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。

●約3%のユーザがSMBポートをインターネットに開放…ラック社が注意喚起

http://internet.watch.impress.co.jp/docs/news/1066547.html
http://news.mynavi.jp/news/2017/06/22/248/

このニュースをザックリ言うと・・・

- 6月21日（日本時間）、国内大手セキュリティベンダーのラック社より、同社が14日から提供しているネットワーク設定の診断サービス「自診くん」による診断結果からの考察が発表されました。

- 診断結果のうち3,000件に対する分析によれば、約3%において、SMB（Windowsの共有フォルダ等に関連する機能）が使用するTCPポート139番または445番が外部に対して公開されている状況だったとされており、これにより、セキュリティパッチを当てていない場合、ランサムウェア「WannaCry/WannaCrypt」に感染する可能性があったとしています。

- 同社では、USB通信機器やSIM内蔵タブレットPCなど、グローバルIPアドレスを割り当てて通信サービスを提供するモバイルデータ通信環境での診断結果であると考察しており、Wi-Fiルータやスマートフォンのテザリングによる接続を行うか、OSのファイアウォール設定により当該ポートへの通信を遮断するよう推奨しています。

- この他、SSHとTelnetがそれぞれ使用する22番・23番が公開されているケースも見られており、IoTマルウェア「Mirai」の例を挙げて対策を行うよう呼びかけています。

AUS便りからの所感等

- クライアントPCがNAT機能を備えるルータ・UTMを介してインターネットに接続するネットワーク構成が一般的になったことにより、PC自体でのセキュリティ対策としてアンチウイルスの導入率は高い一方、「Windowsファイアウォール等の設定については十分に行っていない」というケースは潜在的に少なくないのではと推測され、この場合、一旦内部LANに侵入したマルウェアが同一LAN上の各PCに攻撃を仕掛けてくると十分な防御をとれない可能性があります。

- UTMによる防御のみならず、PC自体でとるべきセキュリティ対策の啓発についても、今後は重要なポイントとなってくることでしょう。

INTERNET Watch

約3%のユーザーがSMBポートをインターネットに開放、ラックが注意喚起

自己診断サービス「自診くん」の結果分析

岩崎 宰守　2017年6月21日 17:27

株式会社ラックは、14日から提供しているネットワークセキュリティ設定の自己診断サービス「自診くん」公開から1週間の結果を公表した。診断を行ったユーザーの約3%がTCPポート139/445番をインターネットに開放していたという。

公表されたのは、診断結果から3000件をランダムに抽出した結果の分析。TCPポート139番はNETBIOS、同445番はWindows用のファイル共有プロトコルであるSMBが利用するもの。ランサムウェア「WannaCry」は、このSMB v1の脆弱性を悪用して感染を広げるものだった。

これらのポートは社内などのローカルネットワーク向けには開放されているのが一般的だが、インターネットに開放される設定は推奨されているとは言えない。

ラックでは、TCPポート445番の開放が確認できた場合、WannaCryなどの侵入余地があることになり、Microsoftが3月に提供開始したセキュリティ更新プログラム「MS17-010」が適用されていなければ、WannaCryに感染する恐れがあるとしている。

マイナビニュース

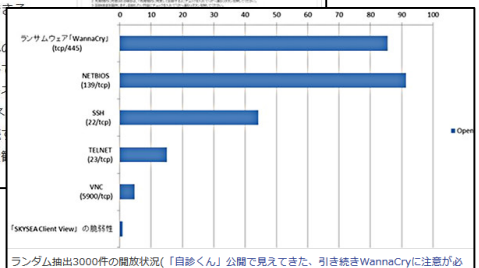
WannaCryで悪用される445ポート、約3%が開放状態 - ラック診断サービス「自診くん」

長岡弥太郎
[2017/06/22]

ラックは、14日に公開した無料のセキュリティ診断サービス「自診くん」のサービス結果からの考察を公表。WannaCryで悪用されるtcp/445を含む開放状況に警鐘を鳴らしている。

14日に公開した「自診くん」は、WannaCryで悪用されるWindows SMBにおける脆弱性(MS17-010)、「SKYSEA Client View」の脆弱性(CVE-2016-7836)を含む、SSH 22/tcp、TELNET 23/tcp、NETBIOS 139/tcp、RDP 3389/tcp、VNC 5900/tcpの通信を診断、塞いでおくべきポートの開放状況を確認でき

