アンラボ・セキュリティレター

Press Ahn

2019.2　Vol.62

コインマイナーが狙う仮想通貨 Top4

2018 年マイニング・マルウェア動向

コインマイナーが狙う仮想通貨 Top4

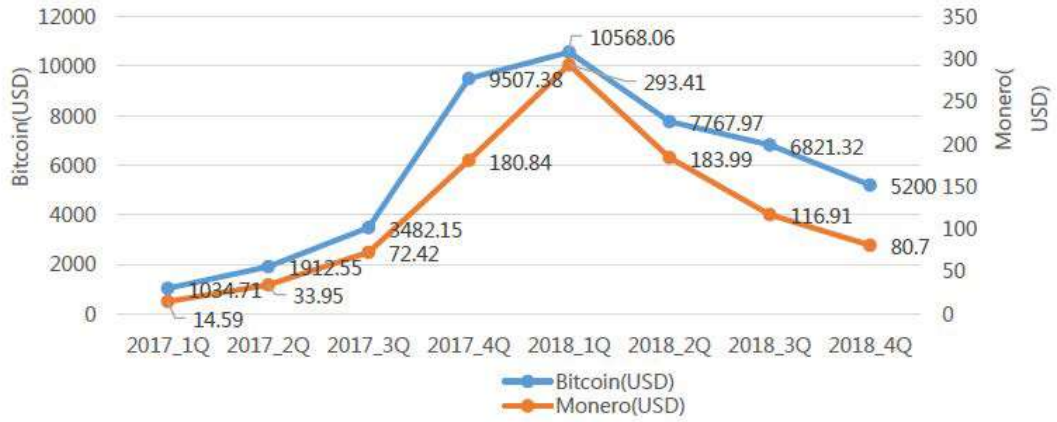
2018年は「コインマイナーの年」といっても過言ではない。2018年アンラボが集計したコインマイナーマルウェアのサンプルは、2017年比 2,254%増という爆発的な数値を記録した。このうち不特定多数に配布されるマルウェアの特性から、マイニング(採掘)演算に CPUを使用する CPUコインマイナー系が最も多いことが分かった。また2018年は、アンラボが確認した感染報告件数 335万4千件のうち上位 10個の診断名の感染報告数が 222万8千件と、全体の約66%を占めていた。

今回のコラムではアンラボセキュリティ対応センター(ASEC)が分析した 2018年コインマイナーの動向と主な特徴を紹介した。

2018年はコインマイナー(Miner)マルウェアサンプルと感染レポートが急増した。同サンプルは、2017年に 12万7千件から、2018年 299万件と2,254%の増加率を見せた。コインマイナーの急増は仮想通貨(Cryptocurrency)の急な価値上昇に起因したものとされ、[図1]と [図2]のビットコイン(Bitcoin、BTC)と Monero、XMR値段の推移グラフから分かるように、2018年第 1四半期仮想通貨の上昇とともにコインマイナーマルウェアの感染報告数が爆発的に増加している。

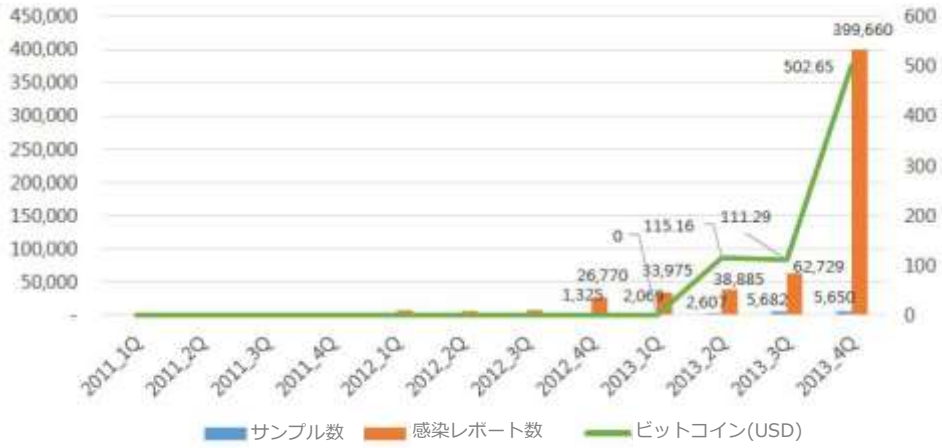
[図1] コインマイナーのサンプル及び感染報告数 vs ビットコイン価格 (※ビットコイン相場 : https://coinmarketcap.com資料基準)

