クリプトジャッキングは今後どうなる？

クリプトジャッキングは監視対象にすべき

マルウェアに感染させて他人のマシンでマイニング
Web ページ改ざんで無断に閲覧者のマシンでマイニング

承諾を得ず、他人のコンピュータを利用して、無断でマイニングする行為は犯罪であり、セキュリティ対策が必要

クリプトジャッキングは、他人のコンピュータを勝手に使用して仮想通貨のマイニングをする行為です。
代表的な手口は、犯罪者が他人のパソコンをマルウェアに感染させてマイニングを行う手口や、Web サイトを改ざんして不正なコードを埋め込み、ユーザーがサイトのページを閲覧すると、マイニングを行うコードが自動的に実行され、犯罪者が仮想通貨を得る方法などです。
このクリプトジャッキングの被害は、知らないうちに不正にコンピュータが使用され CPU パワーが奪われることです。
それによる電力料金や他のアプリへの負荷などが被害の影響ですが、ランサムウェアほど目に見える金額の被害が出ないところが特徴で、本人が気づかないところで犯罪に協力させられてしまっている場合が多いです。
そもそも仮想通貨のマイニングという行為自体は、仮想通貨にとって台帳を承認し運営するために必要なことで、決して悪いことではありません。
実際に国際連合児童基金 (UNICEF) オーストラリアは、「The Hopepage」という Web ページを開いている間、閲覧者の CPU を使用して仮想通貨のマイニングをして、マイニングした仮想通貨を寄付に充てるというウェブサイトを公開していました。寄付したお金は安全な水や食糧、薬など、子どもたちを救うために使われる目的です。
この例のように、広告収入の代わりに、そのサイトを応援する人に同意を得ている場合は、手軽に寄付できる仕組みとしてはとてもよい方法です。
しかしながら、犯罪者は、こうした仕組みを悪用し、たとえばアクセスの多い Web ページを勝手に改ざんし、仮想通貨 Monero のマイニング用コードを埋め込み、閲覧者のコンピュータで Javascript を起動して、不特定多数のリソースによってマイニングして仮想通貨を得るというようなクリプトジャッキングを行っています。
有名な BitCoin などは、GPU などの高性能なマシンがマイニングに必要ですが、仮想通貨によっては普通の CPU でマイニングが可能なものがあるため、スマートフォンや IoT 機器などでもこのクリプトジャッキングは行われています。
これは、本人が同意している場合は、犯罪とは無関係なので防御すべきかが問題だったのですが、多くのウィルス対策ソフトがデフォルトではこの行為をセキュリティ監視対象にしてきたため、今後は沈静化するものと思われます。