2022 年 3 月 16 日

Venture Solution

コラム記事

サイバー攻撃用のツールは、いわゆる闇サイトで高額で取引されています。
サイバー犯罪者などが集う掲示板で売買がされているため、会員となり指定金額を支払えば誰でも攻撃ツールを手に入れることが出来る状態となっております。また、サブスクリプション型のツールも販売されており、運用も簡略化しています。
このようなサイバー攻撃に対応するためにはパッチの適用を怠らないことが大切ですが、PC が重くなるなどの理由により自動更新を無効化されているユーザーも多いかと思います。
誰しもがサイバー攻撃を受ける可能性があるため、ソフトウエアは必ず最新の状態にしておく必要があると感じています。
そこで、サイバー攻撃用ツールの現状についての記事が掲載されておりましたので、ご紹介いたします。

サイバー攻撃ツール 5000 万円超も　売買闇サイトの実態

（日経電子版 2022/3/16(水) 05:00 配信 より引用）

情報セキュリティーの脆弱性を狙う攻撃ツールは売買されており、IT（情報技術）の知識がなくても攻撃を仕掛けることができる（日経電子版より引用）

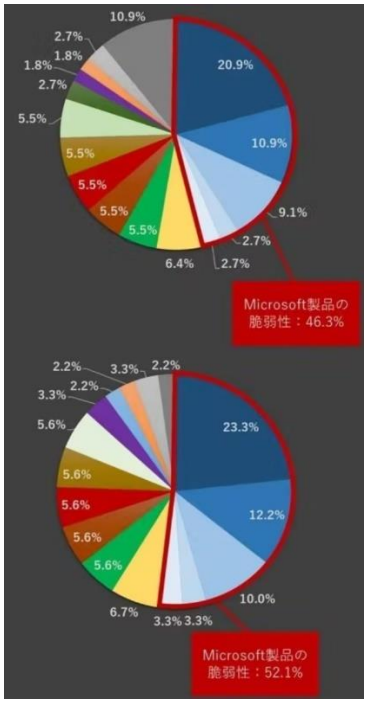
トレンドマイクロは 2 月上旬、ソフトウエアの脆弱性を攻撃するツールの売買状況をまとめたリポートを公表した。
脆弱性を攻撃するツールは「エクスプロイト」と呼ばれる。また、脆弱性とはセキュリティー上の欠陥のこと。エクスプロイトを使えば、企業ネットワークに不正侵入したり、他人のコンピューターを乗っ取ったりすることができる。
つまり、スキルのない人間でもサイバー攻撃が可能になる。実際、多くのサイバー攻撃で使われている。サイバー空間のセキュリティーを脅かす危険な存在といえるだろう。

エクスプロイトは、会員制のアンダーグラウンドフォーラム（サイバー犯罪者などが集う掲示板サイト）などで売買されている。そこでトレンドマイクロは 2019 年 1 月から 20 年 12 月までの 2 年間にわたって、広く知られているアンダーグラウンドフォーラムの「XSS」と「Exploit」に潜入し調査を実施。今回、その結果を公表した。

■マイクロソフト製品を狙う

フォーラムには、エクスプロイトの購入を希望する「購入者」と、販売を希望する「販売者」の書き込みがあふれている。それぞれ、エクスプロイトの種類や価格などを提示している。

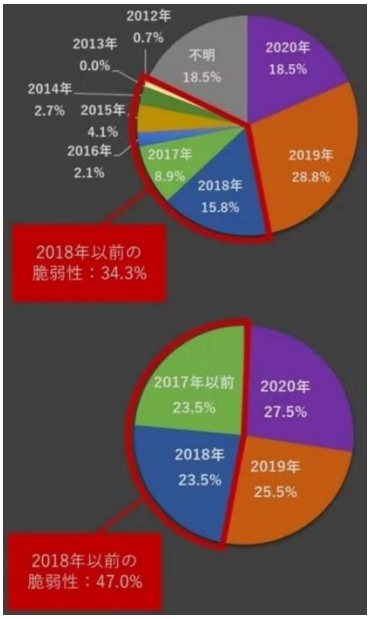
種類別にみると、購入希望と販売希望のいずれでも、米マイクロソフト製品の脆弱性を突くエクスプロイトの書き込みが多かった。ユーザー（攻撃対象）が多いためだ。購入希望では 46.3%、販売希望では 52.1%を占めた。