おもに情報システム部門や診断結果への行える利用者を想定。社外に持ち出しルデータ通信機器を使用してインター続するノートPCやタブレット、社内ネクではなく直接インターネットに接続どが特にリスクが高いと同社は診断を



ランダム抽出3000件の開放状況(「自診くん」公開で見えてきた、引き続きWannaCryに注意が必要な理由より)

●ホスティング業者がランサムウェアに感染、身代金を支払い復旧

https://japan.zdnet.com/article/35102873/

このニュースをザックリ言うと・・・

- 6月14日（現地時間）、韓国のウェブホスティング業者であるNAYANA社より、同社のシステムがランサムウェア「Erebus」に感染し、同社顧客のWebサイト等が利用不可能な状態に陥っていたことが発表されました。

- 発表によれば、10日に同社が管理する153台のLinuxサーバがErebusに感染した結果、これらのサーバにホスティングされていたWebサイトのデータ等が暗号化され、攻撃者からは暗号化解除のために50億ウォン（約4億9000万円）相当をBitCoinで支払うよう要求されたとのことです。

- 同社は自力での復旧を断念し、攻撃者への交渉の末、12億ウォン（約1億7800万円）相当を支払うことにより、復旧に着手できたようです。

AUS便りからの所感等

- Erebusは2016年9月に初めて確認されていましたが、トレンドマイクロ社の分析によれば、今回の件でLinuxサーバに対応した亜種が用いられたとされています。

- NAYANA社が自力での復旧を断念したのは、二重にとっていたはずのバックアップデータまで暗号化されてしまったことが大きいとみています。

- バックアップをとることはもちろん、そのバックアップデータはランサムウェアが到達できない場所に退避すること、例えば外付けハードディスクをデータ退避のときだけ接続するようにする等が重要です。

●「PowerPoint」のハイパーリンクを使うマルウェア登場、マウスオーバーのみで感染

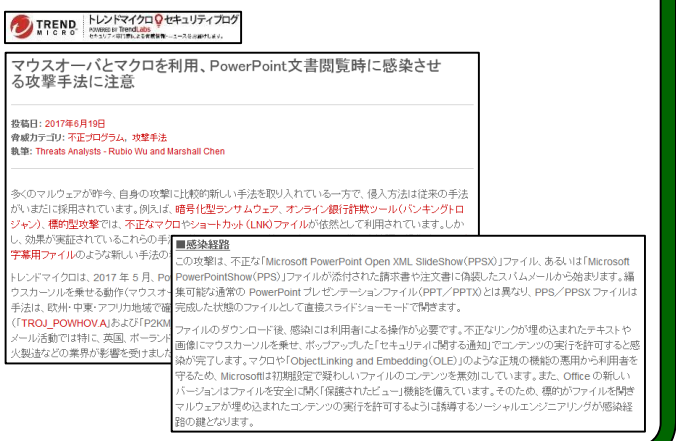
http://blog.trendmicro.co.jp/archives/15257

このニュースをザックリ言うと・・・

- 6月2日（現地時間）、米国のセキュリティ情報サイトBleeping Computerより、新たな攻撃手法によるマルウェアの拡散を確認したと発表されました。

- 細工したPowerPointスライドファイル（.ppsx または .pps拡張子）を添付したスパムメールを用いる手法をとっており、ファイルを開いてスライドショーモードに入り、文書内のハイパーリンクの上にマウスを移動するだけで、インターネットバンキングを標的とするマルウェア「OTLARD(Gootkit)」をダウンロードしようとします。

- トレンドマイクロ社等からも情報が出ており、今回の拡散について「将来のスパムメール活動のための予行演習」として警告されています。



AUS便りからの所感等

- マルウェアのダウンロードは、Office2010以降に採用されている「保護されたビュー」が有効になっていれば食い止められるようで、必ずデフォルトで有効にし、かつ攻撃者がこれを解除するよう誘導する手口にも十分注意を払うことがマルウェアに感染しないようにするための最も重要な点の一つです。

- その上で、こうした不正なファイルを開いたり、あるいはそれが添付されたメールが受信されることを食い止められるよう、アンチウイルスとUTMによるさらなる防御を固めることも肝要です。