2019 年 11 月 29 日

サービス＆セキュリティ株式会社 e-Gate センター

増加を続けるコインマイナーの最新動向と対策

1. はじめに

2017 年に急増した、感染した端末を利用し仮想通貨をマイニングするマルウェア「コインマイナー」による被害は今もなお増加の一途をたどっています。今回のニュースは、コインマイナーの最新動向とその対策についてご紹介いたします。

2017 年 12 月、仮想通貨ビットコインの価値が急騰し、1BTC[1]あたり約 19,000 米ドルという過去最高額を記録し、仮想通貨市場も爆発的に拡大しました。それに伴い仮想通貨のセキュリティに対する不安が叫ばれています。仮想通貨取引所のコインチェックから 580 億円相当の仮想通貨が流出した事件は大きな話題となりました。時間や状況に関係なく送金でき、匿名性の高い仮想通貨はサイバー犯罪者から狙われやすいものといえます。

サイバー犯罪者による不特定多数の端末をターゲットにした仮想通貨発掘マルウェアのコインマイナーによる被害が多数発生しています。脆弱なセキュリティシステムを悪用され、更なるマルウェアに感染する危険性を考えるとセキュリティ対策は必要不可欠です。そこで本記事では、コインマイナーの仕組みやその対策方法をご紹介いたします。

2. 仮想通貨とコインマイナー

仮想通貨とは高度な暗号技術によって取引の安全性が確保されたデジタル通貨の一種です。従来の電子マネーや銀行システムのような直接的な管理者の存在する中央集権型のシステムとは異なり、仮想通貨は公的な管理者が不在の非中央政権型の分散化されたネットワークで管理されています。

仮想通貨の新規発行及び管理は、マイニング（発掘）と呼ばれる暗号化アルゴリズムを利用した演算作業によって行われます。特定用途向け集積回路（ASIC）のような発掘に特化したハードウェアやコンピュータネットワークがマイニングという計算処理を行うことで取引の検証を行います。この処理に対して報酬を与える仕組みが用いられており、計算処理の成功者に仮想通貨が支払われます。マイニングは膨大な計算処理とそれに相応する設備投資が必要となります。マイニング量はハードウェアへの投資額に比例するため、ハイスペックなコンピュータを使うための膨大な資金や電力が必要です。そこでサイバー犯罪者は不特定多数の端末でマイニングを実行するマルウェアのコインマイナーによってこれを解決します。2011 年中ごろから確認され始めたマルウェアですが、2017 年以降全世界的に検出台数の増加がみられており、特に 2017 年第 3 四半期に入り急激な増加が確認されています。この原因としてインターネットユーザーへの攻撃が確認された脆弱性攻撃サイトの増加や、仮想通貨マイニングツール「Coinhive[2]」の悪用が挙げられます。Coinhive のマイニング対象である「Monero」と呼ばれる仮想通貨は高い匿名性を有しており、マイニング効率の良い仮想通貨としてサイバー犯罪者の関心を集めています。