代表的な仮想通貨のビットコインとは異なり、Moneroは取引の匿名性が保証され、誰がどれだけ送金したか把握できない上に性能の良い高価なGPU(Graphics Processing Unit)が搭載されたシステムではなく、一般的なCPU(CentralProcessing Unit)環境でも採掘が可能な代表的なコインだ。これらの理由から、攻撃者は不特定多数に感染させてマイニングできるMoneroを好むとされる。



[図2] ビットコインとMoneroの価格推移（2017～2018）

アンラボは2010年からV3診断名にコインマイナー(Miner)を使用した。マイナーサンプルの拡散は、先述のように仮想通貨の価値に比例して増減してきた。ビットコインは2009年に登場して以来マイニングできるツールが知られ始めた。[図3]のように、2011年以降マイニングを狙ったコインマイナー数と感染レポート数が少しずつ増加したことが分かる。2013年第4四半期の感染レポートは第3四半期比62,700件から399,000件へと537%増加した。この時もビットコイン価格が前四半期の111ドル→502ドルまで350%も急騰している。これらのケースからも、仮想通貨の価値上昇がマイナーマルウェアの増減に影響を与えていると推測できる。



[図3] コインマイナーマルウェアのサンプル数と感染報告数(2011～2013)

しかしコインマイナーの活動が仮想通貨の価値に左右されると断定することはできない。一例として2018年第4四半期のコインマイナーの活動を見ると、この時期は妙な動きを見せている。

2018年第3四半期に257,000件だったサンプル数は2018年第4四半期に730,000件と183%増加した。サンプル数のみ増加したなら単に変形が増加しただけと見て取れるかもしれないが、この期間の感染レポート数もまた第3四半期286,000件→第4四半期634,000件へと121%も増加した。これは今まで見た仮想通貨の価値上昇と比例したコインマイナーの増加と反対の動きである。([図1] 参照)

[図4] コインマイナーのマルウェアサンプル数と感染報告数 vs ビットコイン価格（2014～2015）

過去にも仮想通貨の価値上昇に関係なく、2018年第 4四半期のようにサンプル数や感染レポート数が増加したケースはあっただろうか。

これに対する答えは [図4] で確認できる。2014年第 4四半期から 2015年第 1四半期の間に似たような動きがあった。[図4]のようにビットコインの価格が下落ぎみの中、2014年第 4四半期から増加し始めたサンプル数は 2015年第 1四半期に最高潮に達した。仮想通貨の相場の上昇に関係なくサンプルと感染報告数が増加する理由に特別な因果関係は見受けられなかった。マルウェア作成者は相場の動きと関係なくコインマイナーを拡散させて、積極的に活動することもあるようだ。

コインマイナーの拡散手法

コインマイナーは、ユーザーに知られないようにこっそりとシステムリソース(CPU、GPU演算)を利用して仮想通貨を採掘するマルウェアを指す。ビットコインの場合、取引履歴を記録したブロックを生成するとその褒美に入手できるが、このような行為を「採掘(マイニング、Mining)」という。もともと採掘は正当な目的で利用されていたが最近は関連マルウェアが増加し、ハッカーがユーザーのシステムを利用して採掘する『Cryptojacking』が浮上した。詳しく見てみると、取引履歴を記録したブロックハッシュがランダムに生成され、これを一つ一つ代入することでハッシュを検証する。その過程で演算を高速で繰り返し実行するため、コンピューターの CPUや GPUリソースを多く使用する。コインマイナーはこのような行為をこっそり実行して感染システムのリソースを奪取した。

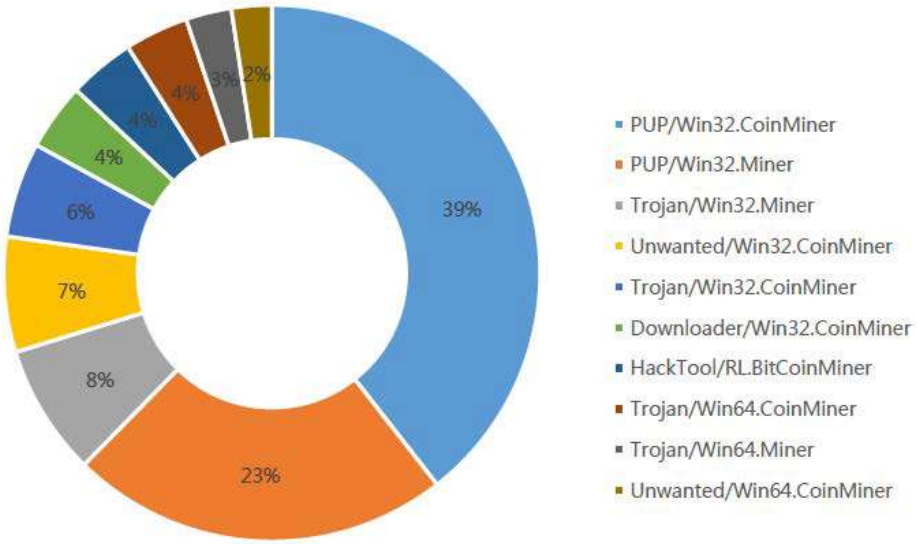
コインマイナーの採掘による被害レベルは個人や企業によって差がある。個人ユーザーの場合は CPUや GPUリソースが消耗されることによる PCのパフォーマンス低下が発生する。企業の場合は不要なリソース消費による電力の浪費に加えて、ビジネスの生産性低下に繋がりかねない。採掘では高速演算を繰り返すために高性能の CPUが搭載されたシステムに加えてより多くの消費電力が必要になる。よって 24時間稼動する企業の高性能サーバー機器は攻撃者にとって恰好のターゲットになる。

