— ＡＵＳ（アルテミス・ユーザ・サポート）便り 2015/11/02号 —

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●2015年第３四半期に狙われたポート番号は「23/TCP(telnet)」がトップ･･･JPCERT/CC

http://itpro.nikkeibp.co.jp/atcl/news/14/110601779/103000379/
https://www.jpcert.or.jp/press/2015.html

このニュースをザックリ言うと･･･

- 10月29日（日本時間）、セキュリティ専門機関JPCERT/CCより、インターネット上の攻撃動向に関する定点観測の2015年第3四半期（7月～9月）の結果が発表されました。

- 何らかの攻撃活動・準備活動の準備（ポートスキャン(※)など）とみられるパケットのうち、宛先ポート番号(※)別で最も多いのはtelnetサービスを狙うTCPポート23番宛で、特に9月前半には1日6,000～8,000パケット台を推移、同月下旬からは9,000パケット台へ右肩上がりの増加傾向を示しています。

- この他での注目点としては、警察庁も9月20日に同様の定点観測で警告した、マルウェア「SYNful Knock」に感染した米Cisco Systems社製ルータを検索するとみられるパケットについて、同月下旬に1日20パケット程度が観測されていることを挙げています。

AUS便りからの所感等

- 今日におけるtelnetサービスの役割はネットワーク機器のコマンドベースでの管理程度であり、不特定多数が外部からアクセス可能な状態であるのは、意図的なものではない限り、アクセス制限の設定ミスである可能性が高いと言えます。

- 管理のために外部ネットワークからtelnetアクセスが必要である場合は、固定IPアドレスからアクセスを行うようにし、他のアドレスからのアクセスが拒否されているか必ず確認しましょう。

- 特にこれができないケースや不用意な設定ミスを防ぐためにも、UTMを前面に設置することにより、攻撃者が多数のログイン試行等によって不正ログインを行おうとするのを検知・遮断することが期待できます。

統計＆調査

[データは語る]2015年第3四半期に狙われたポート番号は「23/TCP (telnet)」がトップ―JPCERT/CC

2015/10/30
下玉利 尚明＝タンクフル（筆者執筆記事一覧）

記事一覧へ >>

JPCERTコーディネーションセンター（JPCERT/CC）は2015年10月29日、不特定多数に向けて発信されるパケットを継続的に収集し、脆弱性情報、マルウエアや攻撃ツールの情報などと対比して分析した「インターネット定点観測レポート」を発表した。それによると、2015年第3四半期（7月～9月）に観測された日本宛てのパケットでは、「23/TCP（telnet）」がトップで、次いで前四半期4位だった「0/ICMP」が2位に、同2位だった「445/TCP（microsoft-ds）」が3位となった。

JPCERT/CCでは、送信元地域についても調査。それによると、1位は中国で、2位はアメリカで、順位の変更はなく、3位に同4位だった日本が入り、4位に同3位だった台湾となった。5位はオランダだった。

JPCERT/CCでは、Telnetサーバーを搭載したネットワーク機器を探索する活動について、今四半期も23/TCP宛てのパケットを多数観測したと発表。また、9月24日から10月上旬に、主に中国、米国を送信元とするパケット数が増加したと分析。しかし、これらは特定のセンサーが1900/UDP宛てにSSDPのM-SEARCHリクエストのパケットを一時的に多数受信した影響によるもので、顕著な変化は見られなかったと指摘した。そのためJPCERT/CCでは、広域的な脅威を示すデータではないと判断したという。

IT用語辞典 e-Words

（※）ポートスキャン【 port scan 】ポートスキャニング / port scanning

ポートスキャンとは、ネットワークを通じてサーバに連続してアクセスし、保安上の弱点（セキュリティホール）を探す行為。

インターネット上で公開されているサーバコンピュータは「TCP/IP」と呼ばれる通信規約（プロトコル）に従って動作しており、通常は「ポート」と呼ばれる接続窓口を複数用意して、利用者からの接続を待っている。

ポートスキャンは、このポートに順番にアクセスし、サーバ内で動作しているアプリケーションソフトやOSの種類を調べ、侵入口となりうる脆弱なポートがないかどうか調べる行為である。

ポートスキャンの結果、セキュリティホールが発見されると、侵入用のプログラムを使って不正侵入を行うことが多い。

ネットワーク管理者が、自分の管理するシステムに弱点がないかどうか調べるためにポートスキャンを行う場合もある。

ポートスキャンを受けたサーバは、通信履歴（アクセスログ）にポートスキャンとおぼしき不審な記録が残るが、間隔を空けてスキャンを行うなど、ポートスキャンの発生を隠蔽する工作が行われている場合もある。

（※）ポート番号【 port number 】

ポート番号とは、インターネット上の通信において、複数の相手と同時に接続を行うためにIPアドレスの下に設けられたサブ（補助）アドレス。単にポートと略されることもある。

TCP/IPで通信を行うコンピュータはネットワーク内での住所にあたるIPアドレスを持っているが、複数のコンピュータと同時に通信するために、補助アドレスとして0から65535のポート番号を用いる。