---

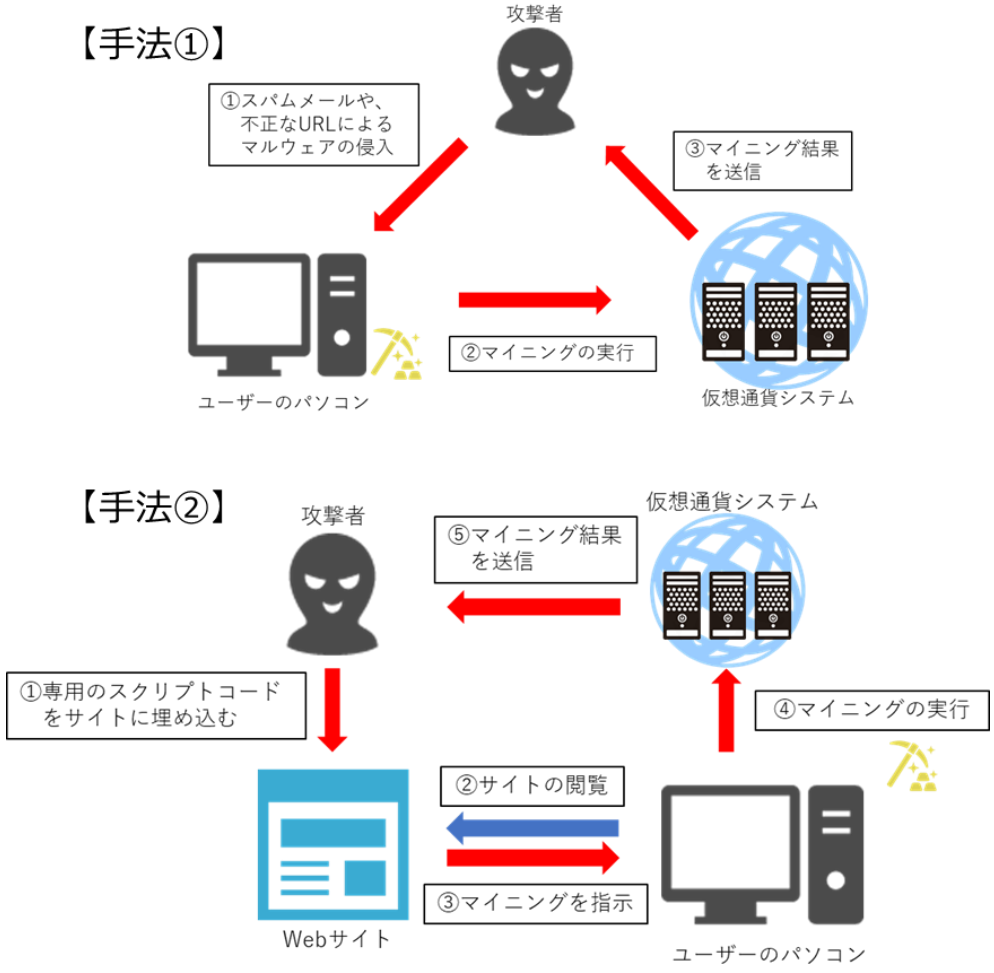
[1] 1BTC＝1 ビットコイン

[2] Coinhive は 2019 年 3 月上旬にツールの提供サイトが閉鎖されました。今後このツールを利用したマイニングは沈静化すると考えられますが。悪意のある Coinhive が完全に消滅するには時間がかかる可能性があります。

2.1. コインマイナーの仕組みと侵入経路

前述の通りサイバー犯罪者は不特定多数の端末にマルウェアを感染させマイニングを実行するシステムを形成します。IoT デバイスがあらゆる場所で利用されるようになり、同時にセキュリティリスクのある IoT デバイスが多く存在しており、これらのデバイスがターゲットとなります。

下図のようにマルウェアの主な侵入経路は２つあり、【手法①】スパムメールの添付ファイル、不正な URL 経由のダウンロードと、【手法②】事前に Web サイトにスクリプトを埋めこむ「クリプトジャッキング」と呼ばれるものが存在します。



【図１　コインマイナーの仕組みと侵入経路】

2.2. 影響

コインマイナーに感染しても端末のデータ破損や OS の損傷といった被害は引き起こされません。しかし、マイニング処理のために CPU などのリソースを使われてしまうため端末の処理能力が低下し、ひどくなると暴走、停止するケースもあります。機密性、完全性に影響を与えるその他のマルウェアや可用性の損失を与えるランサムウェア、DDoS 攻撃のようなサイバー攻撃による脅威と比較すると仮想通貨の無断マイニングはそれほど大きな脅威ではないと判断されるかもしれません。しかし、企業組織における大規模な仮想通貨のマイニングによって生じるエネルギーコストは軽視できるものではありません。また、演算リソースが消費されることで重要な企業資産の可用性に影響を及ぼす可能性もあります。

