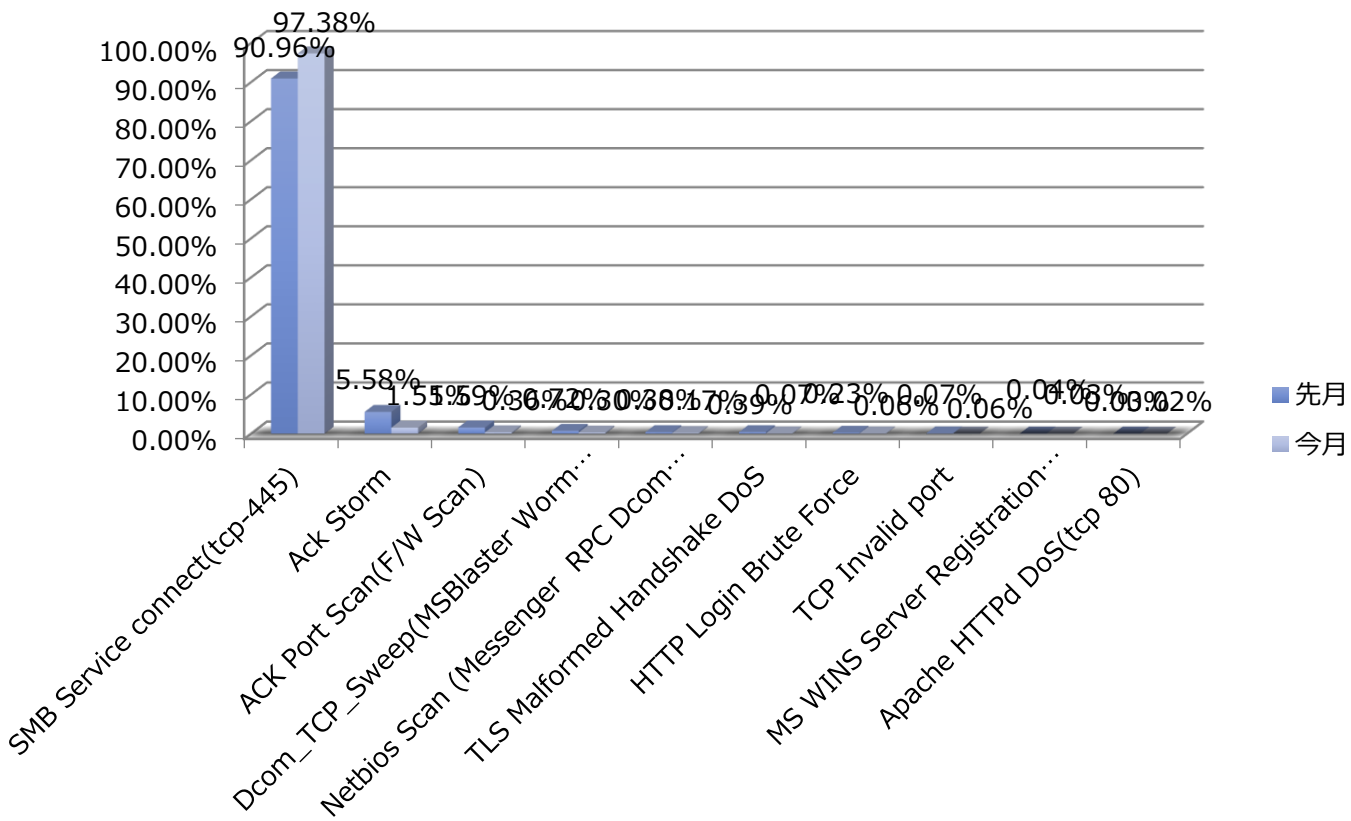
2020年9月の攻撃パターンTOP10では、Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137), TCP Invalid portのイベント順位が多少上昇し、その他、 MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137), Apache HTTPd DoS(tcp 80)イベントが新たに順位に登場した。

順位	パターン	比率(%)	先月比較
1	SMB Service connect(tcp-445)	97.38%	-
2	Ack Storm	1.55%	-
3	ACK Port Scan(F/W Scan)	0.36%	-
4	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	0.30%	-
5	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	0.17%	▲1
6	TLS Malformed Handshake DoS	0.07%	▼1
7	HTTP Login Brute Force	0.06%	-
8	TCP Invalid port	0.06%	▲2
9	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	0.03%	NEW
10	Apache HTTPd DoS(tcp 80)	0.02%	NEW

月次攻撃サービスの統計及び分析 - 2020年9月

06. 攻撃パターン毎のイベント比較

2020年9月の攻撃パターンTOP10では、 MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137), Apache HTTPd DoS(tcp 80)イベントが新たにTOP10に登場し、TCP Invalid portイベントが先月と比べて40万件以上増加した。当該のイベントはSource Port及びDestination Port両方からWell-Know portを使用して、通信を試したり、通常使わいポートでデータを送信し、被害者のサーバの情報を把握するための攻撃で使用できる。管理者は通常使用しないポート通信に対して監視及びアクセス制御を推奨する。



攻撃パターン毎の詳細分析結果

09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。
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。
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。
TCP Invaild Port	ネットワーク規約(RFC 1700)によると、0番ポートはreservedポートでPublicネットワークでは通常使用されない。1024番以下のポートはwell-knownポートで通常SourceとDestinationの両方well-knownポートを使用しない。(ただし、20のftp-dataサービスを提供する場合は例外とする。)。このように通常的に使用されていないポートにデータを送ることで、受信システムに演算エラーを起こしたり、受信者のOSを把握するfingerprint攻撃で使用される可能性がある。
MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	当該の攻撃はWindows WINSサーバにネームが登録される中でNetBIOS通信ネームが適切に検証されていないため発生する脆弱性である。 脆弱性を利用して攻撃者はウェブプロキシをスプーフィングし、攻撃者が選択したアドレスにトラフィックをリダイレクトできる。
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。