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。

●Officeマクロ悪用攻撃、MSの対策で減少効果…一方で回避する手口も増加

https://japan.zdnet.com/article/35191182/
https://www.proofpoint.com/jp/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world

このニュースをザックリ言うと･･･

- 7月28日(日本時間)、メールセキュリティ企業の日本プルーフポイント社より、Officeファイル(Word・Excel等)による攻撃に対するマイクロソフト(以下・MS)の対策とそれに伴う攻撃傾向の変化についての解説が同社ブログで行われています。

- MSではインターネットからダウンロードしたOfficeファイル上でのマクロ実行をデフォルトでブロックする措置を4月から実行しています(7月に一時無効化され、同月には再開するという事態にもなっています)。

- プルーフポイント社の調査では、攻撃者によるマクロ添付ファイルの使用が2021年10月から2022年6月の間に約66%減少しているとのことです。

- 一方で、Officeファイルを直接添付するものではなく、.lnk(ショートカット)や .dll(ライブラリ)ファイルを含む.zipファイル、さらにそれを格納した .iso(DVD-RやBD-R等のイメージ)ファイルを添付することにより、ブロック措置を回避する攻撃も確認されているとしています。

AUS便りからの所感等

- 「インターネットからダウンロードした」ことを示すフラグがOfficeファイルに付加されている場合にマクロの実行をブロックするという挙動となっており、今までもメールの文章でファイルに付加されたフラグを解除させることにより、マクロを実行させるよう誘導する手口は多くとられていましたが、前述の.zipや.isoファイルを用いるものは、それらから展開したファイルにはフラグが付加されない場合があることを悪用したものとみられています。

- .lnkファイルを用いる手口は、OfficeマクロではなくPowerShellスクリプト等を実行させるもので、例えばEmotetでこの手口がとられています。

- くれぐれも「不審なWord・Excelファイルを開いたり、マクロを有効化したりしない限り、マルウェアに感染することはない」といった先入観に囚われず、セキュリティベンダーや団体が提供する情報の収集を随時行い、刻々と変化する攻撃手法について理解しつつ行動することが肝要です。

ZDNet Japan

マイクロソフトのマクロ悪用対策で攻撃減少、しかし代替手法が増加

ZDNet Japan Staff　2022-07-29 14:48

サイバー攻撃者が標的のコンピューターにマルウェアを送り込むべく、なりすましメールなどに不正マクロを組み込んだOfficeファイルを添付して送り付け、受信者にマクロを実行させる手法がある。このためMicrosoftは2月、ユーザーがインターネットから入手するOfficeファイルのVBAマクロをデフォルトでブロックする措置を講じた（7月11日にいったん解除されたが、26日から再びブロックしている）。

メールセキュリティ企業の日本プルーフポイントは、Microsoftが講じた対策が攻撃手法に変化をもたらしたとする調査分析の結果をブログで明らかにした。

それによると、攻撃者がメールに不正なVBAやExcel 4.0マクロを添付して送り付ける手法は、2021年10月～2022年6月に約66%減少した。一方で、ISO、RAR、ZIP、IMGなどのコンテナーファイル形式やショートカットのLNKファイルを使う手法が約175%増加した。LNKファイルを悪用する攻撃は、2月以降に少なくとも10の攻撃者グループが多用しており、2021年10月以降で1675%増加しているという。

●7月はWordPressプラグイン13種に脆弱性…Sucuri発表

https://news.mynavi.jp/techplus/article/20220801-2412700/
https://blog.sucuri.net/2022/07/wordpress-vulnerabilities-patch-roundup-july-2022.html

このニュースをザックリ言うと･･･

- 7月29日(現地時間)、WordPress用セキュリティプラグイン等を提供する米Sucuri社より、同月にWordPressプラグインで確認された脆弱性についてのまとめが発表されています。
- 脆弱性が報告されたプラグインは13種にのぼり、特に「Youzify」のSQLインジェクション脆弱性と「User Private Files」の不正なファイルアップデートの脆弱性について最も緊急度が高いとされています。
- 殆どのプラグインは脆弱性が修正された最新バージョン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

- Sucuri社ではWordPressプラグインに報告された脆弱性の内容と回避策をまとめた記事を毎月発表しており、他にも国内外のベンダーで同様のまとめを発表している所もあります。
- WordPress本体についても、ここ数ヶ月は落ち着いているものの、脆弱性が発見され、アップデートがリリースされるケースがよくみられます。
- 本体およびインストールされているプラグイン全てについて、最新バージョンがリリースされているものを可能な限り速やかに適用する体制を整えるとともに、Sucuri社や他のベンダーが提供するセキュリティ機能を提供するプラグインについても導入、さらにはサーバー自身への導入またはその前面に設置したUTM等によるWAF機能も有効にすることにより、WordPressやその他Webアプリケーション・サーバーに対する攻撃を効果的に防御することを強く推奨致します。

●Linuxにおける新規マルウェアのサンプル数、650%近く急増…Atlas VPN発表

https://news.mynavi.jp/techplus/article/20220730-2411054/
https://atlasvpn.com/blog/linux-malware-on-a-rise-reaching-all-time-high-in-h1-2022

このニュースをザックリ言うと･･･

- 7月27日(米国時間)、フリーVPNサービス「Atlas VPN」を提供するPeakstar Technologies社より、同社が発見したOS毎の新規マルウェアのサンプル数が発表されました。
- Windowsをターゲットとした新規マルウェアは2022年上半期で41,402,204種と他のOSに比べ圧倒的に多いものの、2021年上半期の63,766,520種から35%の減少となっています。
- 一方で、Linuxをターゲットとした新規マルウェアは2022年上半期で1,687,746種となっており、2021年上半期の226,324種から650%近くの増加となっています。
- また2021年全体で1,289,068種だったのに比べても、その半分の期間で既に30%上回っているとされています。

AUS便りからの所感

- Linuxをターゲットとした新規マルウェアは2021年第3四半期の190,579種から第4四半期の872,615種と急激な増加を見せ、2022年第1四半期に854,688種、第2四半期に833,058種となっています。
- Windowsをターゲットとするものと異なり、メールの添付ファイルからクライアントPCへ感染を狙うケースより、Webアプリケーション等からLinuxサーバーへ感染を狙うケースが多いものとみられます。
- Linux等Windows以外のOSについても有償・無償のアンチウイルス製品が提供されており、またUTM等も含め多くのセキュリティプロダクトはあらゆるOSをターゲットとするマルウェアからの防御を行いますので、これらを可能な限り導入し、Windows以外のOSについてもマルウェアの感染からの防御を図ることが重要です。