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。

●マルウェア「Emotet」国内で26,000件の感染か…警察庁・総務省がISP通じ注意喚起実施へ

https://www.asahi.com/articles/ASP2M3CCNP2LUTIL05S.html
https://www.npa.go.jp/cyber/policy/mw-attention.html
https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00095.html
https://notice.go.jp/Emotet

このニュースをザックリ言うと･･･

- 2月19日(日本時間)、警察庁および総務省より、マルウェア「Emotet」に感染しているPCが依然国内に多数あるとして、2月下旬より注意喚起を行うと発表されました。

- 海外の捜査当局から警察庁に対し、国内のEmotetに感染している機器に関する情報提供があったとのことで、一部報道によればその数は26,000IPアドレスに上るとのことです。

- 総務省では、安全でないIoT機器の調査と注意喚起を行う「NOTICE」プロジェクトにより、今回もISPを仲介して感染の疑いのある機器の所有者に連絡を行い、感染確認や駆除の方法を案内するとしています。

AUS便りからの所感等

- 1月までに、欧米の警察当局が連携してEmotetに関与する人物の摘発や指令サーバーの押収を行い、世界中のEmotetを無力化させることに成功したと報じられていました(AUS便り 2021/02/01号参照)。

- 3月25日に予定されている自己削除の実行まで引き続き局所的に活動を続けるEmotetが存在するとみられること、Emotetが感染したPCに他のマルウェアもダウンロードされている恐れがあること等を鑑み、恐らくは過去に感染が確認されたアドレスも含め注意喚起を行い、徹底した駆除に乗り出しているものと考えられます。

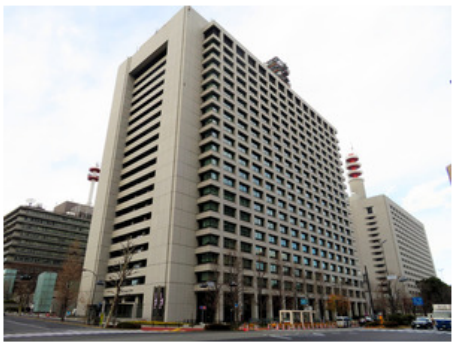
- 「感染したPCに保存されている送受信メールのアドレス・文面を悪用する」という、ビジネスでのメールのやり取り等における油断を巧妙に突くEmotetの拡散の手口は、後発のマルウェアにも用いられており、仮にEmotetが無力化によって消滅したとしても決して安心することなく、アンチウイルスやUTM等による各種マルウェアに対する防御および不審なファイルが添付されたメールへの慎重な対応を行い、万が一の感染時には、駆除の後にメールアカウントのパスワード変更により安全を確保すること等に留意してください。

朝日新聞 DIGITAL

国内PC2万6千件、「エモテット」感染か　注意喚起へ

田内康介　2021年2月19日 10時19分

シェア　ツイート　ブックマーク　メール　印刷
list　0



警察庁が入る中央合同庁舎第2号館=東京都千代田区

「Emotet(エモテット)」と呼ばれるコンピューターウイルスに感染しているパソコンが国内に多数あるとして、警察庁などは19日、感染した恐れのあるパソコンの利用者に注意喚起すると発表した。海外の捜査当局から、インターネット上の住所にあたるIPアドレスで約2万6千件の感染が確認されたとする情報が寄せられたという。

警察庁は総務省などを通じ、プロバイダー側に感染に関する情報を提供。これを元にプロバイダー各社が22日以降、パソコンの利用者の特定を進め、メールなどで注意喚起する予定という。

● NICTが「NICTER観測レポート2020」公開…攻撃関連通信量は2年連続で前年比約1.5倍に

https://www.is702.jp/news/3819/
https://www.nict.go.jp/press/2021/02/16-1.html

このニュースをザックリ言うと・・・

- 2月16日(日本時間)、情報通信研究機構(NICT)サイバーセキュリティ研究所より、サーバー攻撃関連通信の観測分析を行う「NICTER」プロジェクトの2020年における分析結果「NICTER観測レポート2020」が公開されました。

- 2020年に観測されたサイバー攻撃関連通信は合計5,001億パケットで、2019年(AUS便り 2020/2/17号参照)の3,279億個から約1.5倍に増加、うち53%近くの1,750億個が海外組織からの調査目的のものとされています。

- また1IPアドレスあたりの観測パケットは約182万個とこちらも前年(約120万個)の約1.5倍に増加しています。

- 宛先ポート別のパケットの割合は、Telnetサービスで用いられるTCPポート23番宛がやはり最も多いものの16.3%と前年(24.2%)より減少、上位10位についても37.1%と前年(49.8%)と減少しており、IoT機器を狙う傾向は前年と同様ながらも、多くのポート番号をターゲットとするボットネットの活動により攻撃が多様化しているためと推測されています。

