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。

●ランサムウェア攻撃は減少傾向、密かに仮想通貨を採掘させられる「クリプトジャッキング」が増加…米調査

https://japan.cnet.com/article/35113834/
https://wired.jp/2018/01/20/cryptojacking-out-of-control/

このニュースをザックリ言うと・・・

- 1月25日（現地時間）、アンチウイルスソフトベンダーの米Malwarebytes社より、2017年のマルウェアの傾向に関するレポートが発表されました。

- 発表によれば、2017年5月に猛威をふるったWannaCry（WannaCrypt）等のランサムウェアは、ユーザ側でデータバックアップ等の対策が進んだことにより、7月以降感染率が急減したとされています。

- 一方で、従来からあるオンラインバンキングを狙うトロイの木馬やアドウェアへの回帰の他、ユーザのPCリソースを密かに仮想通貨の採掘に使用させる「クリプトジャッキング」が増加しているとのことです。

AUS便りからの所感等

- クリプトジャッキングはWebサイト上にJavaScriptのコンポーネントを埋め込むことにより実現可能とされ、Webサイトを訪問したユーザのPCリソースを（大抵はユーザの了承なく）消費させられ、ブラウザやPC全体のパフォーマンスに影響が及ぶ恐れがあります。

- Webブラウザ「Opera」が広告ブロック機能においてクリプトジャッキングもブロック対象に追加しており、以後も他のブラウザや広告ブロックのアドオン、あるいはアンチウイルス・UTMにおいて同様の実装が行われるものと考えられます。

- ランサムウェアの感染率は減少したとしていますが、実際に身近で経験がないユーザにおいてはデータのバックアップ体制が整っていないところもあるかも知れませんので、引き続き、バックアップされたデータまで破壊されないよう可能な限りオフラインバックアップを行う等に留意しましょう。


cnet Japan

ランサムウェア攻撃は減少傾向、「クリプトジャッキング」が増加--米調査

Laura Hautala （CNET News） 翻訳校正： 湯本牧子 高森郁哉 （ガリレオ） 2018年01月29日 11時33分

ニュースの見出しを飾ったランサムウェア攻撃から1年になるのを前に、ハッカーらが仕掛ける攻撃の頻度は低下しつつあるようだ。

ランサムウェアは、2
た。しかし、Malwa
たという。

レポートによると、コンピュータユーザーがランサムウェアに対抗する非常に有効なツールを手にしたことが明らかになった。そのツールとは、ファイルのバックアップだ。

そう指摘するのは、Malwarebytesでマルウェア担当アナリストを務めるChris Boyd氏だ。同氏は米ZDNetの取材に対し、大規模なランサムウェア攻撃に関する報道がおそらく、人々がファイルをクラウドやバックアップデバイスにアップロードして身代金支払いを回避する方法を学ぶのに役立ったのだろうと述べた。

「それだけで、追加のセキュリティ対策をしなくても、本来なら相当なものだったはずの脅威が効果的に緩和される」とBoyd氏は述べた。同社はビジネスユーザーや一般ユーザー向けに、悪意のあるソフトウェアに対して保護やブロックを提供する製品を販売している。

しかし、ハッカーらが活動しなくなったというわけではない。従来からあるバンキング型トロイの木馬やアドウェアなどの、他の攻撃手段に乗り換えている。

またハッカーらは、依然として革新を図っている。Malwarebytesでマルウェア関連情報担当ディレクターを務めるAdam Kujawa氏によると、同氏が12月に確認した最大のトレンドは「クリプトジャッキング」の増加だという。これは、ネットユーザーが訪れたウェブサイトがひそかにユーザーのPCの処理能力を利用して、仮想通貨をマイニングするプログラムを実行する、というものだ。

ハッカーらはクリプトジャッキングにより、ユーザーのPCから利益を得ることができる。Kujawa氏によると、「これによりリソースが一気に消耗」し、コンピュータのパフォーマンスが遅くなるという。


WIRED

2018.01.20 SAT 17:00

止まらない「クリプトジャッキング」──暗号通貨の採掘がもたらす「狂騒曲」の行く末

ウェブサイト訪問者の
グ）を行う「クリプト
スの処理能力をかすめ
影響を及ぼす可能性が

TEXT BY LILY HAY NEWMA
EDITERD BY CHIHIRO OKA

WIRED(US)

ツイート いいね

ウェブサイト訪問者の端末を利用し、無許可で暗号通貨の採掘（マイニング）を行う「クリプトジャッキング」と呼ばれる手法 が問題になっている。

この問題だが、マイニングを行うサイトの運営側にも一応それなりの言い分がある。サーヴィスを提供する資金を得るために、誰も使っていない“資源”を利用して広告収入への依存を減らす。つまり、広告を少なくする代わりにユーザーのパソコンを「ちょっとお借りしているだけ」だというのだ。

クリプトジャッキングは、ウェブサイトにJavaScriptのコンポーネントを埋め込むことで、閲覧に使われているデヴァイスの処理能力を暗号通貨（たいていは「Monero」だ）の採掘に利用する。個々のデヴァイスの貢献はほんのわずかなものだが、塵も積もれば、訪問者すべての力をかき集めてある程度の時間にわたって採掘を続ければ、実際に儲かるというわけだ。

