CyberFortress Report

2020
AUGUST

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8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

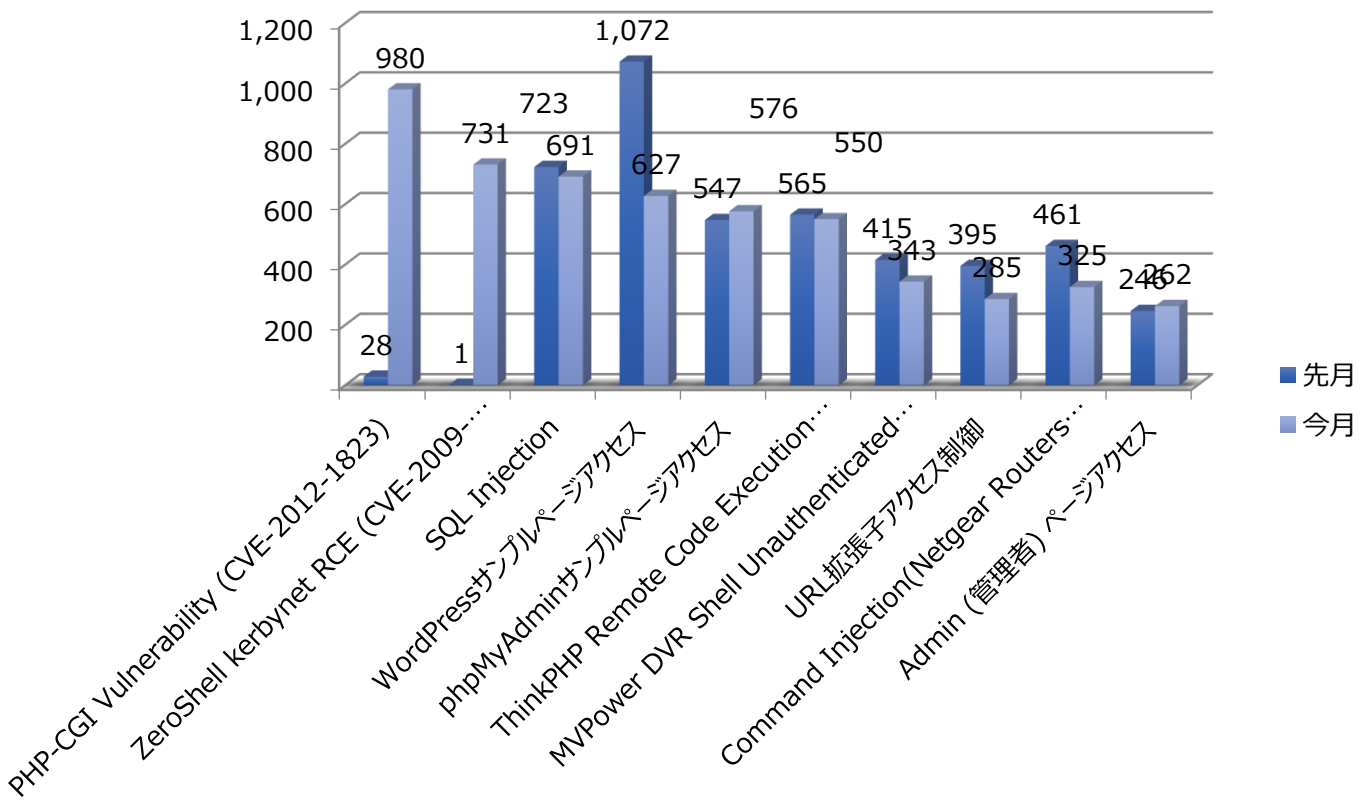
PHP-CGI Vulnerability (CVE-2012-1823), ZeroShell kerbynet RCE (CVE-2009-0545), Admin (管理者) ページアクセス脆弱性を利用した攻撃が新たに登場した。その他、先月は高い順位であったWordPress サンプルページアクセス、ThinkPHP Remote Code Execution Vulnerability脆弱性攻撃は減少した。

