令和４年７月１日

サイバーセキュリティ関連情報（７月号）

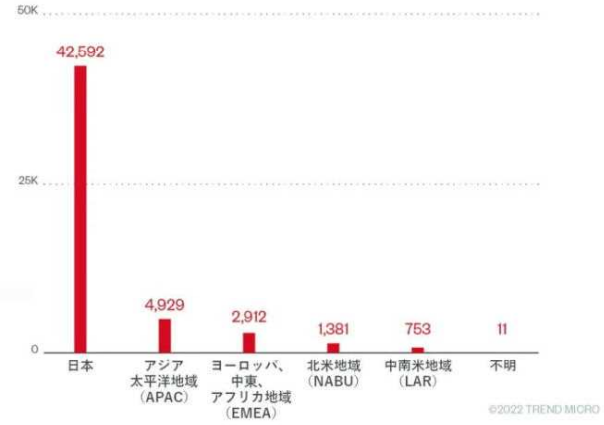
鳥取県警察本部サイバー犯罪対策課

○　「Emotet」の新機能実装を確認！！

国内外で感染被害が拡大している「Emotet」に関して、ウェブブラウザ「Google Chrome」に保存されたクレジットカード番号や名義人氏名、カード有効期限等を盗み、外部に送信する機能が追加されたことが確認されました。

「Emotet」は、主にメールを感染経路としたマルウェア（不正プログラム）であり、メールソフトに登録されている連絡先から知り合いのメールアドレスを盗んで使うなどして、本人作成のメールであると信じ込ませ、不審に思わず開封してしまいそうなメールを装い送信されてきます。

本年４月下旬以降は、ショートカットファイルを添付し、これをダブルクリックなどで開いた場合に「Emotet」に感染させる手口が確認されるなど、手口が巧妙化してきています。



【2022年第１四半期におけるEmotet検出台数（地域別）】

また、トレンドマイクロによると、２０２２年第１四半期における「Emotet」は、新亜種を複数用いた感染活動が数多く発見されており、地域別に見た感染被害では、「アジア太平洋地域（APAC）」、「ヨーロッパ、中東、およびアフリカ（EMEA）」などの地域を大きく上回り、日本国内での検出が最多となっています。

引き続き、

・不用意にメールの添付ファイルを開かない。

・ウイルス対策ソフトやOSを最新の状態にアップデートする。

などの対策をお願いします。

引用：【警察庁】https://www.npa.go.jp/cyberpolice/important/2020/202012111.html
【トレンドマイクロ株式会社】https://blog.trendmicro.co.jp/archives/31438

○ 公的機関や企業等の偽サイトに注意！！

内閣サイバーセキュリティセンター（NISC）は、政府機関や地方公共団体などの公的機関、企業・団体等の本物のWebサイトと同じ内容を表示する偽サイトの存在が確認されているとして、注意を呼び掛けています。

これらの偽サイトの中には、クリック先が悪質なサイトへのリンクに置き換えられているものもあり、サイバー犯罪に用いられる可能性があります。

被害に遭わないためにも、

・URLリンクから他のWebサイトに移る際は、リンクにポインタを置く、アドレス欄をよく見る等により、URLのドメイン名を必ず確認する。

・ドメイン名が正規の公的機関等と無関係なものである場合には、別の検索エンジンを利用するなどの方法で、本物のWebサイトのURLを確認する。

などし、少しでも不審な点を感じた場合には、安易にアクセスしたり、当該Webサイト上でクリック等の動作をしないようお願いします。

引用：【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/pdf/press/20220615NISC_press.pdf