こうした仕組みについて、ユーザーは何が起きているのかまったく気づかないかもしれない。理論上はWin-Winということになるが、もちろん実際にはそんなことはない。

●12月の不正侵入の件数は前月比2割以上の増加…警察庁発表

https://scan.netsecurity.ne.jp/article/2018/01/15/40498.html

このニュースをザックリ言うと・・・

- 1月12日（日本時間）、警察庁より、同庁が設置する定点観測センサーに対するアクセス観測状況をまとめた「平成29年12月期観測資料」が発表されました。

- センサーが検知した1日・1IPあたりのアクセス数は1966.8件で、前期（11月期）より73.6件（3.6%）減少である一方、不正侵入等の行為として検出されたのは862.8件で、前期より164.1件（23.5%）増加となっています。

- また、DoS攻撃被害観測において検知した1日あたりの件数は、51707.6件で、前期より32258.4件（165.9%）増加という結果が出ています。

AUS便りからの所感等

- 前述した以外の結果では、アクセス先ポートの上位に「23/TCP(Telnet)」「445/TCP(Windowsのファイル共有等)」「22/TCP(SSH)」「1433/TCP(SQL Server)」に次いで「2323/TCP(一部IoT機器の管理ポート)」が入り、徐々に増加しており、マルウェアMiraiの亜種であるSatoriの攻撃が活発化したことが要因とみられます。

- PCのように自身でファイアウォール機能等を持っているとは限らず、インターネット上から直接アクセスされる状態で設置されるIoT機器は攻撃者の格好のターゲットですので、機器の意図しないポートにアクセスされないよう、必ずルータ・UTMのポートフィルタリング機能等により、防御を行ってください。


ScanNetSecurity

調査・レポート・白書／ブックレビュー

不正侵入は2割増加、DoS攻撃は2.5倍以上の増加--12月のアクセス観測状況（警察庁）

警察庁は1月12日、同庁のセンサーに対するアクセス観測状況をまとめた「平成29年12月期観測資料」を「@police」において公開した。これによると、センサーに対するアクセス件数は、1日・1IPアドレスあたり1,966.8件で、11月期（前期）から73.6件（3.6%）減少した。発信元IPアドレス数は、1日あたり62,575.6個で、前期から3,534.5個（6.0%）増加している。

シグネチャで検知した不正侵入等の行為の件数は、1日・1IPアドレスあたり862.8件で、前期から164.1件（23.5%）の増加。発信元IPアドレス数は1日あたり1,165.9個で、前期から110.4個（10.5%）増加した。DoS攻撃被害観測において検知した件数は、1日あたり51,707.6件で、前期から32,258.4件（165.9%）増加した。発信元IPアドレス数は1日あたり282.0個で、前期から59.2個（17.3%）減少している。

宛先ポート別検知件数（今期順位）

発信元国・地域別検知件数（今期順位）

不正侵入等の攻撃手法別検知件数（今期順位）

シェア　ツイート

もっと「警察庁」のニュース

「Mirai」に感染したRealtek社製SDK搭載Wi-Fiル…

IoT機器への不正アクセスが目的と思われる、MQT…

「WannaCry」や「Mirai」の亜種や別種によるアク…

●ネットショップ運営サービス「カラーミーショップ」不正アクセス…個人情報7万7000件以上流出か

http://www.itmedia.co.jp/news/articles/1801/26/news066.html

このニュースをザックリ言うと・・・

- 1月26日（日本時間）、各種ネットサービスを提供するGMOペパボ社より、ネットショップ運営サービス「カラーミーショップ」が不正アクセスを受け、クレジットカード情報を含む個人情報の流出の可能性があると発表されました。

- 発表によれば、流出が確認されたのはショップオーナーのクレジットカード番号22件およびログインID・住所・氏名等77385件とされ、他にショップオーナーのクレジットカード情報（最悪セキュリティコードを含む）最大9430件、購入者のクレジットカード情報最大2711件も流出した可能性があるとされています。

- 同7日に不正アクセスの発生が確認されて侵入経路を遮断、その後の調査により、第三者にクレカ情報を閲覧された可能性があることが判明しています。

AUS便りからの所感等

- クレジット取引セキュリティ対策協議会では2016年に「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」を取りまとめており、EC事業者は2018年3月末までに、カード情報を保持しないシステムとする、またはクレジットカードにおけるデータセキュリティの国際基準である「PCIDSS」に準拠することが要求されています。


ITmedia NEWS

GMOペパボ「カラーミーショップ」に不正アクセス　クレジットカード情報が流出

2018年01月26日 11時40分 公開　[ITmedia]

印刷　通知　145　53　B! 6

GMOペパボは1月26日、同社のネットショップ運営サービス「カラーミーショップ」が不正アクセスを受け、ショップオーナーのクレジットカード情報22件、それ以外の個人情報77万7385件が流出したと発表した。加えてショップオーナーと購入者のクレジットカード情報約1万2000件が流出した可能性もあるという。現時点では、不正利用の被害報告はないとしている。

- PCIDSSにおいては、カード番号・利用者名・有効期限は業務上必要な場合のみ保存可、一方セキュリティコードは保存不可とされているものの、セキュリティコードを含むクレジットカード情報の流出は後を絶ちません。

- 不正アクセスされない・されても情報が流出しないシステムであるだけでなく、流出しては困るセンシティブな情報をできる限り保持しないようにすることが流出によるダメージを抑えるために重要な要素と言えます。