順位	パターン	比率(%)	先月比較
1	PHP-CGI Vulnerability (CVE-2012-1823)	18.25%	NEW
2	ZeroShell kerbynet RCE (CVE-2009-0545)	13.61%	NEW
3	SQL Injection	12.87%	-
4	WordPressサンプルページアクセス	11.68%	▼3
5	phpMyAdminサンプルページアクセス	10.73%	-
6	ThinkPHP Remote Code Execution Vulnerability	10.24%	▼2
7	MVPower DVR Shell Unauthenticated Command Execution	6.39%	-
8	URL拡張子アクセス制御	5.31%	▲1
9	Command Injection (Netgear Routers Vulnerability)	6.05%	▼3
10	Admin (管理者) ページアクセス	4.88%	NEW

月次攻撃サービスの統計及び分析 - 2020年8月

02. 脆弱性攻撃毎のイベントの比較

2020年8月、1ヶ月間収集されたイベントを分析した結果、PHP-CGI Vulnerability (CVE-2012-1823), ZeroShell kerbynet RCE (CVE-2009-0545)脆弱性を利用した攻撃が幅広く増加し、Top 10に新たに登場した。PHP-CGI Vulnerability (CVE-2012-1823)はリモート攻撃者が脆弱なphp-cgiを利用し、-dオプションを介してphpの環境変数を操作、phpコードが実行できる環境を作り、攻撃者がphpコードを挿入してコードを実行する脆弱性である。当該の脆弱性はphpバージョン5.3.12及び5.4.2以下のバージョンから発生する。脆弱なバージョンのphpを使用している場合、最新アップデートを推奨する。



月次攻撃サービスの統計及び分析 - 2020年8月

03. 月次攻撃サービス(ポート)TOP 10

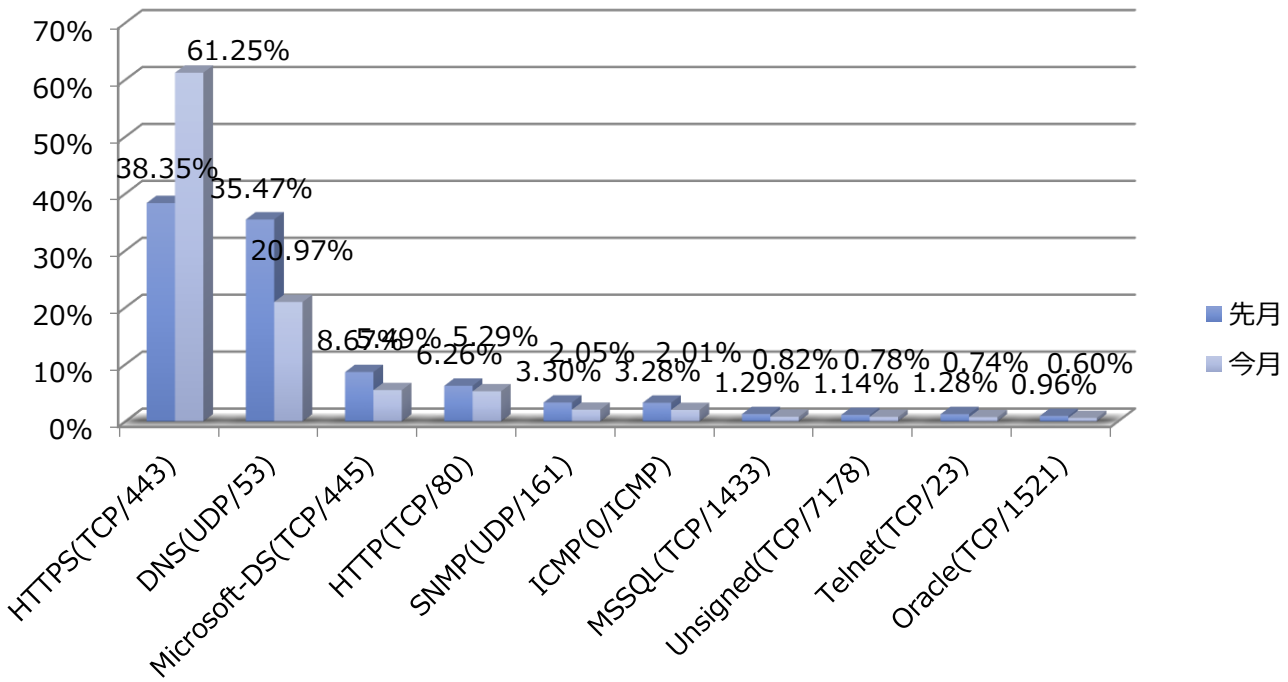
2020年8月の1ヶ月間で収取されたサービスポートのTOP10では、 先月と比べてHTTPS(TCP/443)ポートの使用件数が急増し、Oracle(TCP/1521)ポートが新たにTop 10に登場した。その他、サービスポートの順位に大きい変動はない。

