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」の無力化に成功か、オランダ警察当局発表

https://japan.cnet.com/article/35165702/
https://gigazine.net/news/20210129-europol-exterminate-malware-emotet/

このニュースをザックリ言うと・・・

- 1月27日(現地時間)、欧州警察刑事機構(Europol)より、マルウェア「Emotet」を無力化する計画が成功したと発表されました。

- 発表によれば、欧米8か国の警察等が連携してのプロジェクト「LadyBird」において、Emotetを拡散させたサーバーの押収、関与した人物の逮捕等を経て、主要な指令サーバー3台のうち2台がオランダに設置されていたことを突き止めたとしています。

- また、その2台の指令サーバーから、Emotetに感染した全てのPCに対し、動作を無害化するようなアップデートを配信することに成功し、これにより、世界中のEmotetが3月25日正午に自身を削除する予定とのことです。

AUS便りからの所感等

- Emotetは2019年以降断続的に活発な活動を続けていたマルウェアで、最近では昨年12月21日に活動の再開が報告されたばかりでした(AUS便り 2020/12/28号参照)。

- Emotetの特徴として「感染したPCに保存されている送受信メールのアドレス・文面を悪用して、マルウェア添付メールを送信する」ことが知られていますが、同様の挙動をとる別のマルウェア「IcedID」が依然として存在していることには注意が必要です。

- IPAがEmotetについて随時更新している情報(https://www.ipa.go.jp/security/announce/20191202.html)等を参考に、アンチウイルス・UTMによる防御を確実に行う、日頃メールのやり取りをしている取引先等からのメールに対しても簡単に添付ファイルを開かない、特にWordファイル等を開いた際に「セキュリティの警告」が出るようなケースでは用心する、場合によっては相手との安全な情報共有について取り決めを交わす等、慎重に行動するよう努めましょう。

c|net Japan

マルウェア「Emotet」、感染ホストから一斉削除へ--蘭警察がアップデート配信

Catalin Cimpanu （Special to ZDNet.com） 翻訳校正： 佐藤卓 長谷睦 （ガリレオ） 2021年01月28日 12時07分

オランダの警察当局がマルウェアの「Emotet」を削除するアップデートの配信計画を進めていることを、米ZDNetが現地時間1月27日に確認した。このアップデートは、Emotetに感染しているすべてのコンピューターからこのマルウェアを削除する動作を、3月25日に開始するという。

このアップデートの配信が可能になった背景には、8カ国の警察がこのほど一斉摘発を実施し、現時点で最大のマルウェアボットネットと考えられているEmotetを拡散したサーバーの押収やこのボットネットに関与した人物の逮捕を進めたという事情がある。

サーバーは複数の国に設置されていたが、オランダ当局によれば、Emotetの主要なC&C（コマンドアンドコントロール）サーバー3台のうち2台がオランダ国内に設置されていたという。

●sudoに一般ユーザーの権限昇格の脆弱性、アップデートを

https://www.jpcert.or.jp/at/2021/at210005.html

このニュースをザックリ言うと・・・

- 1月27日(日本時間)、JPCERT/CCより、Linux等で利用されるsudo(一般ユーザーから管理者権限でコマンドを実行するためのツール)に脆弱性が発見されたとして注意喚起が出されています。

- 脆弱性の悪用により、Linuxサーバー上のローカルユーザーが不正に管理者権限を奪取し、サーバーを乗っ取る可能性があるとされています。

- sudoのソースコードおよびLinuxディストリビューション(CentOS・RHEL・Debian・Ubuntu等)において既に脆弱性を修正したバージョンがリリースされており、速やかにアップデートを行うよう呼び掛けられています。

AUS便りからの所感

- sudoでは利用可能なコマンドやユーザーを制限する設定が可能ですが、脆弱性を悪用されると、それらの制限が無視され、本来sudoを使用できないユーザーに管理者権限を取得される恐れがあります。

- 通常、Webサーバー・メールサーバー等に対し直接攻撃を行うことは困難とみられ、何らかの方法でサーバー上への侵入に成功した攻撃者が攻撃コードをダウンロード・実行するケース、あるいはサーバー上にSSH等でログイン可能な一般ユーザーが悪意を持って攻撃を行うケースが考えられます。

- 大抵のLinuxディストリビューションでは、全てのソフトウェアパッケージを一括してアップデートする仕組みが提供されていますので、OSを常に最新に保つために随時これを実行するルーチンを確立すること、またパッケージからではなくソースからコンパイルしたソフトウェアについても、同様に新しいバージョンを確実にインストールする管理体制を整えることが肝要です。

- Linuxを使用するNAS等のアプライアンスでもアップデートがリリースされる可能性があり、これらについてもベンダー情報の確認は必須でしょう。

JPCERT CC sudoの脆弱性（CVE-2021-3156）に関する注意喚起

2021年1月26日（現地時間）、sudoにおけるヒープベースのバッファオーバーフローの脆弱性（CVE-2021-3156）に関する情報が公開されました。
sudoersファイル(通常は/etc/sudoers配下)が存在する場合に、脆弱性を悪用することにより、ローカルユーザがrootに権限昇格する可能性があります。

● IPA、「情報セキュリティ10大脅威 2021」公開…テレワークの脅威初登場

https://news.mynavi.jp/article/20210127-1674945/
https://www.ipa.go.jp/security/vuln/10threats2021.html

このニュースをザックリ言うと・・・

- 1月27日(日本時間)、IPAより、「情報セキュリティ10大脅威 2021」の概要が発表されました。

- 2020年に発生した、社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者等約160名によって、個人と組織それぞれのカテゴリーでの10大脅威を決定しています。

- 個人側の10大脅威は昨年度と順位は変動しつつも同じ顔ぶれである一方、組織側では「テレワーク等のニューノーマルな働き方を狙った攻撃」が3位に初登場しています。

AUS便りからの所感

- 昨年12月にマカフィー社が発表した「10大セキュリティ事件ランキング」(AUS便り 2020/12/28号参照)のように、年末年始等には、大手セキュリティベンダーや関連団体等から、各組織の立ち位置・観点等の違いを少なからず反映した年間のセキュリティ関連ニュースのまとめ、あるいは翌年度における業界の動向予測等がリリースされています。

- IPAの「情報セキュリティ10大脅威 2021」については、2月下旬に詳しい解説が発表される予定となっていますので、その折には再度挙げられている各項目に目を通し、自分自身や自組織に関連するもの以外であっても各種脅威について知識を得る、あるいは以前に得た知識が正しいかの再確認をし、今後の行動に役立てるのが良いでしょう。

■「情報セキュリティ10大脅威 2021」　NEW：初めてランクインした脅威

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位