ならコインマイナーは、どのようにして配布されるのだろうか。まず Windows環境では「ブラウザベースのマイニング」または「ドライブ・バイ・マイニング(Drive by Mining)」がある。この方式は、システムにアドウェアおよびマルウェアを個別にインストールさせたり感染させることなく採掘可能であることが特徴だ。攻撃者はマルウェアをサイトに挿入した後でユーザーがサイトを訪問したり、攻撃者が意図したサイトにアクセスすると採掘を行う。

だがこの方法の欠点は、ブラウザでそのページが開いているときのみ動作するという点だ。このため同手法で採掘を行おうとする攻撃者は、ユーザーがそのページに最大限留まるように刺激的な内容のサイトを運営することが多い。もちろんこのようなサイトを運営しなくても、一般的な Webサイトの脆弱性を利用して管理者がこっそりとスクリプトを挿入することもある。

コインマイナーが使用する手法のうち 2018年に最も多く利用されたのは『アドウェア』だった。([図5]を参照)

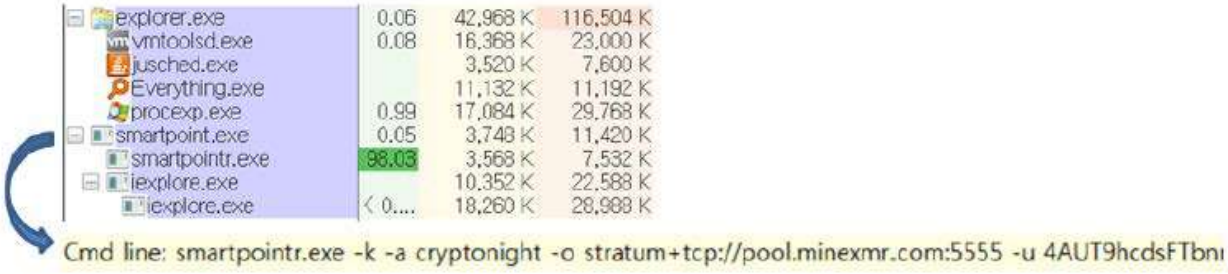
2018年アンラボが集計した感染報告例 335万4千件のうち、上位 10個の診断名の感染レポートが 222万8千件で、全体の約 66%を占めた。



[図5] 2018年コインマイナー感染報告サンプル数 TOP10

アンラボ診断名を基準に 1位と 2位を占めた PUP/Win32.CoinMinerとPUP/Win32.Minerは、スマートポイント(SmartPoint)アドウェアによってインストールされる。このプログラムは PUP(Potentially Unwanted Program)タイプであり、ユーザーに『インストールするとポイントを獲得できる』旨の案内ページを提供している。だがインストールする際に PCリソースを多く使用するため、ユーザーに不快感を与えることになる。

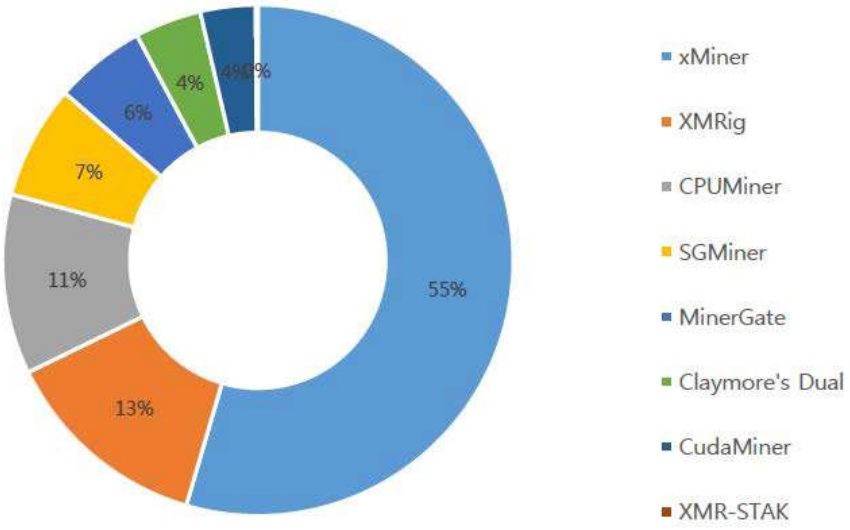
4位にランク入りした Unwanted/ Win32.CoinMinerは、今は頒布が中断された Epic Scaleアドウェアと関連がある。同アドウェアは主にファイル共有プログラムである『Torrent』のインストールファイルに含まれて拡散され、ユーザー数が多いプログラムであるだけに実際の感染者も多かったことが確認された。