順位	サービス(ポート)	比率(%)	先月比較
1	HTTPS(TCP/443)	61.25%	-
2	DNS(UDP/53)	20.97%	-
3	Microsoft-DS(TCP/445)	5.49%	-
4	HTTP(TCP/80)	5.29%	-
5	SNMP(UDP/161)	2.05%	-
6	ICMP(0/ICMP)	2.01%	-
7	MSSQL(TCP/1433)	0.82%	-
8	Unsigned(TCP/7178)	0.78%	▲1
9	Telnet(TCP/23)	0.74%	▼1
10	Oracle(TCP/1521)	0.60%	NEW

月次攻撃サービスの統計及び分析 - 2020年8月

04. 攻撃サービス(ポート)毎のイベント比較

2020年8月、1ヶ月間収集されたイベントを分析した結果、 HTTP及びDNSサービスポートが持続的に高いシェアを占めていて、今月Oracle(TCP/1521)サービスポートが新たにTOP 10に登場した。Oracle DBに対してのPort Scan攻撃が多数増加し、先月と比べてOracle(TCP/1521)サービスポートに対してのイベントが増加しているとみられている。SQLクエリを使用して内部システムの情報を検索、挿入、修正などができるため、外部に漏出されたり、アクセスできないように周期的なチェック及び監視が必要である。