エクスプロイトが攻撃対象とする製品の内訳（上:購入者の希望、下:販売者の提供物、出所：トレンドマイクロ）（日経電子版より引用）

■実は古い脆弱性を狙う

次に、エクスプロイトが突く脆弱性の公表時期を見てみよう。脆弱性が新しければ新しいほど、ユーザーによるパッチ（修正プログラム）の適用が間に合っていない可能性が高い。このため、最新の脆弱性を突くエクスプロイトが多いように思える。だが実際にはそうではなかった。調査を開始した 19 年 1 月よりも前に公表された脆弱性が多かった。18 年以前の脆弱性を悪用するエクスプロイトが、購入希望では 34.3%、販売希望では 47.0%に上った。



エクスプロイトが攻撃対象とする脆弱性の公表年（上:購入者の希望、下:販売者の提供物、出所：トレンドマイクロ）（日経電子版より引用）

■Office 攻撃、35 ドルから

さて、一番気になるのは価格だ。販売価格には幅がある。例えばマイクロソフトの業務ソフト「Office（オフィス）」に対するエクスプロイトの価格は 35 ドルから 50 万ドルだ。50 万ドルは 22 年 3 月第 1 週のおおよその円ドルレート（1 ドル 115 円）で計算すると **5,750 万円**にもなる。

影響を受ける製品	価格
Microsoft Office	35米ドル～500,000米ドル
Microsoft RDP	200米ドル以上
WinRAR	200米ドル～10,000米ドル
PDF	250米ドル以上
Microsoft Windows	500米ドル～10,000米ドル
Cisco	1,000米ドル以上
Internet Explorer	25,000米ドル以下

エクスプロイトの販売価格例（出所：トレンドマイクロ）（日経電子版より引用）

また、エクスプロイトの価格は時間経過とともに下がっていく。ユーザーのパッチ適用が進むためだ。

例えば 18 年 10 月に公開された基本ソフト（OS）「Windows（ウィンドウズ）」の脆弱性を突くエクスプロイトは、同年 12 月には 1 万ドルで販売されていた。だが 19 年 2 月には **5000 ドル**まで下がった。

あるネットワーク機器の脆弱性を突くエクスプロイトは、パッチ公開前の 20 年 2 月には 2 万ドルの値を付けていた。だが同年 3 月にパッチが公開されると販売価格は 1 万ドルになり、同年 8 月には **2000 ドル**になっていた。

■サブスクリプション型サービスが登場

エクスプロイト市場の新潮流としては、サブスクリプション（定額課金）型サービスの登場が挙げられる。

エクスプロイトを売り切るのではなく、エクスプロイトをサービスとして提供する。月額料金を払えば、メニューにある様々なエクスプロイトを使用できる。

サブスクリプション型サービスの広告例（出所：トレンドマイクロ）（日経電子版より引用）

加えて、セキュリティーソフトに検出されないようにエクスプロイトを継続的に改変することや、毎週バージョンアップすることを保証するとうたう。月額料金は 60 ドルから 2000 ドル。サービスによって大きく異なる。

トレンドマイクロによると、サブスクリプション型サービスではほとんどの作業が自動化されているので、高度な知識を持っていなくてもすぐに利用できるという。サイバー犯罪のハードルは下がるばかりである。

一般のユーザーとしては、こういった状況をきちんと認識し、パッチの適用を怠らないことが重要だ。

幸い、現在では多くのソフトウエアがパッチの適用を自動化している。ただ「パソコンが重くなる」などの理由で意図的に自動化を無効にしているケースもあるという。もってのほかである。無効にしてはならない。

またソフトウエアによっては手動で適用する必要がある。その場合には確実に適用する。

脆弱性を放置することは、「攻撃を受けても構わない」と言っているのと同じだ。それぐらい、エクスプロイトを使えば誰でも容易に攻撃できる。実際に攻撃を受けても構わないと思っている人はいないはず。脆弱性は必ず解消しておこう。

毎日使用するパソコンが重くなり、処理速度が遅くなると不便を感じる方がほとんどだと思います。

もちろん、日々セキュリティー関連情報を確認し、自身の知識も最新の状態へ更新することも大切ですが、

被害事例や被害企業は様々で、日々増加するサイバー攻撃に対抗する 1 番初めの対策として、使用しているソフトウエアの修正プログラムの適用が必要だと感じています。