AUS便りからの所感

- Telnetポートに次いでパケットの割合が多かったポートとしては、いずれもTCPで445(Windowsサーバー・SMB)、80(HTTP)、22(SSH)、1433(MSSQL)、8080(HTTP)、81(HTTP)、5555(Androidによるセットトップボックス等が使用)、8845(仮想通貨イーサリアムが使用)、3389(リモートデスクトップ)となっています。

- 特に日本においては、NATやファイアウォールを用いたネットワーク構成により、内部ネットワーク上の機器へは直接アクセスできない状況が通常でしたが、UPnPが意図せず機能した、IPv6について適切にフィルタリング設定が行われなかった等により、外部から直接アクセス可能な状態となるケースもあるとみられます。

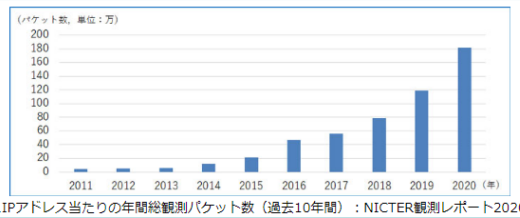
- 社内に設置されているネットワーク機器やIoT機器全てを確実に管理下に置き、意図してインターネットに直接接続しているかどうか、外部から意図していないポートにアクセスされないかの確認と対策をとることが重要です。

TREND MICRO | is702 インターネット セキュリティ ナレッジ

「NICTER観測レポート2020」公開、サイバー攻撃関連通信が前年の1.5倍に | NICT

2021/02/19 ツイート いいね！0 B!ブックマーク 0 EMail

国立研究開発法人情報通信研究機構（NICT）サイバーセキュリティ研究所は2月16日、「NICTER観測レポート2020」を公開しました。NICTERプロジェクトにおける2020年のサイバー攻撃関連通信の観測・分析結果をまとめた内容です。



図：1IPアドレス当たりの年間総観測パケット数（過去10年間）：NICTER観測レポート2020より

● OpenSSLとBINDに相次いで脆弱性報告

https://news.mynavi.jp/article/20210219-1741329/
https://news.mynavi.jp/article/20210219-1738789/

このニュースをザックリ言うと・・・

- 2月17日と18日(日本時間)、幅広く利用されている著名なオープンソースソフトウェアに相次いで脆弱性の存在が発表されています。

- 2月17日、暗号化通信ライブラリ「OpenSSL」において、これを利用しているサーバーのダウンが可能な脆弱性等が発表され、修正バージョン1.1.1等がリリースされています。

- 2月18日、DNSサーバー「BIND」においても、特定のケースでやはりサーバーをダウンさせられる脆弱性が発表され、こちらも修正バージョン9.16.12・9.11.28がリリースされています。

- JPCERT/CC等各種機関からもこれらの発表を受け、速やかに各ソフトウェアのアップデートを行うよう注意喚起が出されています。

AUS便りからの所感

- いずれも、前述の通り幅広く利用されていることと、長年の間頻繁に脆弱性が発見されることで共通していますが、特にOpenSSLはLinuxで構築されるほぼ全てのサーバーで必須となり、脆弱性の内容によっては広範囲に影響を受けることが予想されます。

- 一方のBINDについては、既に様々な代替ソフトウェアが利用されるケースも多くなっていますが、大規模な組織内での利用の他、メーカー製アプライアンスにおいて依然採用されているケースも考えられ、ベンダーから情報が出ていないか随時確認するべきでしょう(また代替ソフトウェアにおいても脆弱性が報告される可能性は皆無ではないことには注意が必要です)。

- いずれにせよ、Linuxディストリビューション等からのセキュリティアップデートがリリースされ次第、直ちに適用できるような体制が整っているか、確認することが肝要です。

TECH+ Powered by マイナビニュース

ISC BINDに深刻な脆弱性、アップデートを

2021/02/19 12:34 著者：後藤大地

B! URLをコピー

JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）は2月18日、「JVNVU#90613078: ISC BIND にバッファオーバーフローの脆弱性」において、ISC BINDに脆弱性が存在すると伝えた。この脆弱性を悪用されると、サービス妨害攻撃(DoS: Denial of Service attack)を引き起こされる危険性があるほか、まだ実証はされていないものの遠隔からコードが実行されるおそれがあるとされている。

OpenSSLに複数の脆弱性、DoSを受けるおそれ

2021/02/19 06:12 著者：後藤大地

B! URLをコピー

JPCERTコーディネーションセンター（Japan Computer Emergency Response Team Coordination Center：JPCERT/CC）は2月17日、「JVNVU#94508446: OpenSSL に複数の脆弱性」において、OpenSSLに複数の脆弱性が存在すると伝えた。これら脆弱性を悪用されると、攻撃者によってサービス妨害攻撃(DoS: Denial of Service attack)、SSLv2接続の強制、アプリケーション不正動作やクラッシュなどを引き起こされる可能性があるとされており注意が必要。