月次攻撃サービスの統計及び分析 - 2020年8月

05. 月次攻撃サービスパターンTOP 10

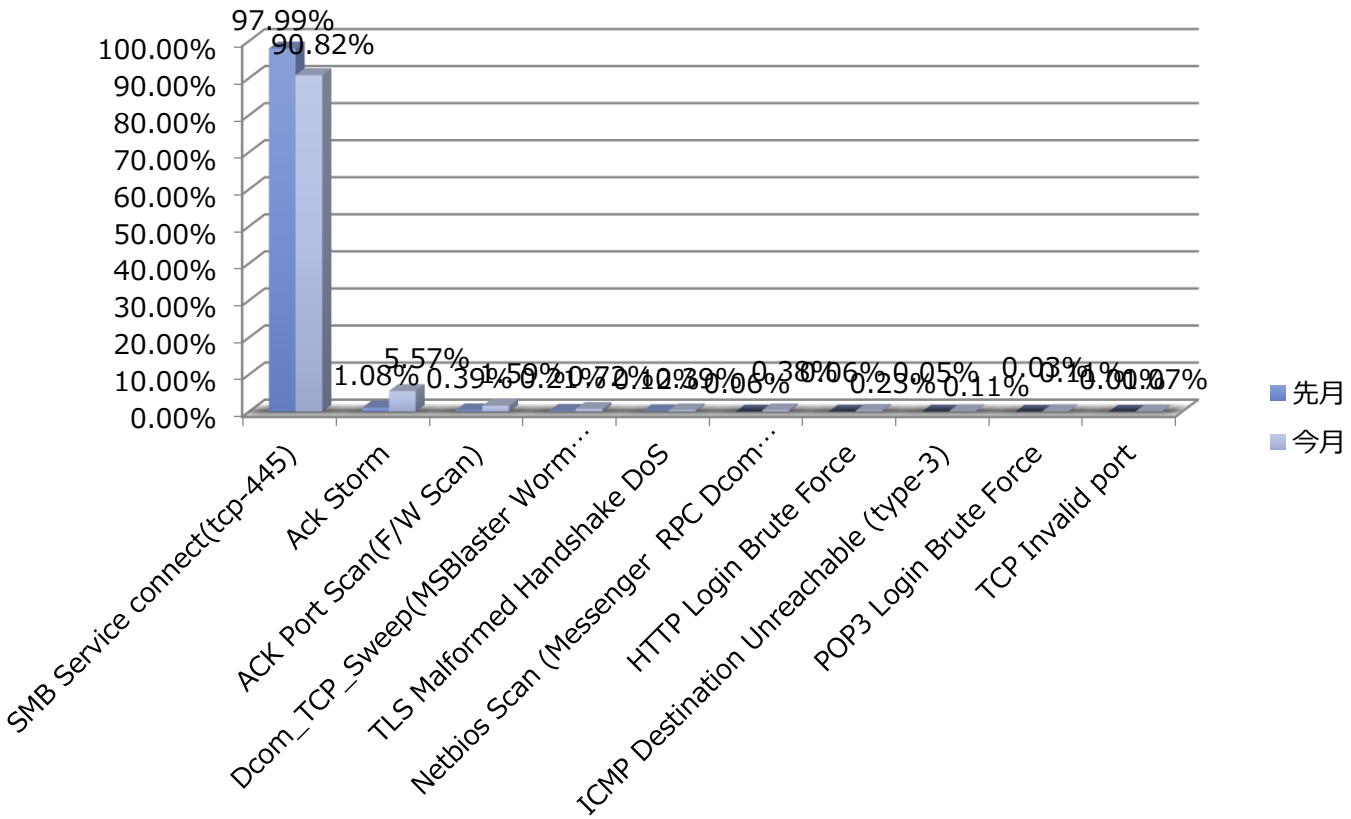
2020年8月の攻撃パターンTOP10では、 TLS Malformed Handshake DoSイベントの順位が多少増加し、Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137), HTTP Login Brute Forceイベントの順位が下落したと見られている。その他、TCP Invalid portイベントが新たに登場した。

順位	パターン	比率(%)	先月比較
1	SMB Service connect(tcp-445)	90.82%	-
2	Ack Storm	5.57%	-
3	ACK Port Scan(F/W Scan)	1.59%	-
4	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	0.72%	-
5	TLS Malformed Handshake DoS	0.39%	▲2
6	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	0.38%	▼1
7	HTTP Login Brute Force	0.23%	▼1
8	Multi Packet Inspection	0.11%	-
9	POP3 Login Brute Force	0.11%	-
10	TCP Invalid port	0.07%	NEW

月次攻撃サービスの統計及び分析 - 2020年8月

06. 攻撃パターン毎のイベント比較

2020年8月の攻撃パターンTOP10では、TCP Invalid portイベントが新たに登場し、SMB Service connect(tcp-445)を利用した攻撃パターンが先月と比べて件数は大幅に減少した。しかし、まだ高いシェアを持っているため、注意が必要である。セキュリティ管理者はSMBサービスの使用有無を確認後、使用していない場合、445, 135, 139ポートに対してセキュリティ機器及びサーバのACL(Access Control List)設定を推奨する。SMBサービスを使用している場合、周期的なセキュリティアップデートを通じてセキュリティに強化及びユーザーアカウントの分かりやすいパスワードの使用禁止などの対処を推奨する。



攻撃パターン毎の詳細分析結果

08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。
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。
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。
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とパスワードをリストとして登録し、手作業もしくはツールなどを利用して繰り返してログインを試す。攻撃者はシステムユーザーのアカウントを獲得し、アクセス権限を奪うことができる。
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の共にwell-knownポートを使用しない。(ただし、20番ポートがftp-dataサービスを提供する場合は例外とする。)。このように一般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。