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。

●警察庁を騙り、銀行の偽サイトへ誘導するフィッシングに注意喚起

https://www.jc3.or.jp/topics/banking/NPAphishing.html
http://www.npa.go.jp/bureau/info/chuikanki.pdf

このニュースをザックリ言うと・・・

- 6月26日(日本時間)、警察庁および日本サイバー犯罪対策センター(JC3)より、警察庁を騙るショートメール(SMS)によるフィッシング(スミッシング)が確認されたとして注意喚起が出されています。

- JC3ではSMSの一例として、本文に「【警察庁】銀行をご利用のお客様に対し不正防止措置の認証確認を行っております」と記載、リンクのクリックにより、認証を促すポップアップ→警察庁のサイトを模倣した偽サイト→銀行のフィッシングサイトと誘導されるとのことです。

- 警察庁においても、「金融機関の口座情報等を入力させる画面に誘導することはありません」とし、同庁のドメインである「npa.go.jp」を使用していない偽サイトにはアクセスせず、またそういった画面が表示されても口座情報等を入力しないよう呼び掛けています。

AUS便りからの所感等

- 当該フィッシングを取り上げたトレンドマイクロ社の記事(https://www.is702.jp/news/3703/)では、複数の大手銀行のフィッシングサイトが表示される様子、あるいは警察庁を騙る上記とは別の本文とともに銀行のフィッシングサイトが表示される一例が挙げられています。

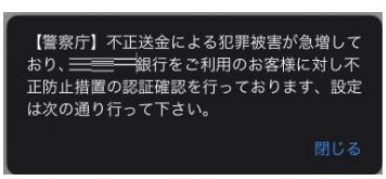
- セキュリティベンダーや、JC3あるいはフィッシング対策協議会(https://www.antiphishing.jp/)のようなマルウェア・フィッシングについて啓発を行っている団体等から発表されている、詐欺の手口に関する情報を随時収集し、フィッシングを回避するためのリテラシーを地道に高めていくことが最も重要であり、それを補助する意味でも、アンチウイルス・UTMやWebブラウザーのアンチフィッシング機能を併せて有効にすることを推奨致します。

2020年 6月 27日　作成

警察庁を騙るフィッシング

6月26日、インターネット上において、警察庁を騙るＳＭＳが確認されました。
同ＳＭＳは、銀行への認証の設定を促す内容となっており、リンクをクリックすると、認証を促すポップアップが表示されます。ポップアップを閉じると、警察庁の偽のウェブサイトが表示された後、自動的に銀行のフィッシングサイトへ誘導されます。
不審なＳＭＳのリンクは、クリックしないようにしてください。
また、以下の注意喚起もご参照ください。
「インターネットバンキングの不正送金の被害に注意」（詳細はこちら）

警察庁を騙ったＳＭＳ
（インターネット上に掲載されていたものを加工したもの）



リンクにアクセスした際に表示されるポップアップ

●モバイルバンキングを狙うトロイの木馬、2020年第1四半期に急増…カスペルスキー発表

https://www.kaspersky.co.jp/about/press-releases/2020_vir10062020

このニュースをザックリ言うと・・・

- 6月10日(日本時間)、セキュリティベンダーのカスペルスキー社より、「2020年第1四半期（1～3月）のサイバー脅威に関する調査結果(5月発表)」に基づくプレスリリースが公開されました。
- この期間に同社モバイル向け製品で検知されたモバイルバンキングを狙うトロイの木馬(以下、トロイ)は42,115件で、2019年第2・3・4四半期にそれぞれ13,899・13,129・15,410件だったものから急増しています。
- 国別のユーザーの中でトロイの攻撃に遭ったユーザーの割合が最も高かった国は日本の0.57%で、こちらも2019年第1四半期から顕著な増加傾向にあるとのことです。
- 日本のユーザーが攻撃を受ける割合が高まった理由として、Android向けのトロイ「Wroba」による「Roaming Mantis」と呼ばれる攻撃が、2019年第4四半期から日本向けの攻撃に注力していることを挙げています。

AUS便りからの所感

- Roaming Mantisにより、例えばDNS情報が改ざんされ、悪意のある偽サイトに誘導される恐れがあるとされています。
- 同社では、アプリは(Google Playのような)公式のストア等信頼できるソースからインストールすること、Androidデバイスをroot化しないこと、同社(あるいはベンダー各社)が提供するセキュリティソフト等を使用することを推奨しています。
- Google Playであっても有害なアプリが登録されるケースが時々発生しており、インストールするアプリは最小限に留めること、事前にアプリストアでのレビューやSNS等での評判を参考として可能な限り実績のあるアプリを採用することも、マルウェアへの感染を避けるためには有用となるでしょう。

kaspersky

2020年6月10日

<Kaspersky サイバー脅威レポート：2020年第1四半期> モバイルバンキングを狙うトロイの木馬が過去18カ月で最多、最も検知の割合が高かったのは日本

この期間には、モバイルバンキングを狙うトロイの木馬が急増し、2019年第4四半期（10～12月）の1万5410件の2.5倍超となる4万2115件のインストールパッケージを検知しました。最も検知の割合が高かったのは日本（0.57%）で、2019年第1四半期は77位（0.01%）でしたが、第4四半期には4位（0.13%）となり、顕著な増加傾向がみられます。

[本リリースは、2020年5月20日にKasperskyが発表したプレスリリースに基づき作成したものです]

Kasperskyの調査チームは、2020年第1四半期（1～3月）のサイバー脅威に関する調査結果を公表

●Apache TomcatにDoSの脆弱性、アップデートを

https://news.mynavi.jp/article/20200630-1075271/
https://jvndb.jvn.jp/ja/contents/2020/JVNDB-2020-006033.html

このニュースをザックリ言うと・・・

- 6月26日(日本時間)、US-CERTやJVNより、Apache Tomcatに脆弱性(CVE-2020-11996)が存在するとして注意喚起が出されています。
- 脆弱性の悪用により、サーバーのCPUリソースが浪費して動作が遅くなる、ないし動作しなくなるよう仕向けるDoS攻撃が可能になるとされています。
- Tomcatの開発元より修正バージョン(9.0.36・8.5.56)がリリースされており、アップデートが推奨されています。

AUS便りからの所感

- Tomcatは、サーバーサイドでJavaによるWebアプリケーション(Servlet・JSP)を実行するために良く用いられるソフトウェアです。
- 通常のWebサーバー・アプリケーションの構成では、Tomcatへの直接アクセスを制限するよう設定されることが多いですが、アクセス制限に設定していない場合にリモートから、あるいは開発環境等の場合に同一LAN上から攻撃を受けるといった恐れが考えられます。
- ともあれ、脆弱性の根本的な対策として、OS自体からあらゆるアプリケーションに至るまで、ソフトウェアを常時最新のバージョンに保つことと、サーバー自体やUTMによるパケットフィルタリング(あるいはWebアプリケーションファイアウォール(WAF))の設定とをそれぞれ確実に行うことが重要です。

マイナビニュース

印刷

Apache TomcatにDoSの脆弱性、アップデートを

後藤大地　2020/06/30 06:23

関連キーワード：脆弱性

United States Computer Emergency Readiness Team (US-CERT)は6月26日(米国時間)、「Apache Releases Security Advisory for Apache Tomcat | CISA」において、Apache Tomcatに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)を引き起こされる危険性がある。