IPアドレスとポート番号を組み合わせたネットワークアドレスを「ソケット」と呼び、実際にはデータの送受信はソケット単位で行われる。実世界の住所で例えれば、マンションの所在地（「〇〇市××町4-2-1 コーポ△△」）がIPアドレスにあたり、部屋番号（「305号室」）がポート番号に対応する。

（TCP/IPの有名ポート番号）

22番（TCP/UDP）ssh、23番（TCP）Telnet、25番（TCP/UDP）SMTP、53番（TCP/UDP）DNS、80番（TCP/UDP）HTTP、110番（TCP）POP3、443番（TCP/UDP）HTTPS、587番（TCP）SMTP Message Submission など

●ウイルスメール1万1000通以上の送信を確認、今度は「請求書」や「FAX受信通知」に偽装

http://news.mynavi.jp/news/2015/10/28/254/

このニュースをザックリ言うと・・・

- 10月27日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、同日朝に3種のウイルスメール計1万1000通以上の送信が確認されたとして警告が出されました。

- ウイルスメールは、実在の印刷会社および建設会社からの請求書に偽装したメール2種（件名は「タンケンー請求書（小）の件です」および「請求書」）と、やはり実在のレンタルオフィス会社からのFAX受信通知に偽装したメール1種（件名は「ファックス受信完了：Fax Received」）からなります。

- いずれも不正なマクロを含んだWord文書が添付されており、これを開くことにより、オンラインバンキングの認証情報を奪取するマルウェア「SHIZ」に感染する可能性があるとされています。

- 同社では、誤って不正なマクロを含むWordファイルを開き「マクロが無効にされました」というメッセージが表示されてもそのままマクロを有効化してしまい、結局マルウェアに感染してしまうケースが見受けられるとして、無闇にマクロの有効化をしないよう注意を呼びかけています。

AUS便りからの所感等

- トレンドマイクロ社は6月や9月にも同様のウイルスメールについて警告しており、最近では10月9日、初めて2種類のウイルスメールが送信されたとしていますが、今回は更に同時送信される種類が増えています。

- とにかく、送信元と関係があったり、あるいは関係がなくとも、添付ファイルの中身に興味を持つなどによりマルウェアに感染してしまう可能性を抑制するためにも、アンチウイルスやUTMによるファイルのチェックを全てのケースにおいて行うことが肝要です。

マイナビニュース

マルウェアを含む1万件超の新たなスパムメール、トレンドマイクロが確認

[2015/10/28]

トレンドマイクロは10月27日、メールに添付したMicrosoft Office文書のマクロを利用して、オンライン銀行詐欺ツールをダウンロードさせる手口を新たに3件確認したとセキュリティブログで注意喚起した。

3種のマルウェアスパムは、すべて同一のオンライン銀行詐欺ツールを頒布するもの。Trend Micro Smart Protection Networkの観測によると、10月27日中に合計1万1000通以上の偽装メールを確認しているという。

●SNSで安易な友達リクエストは控えて・・・IPAが注意喚起

http://news.mynavi.jp/news/2015/10/30/151/

このニュースをザックリ言うと・・・

- 10月28日（日本時間）、独立行政法人情報処理推進機構（IPA）より、SNSユーザからの相談が10月に入って急増しているとして警告が出されました。

- 相談の内容は、「友人からの友達リクエストと思しきメールが届いたので承認したら、GMailの連絡先に登録しているアドレス宛に自分名義での招待メールが不正に送信されている」というもので、9月に11件程度だった相談件数が10月には39件に上っているとのことです。

- IPAでは、海外のSNSから求められたサービスの連携を許可することにより、GMailの連絡先へのアクセスが可能となってしまうケースがあること、特にGoogle Apps（GMail等のサービスを組織単位等で利用する）を利用している場合には、連携の許可により、組織内で共有している連絡先情報を悪用され、被害が増大する可能性があるとして注意を呼びかけています。

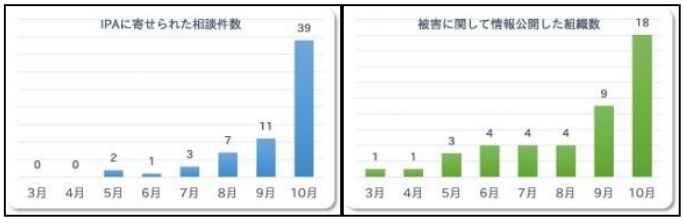
- また、事前の対策として、「不用意にサービス連携を許可しない」「組織の管理者は組織内に対して注意を促す」こと、事後の対策として「意図せず許可したサービス連携は削除する」ことを挙げています。

AUS便りからの所感等

- 例えばTwitterでは、不正なアプリとの連携により、身に覚えのない投稿やDM送信を行ってしまうケースが時々報告されており、比較的似通った例と言えます。

- IPAも説明していますが、サービスとの連携時には、サービス提供者に対してアクセスを許可することになる情報の一覧が表示されるため、必ずこれを確認し、また適宜ネット上の評判も確認しつつ、連携の可否を検討すべきでしょう。

マイナビニュース



IPAに寄せられた相談件数(左)、被害に関して情報公開した組織数(右)