[図6] スマートポイントアドウェアのマイニング

感染報告サンプルで確認されたコインマイナー

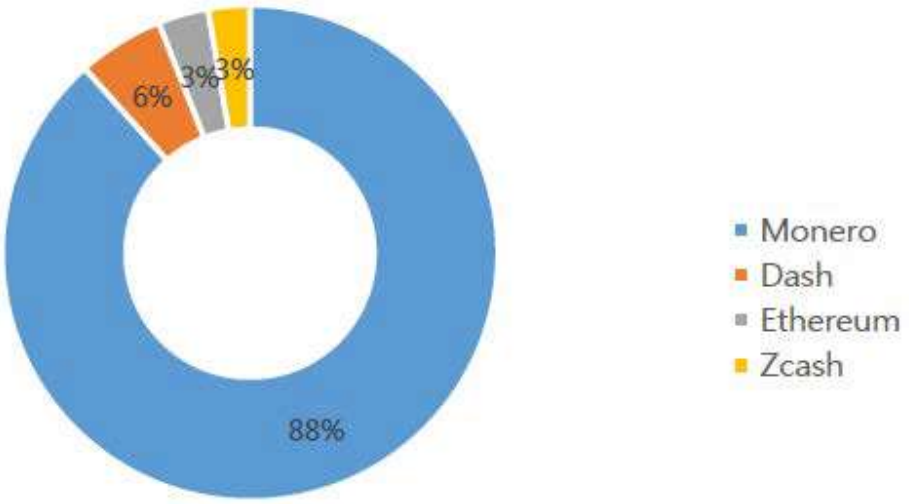
2018年最も悪用されたマイナータイプは、オープンソースをベースにした CPUマイナー(xMiner、XMRig)類だった。[図7]のように 2018年マイナーマルウェア感染レポートサンプルの上位 10個のサンプルから 40,000個の標本サンプルを抽出して分析した結果から確認された。攻撃者は自主的に制作するよりも、知られたオープンソースを変形したコインマイナーを攻撃に用いたと見られる。



[図7] コインマイナータイプの割合（感染報告のサンプル基準）

2018 年コインマイナーが最も多く狙った仮想通貨は

コインマイナーはどんな仮想通貨を採掘するだろうか。最も多く採掘対象とされた仮想通貨は、Monero、Dash、Ethereum、Zcashの 4種だった。



[図8] 採掘対象となった仮想通貨 TOP 4（感染報告のサンプル基準）

Moneroが最多となった理由には、他の仮想通貨とは異なり匿名性に重点を置いて開発されたため、マルウェア作成者に悪用されやすい点がある。マルウェアを利用した金銭的利益は、マルウェア作成者たちにとって強力な動機となる。すでにランサムウェアを介して金銭的利益を得た経験があるだけに、匿名性まで保証される仮想通貨はうってつけのターゲットだろう。
さらに、コインマイナー作成はランサムウェアよりも時間とコストの面でより経済的だ。ほとんどがオープンソースを変形したものであるため、ランサムウェアに比べて比較的スムーズに着手できるからだ。

多くのセキュリティ企業でも証言するように、マルウェア作成者はランサムウェアからコインマイナーのほうに移行しつつある。今後はユーザーに発覚されることなく少しでも長くシステムに留まる戦略に進化するだろう。また Windows環境以外の IoT環境でも配布・動作する脅威も見過ごせない。これら脅威動向の変化に対応するため、セキュリティ企業らは従来の Windows、Linux、Mac OS 環境だけでなく、より多くのデバイスのセキュリティをカバーしようと取り組んでいる。このような試みはセキュリティベンダーレベルで終わるのではなく企業の管理者や個人ユーザーの積極的な参加が必要だ。ユーザーは製品を選択する際にセキュリティに配慮された製品を優先し、製品のセキュリティパッチと最新バージョンのアップデートを習慣づけして、新たな脅威の登場に先手を打つことが重要だ。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

© 2019 AhnLab, Inc. All rights reserved.