マイニングを目的とした攻撃の手法やその対策について情報を取りまとめたニュースを e-Gate センター及びグループ会社のセキュアソフトより発行しておりますので、詳しくは下記 URL をご参照下さい。

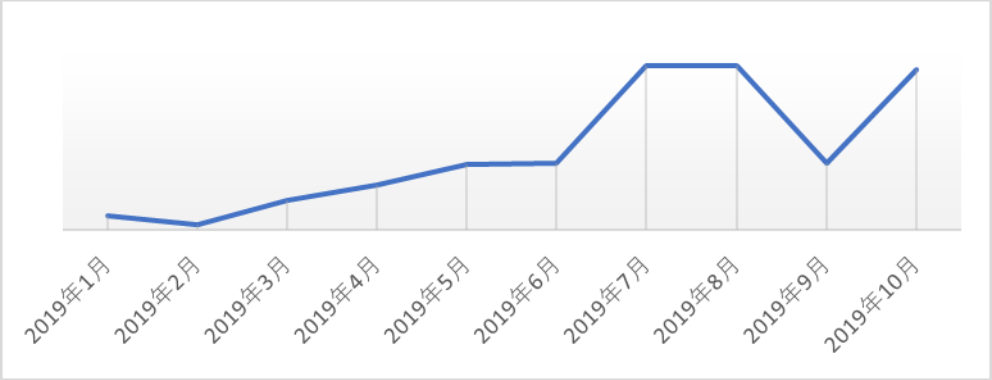
【仮想通貨のマイニングを目的とした攻撃や脅威に関連するニュース】
注意喚起：WebLogic Server の脆弱性を突いた攻撃について
https://www.ssk-kan.co.jp/topics/?p=9093
注意喚起：Drupal の脆弱性を狙った攻撃について
https://www.ssk-kan.co.jp/topics/?p=9115
注意喚起：クリプトジャッキングの脅威について
https://www.securesoft.co.jp/news_mt/2017/12/2-1/

2.3. 最新動向

・ThinkPHP の脆弱性を利用したコインマイナーボットネット

中国製の PHP フレームワークである ThinkPHP で構築された Web サイトを標的とした攻撃が多数報告されています。この脆弱性が悪用されると攻撃者はリモートから任意のコードを実行することができます。この ThinkPHP の脆弱性を悪用し、仮想通貨のマイニングを目的としたワーム機能によって増殖する 2 つのボットネット[3]が存在します。

e-Gate センターにおいても ThinkPHP の脆弱性を狙ったとみられる通信を観測しています(図 2)。2019 年に入ってから検知数が増加しており、依然として多くの通信を確認しております。



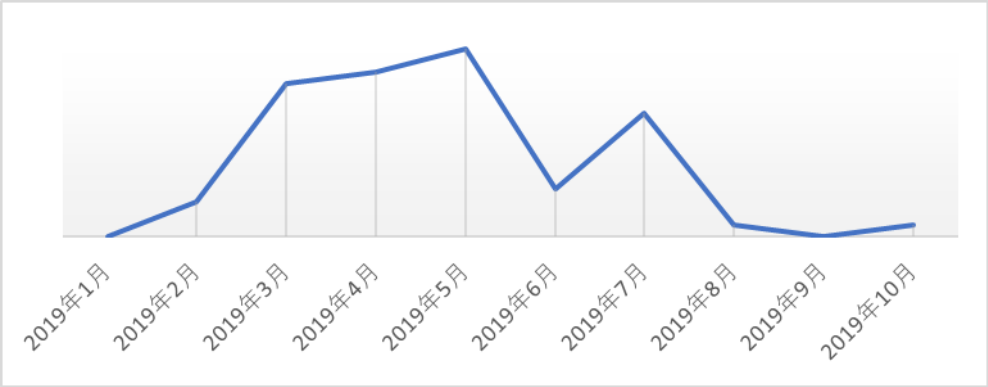
【図 2 ThinkPHP 関連の攻撃イベント数の推移】

① BuleHero

「BuleHero」は複数のセキュリティ脆弱性を悪用し、Windows サーバを制御してマイニングを行うボットネットです。リモートコード実行の脆弱性を利用することで、仮想通貨「Monero」のマイニングツールを含む悪質なバイナリファイルをダウンロードし実行します。ThinkPHP の脆弱性を持ち、インターネットに公開されているホストはワームに感染し、このボットネットに強制的に組み込まれます。

図 3 は e-Gate センターの監視するシステムにおける BuleHero に関連する攻撃イベント数の推移です。2019 年 7 月以降、イベント数は減少傾向にありますが、10 月以降も継続し検知されており依然として警戒が必要です。

[3] ボットネットとは、サイバー犯罪者の指令や遠隔操作などを受け入れるよう悪意のあるソフトウェア（マルウェア）に感染させた多数のコンピュータから成るネットワーク。



【図 3　BuleHero 関連の攻撃イベント数の推移】

② **sefa**

「sefa」は ThinkPHP の脆弱性を利用し、ホストの制御を奪う IoT ボットネットです。マイニングソフトウェア Mcoin をダウンロードする＜シェルファイル＞とワームを拡散するために使われるランダムに生成された IP アドレスをスキャンする＜攻撃モジュール＞の２つをダウンロードして実行します。IoT ネットワークを悪用し、「Monero」をマイニングします。また、IoT デバイスだけでなく、Linux サーバを制御しマイニングを行うことも報告されています。

・ハイブリッド化する攻撃

サイバー犯罪者の攻撃目的にも変化がみられています。仮想通貨価格の高騰が落ち着き、マイニング報酬が停滞しており、これまでのマイニングのみを目的としていたものからクロスサイトスクリプティングや SQL インジェクションなどの＜Web ベース攻撃＞や DDoS 攻撃などの＜ネットワークベース攻撃＞を同時に引き起こすものへと徐々に変化しています。マイニングによるリソースの消費に留まらず、これらの攻撃はネットワークやコンピュータの可用性、完全性、機密性に脅威をもたらし、機密情報の流出といった重大な影響を招きます。また今後、更なるマルウェアの侵入経路として悪用される可能性も考えられます。

3. 対策

コインマイナーの侵入経路は基本的に既知のマルウェアと同じであるため、以下のような通常のマルウェア対策が有効となります。

① **セキュリティソフトの有効化、最新化**

マルウェア対策製品の定義ファイルを最新にして定期的にスキャンを行うことで感染を防ぐことができます。

② **スクリプトをブロックするブラウザ拡張機能の利用**

Coinhive を始めとする Web サイトに埋め込まれたスクリプトによるマイニング（クリプトジャッキング）の多くは JavaScript によって動作します。これを無効化することも有効な対策の一つです。しかし、最近の Web サイトは JavaScript での動作を前提としていることも多く現実的とは言えません。

③ **パッチの適用**

公開されたセキュリティパッチを適用することで、侵入経路として利用される脆弱性から機器を守ることができます。

④ **セキュリティ機器の導入**

IPS は通信を監視するネットワーク機器です。IPS はネットワークやサーバ、エンドポイントへの既知の攻撃パターンに一致する通信の通知や、不正な通信を遮断しシステムを防御する機能を持っています。セキュリティ機器を導入し、適切に運用及び監視をすることによって、マルウェア感染による被害を抑えることができます。

4. e-Gate の監視サービスについて

サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行うことが重要です。“e-Gate“の 24 時間 365 日有人監視体制のセキュリティ監視サービスをご活用頂きますと、最新の分析システムを活用し精度の高い検知、専任のアナリストによる分析、迅速なセキュリティインシデント対応支援でセキュリティ対策を強化することが可能です。“e-Gate”の MSS の導入をぜひご検討ください。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと最新のメソッドで構築した次世代 SOC“e-Gate センター“。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp