2017 年 12 月 28 日
株式会社セキュアソフト

注意喚起：クリプトジャッキングの脅威について

1. 概要

昨今、ビットコインなど仮想通貨に対応する金融機関も出てきており、仮想通貨の対応サービスは広がりを見せています。仮想通貨の入手にはマイニングという方法が存在し、クリプトジャッキングという手法が最近話題となっております。
クリプトジャッキングは、Web サイト上に設置された JavaScript コードによりマイニングを行う手法で Web サイト閲覧者の PC が、マイニングに利用されてしまうものとなっています。マイニング処理はバックグラウンドにて動作する為、ユーザーに発見されにくいという特徴があります。
また、ハッキングなどにより乗っ取られた Web サイトにこのコードが勝手に設置されていたという例も報告されており、被害が拡大する可能性がある為より一層の注意が必要です。

2. クリプトジャッキングとは

クリプトジャッキングとはマイニングの手法の一つです。
Web サイト上に JavaScript のマイニングスクリプトを設置する事により、サイト閲覧者のブラウザ上にてマイニングを実行させることにより収入を得ます。
スクリプトはインストール作業を必要とせず、バックグラウンドにて動作します。また一部スクリプトはユーザーの同意なしに動作させる事が可能です。
スクリプト設定により CPU の使用率をコントロールすることが可能となっており、CPU 使用率を抑えることでサイト閲覧者に発見されにくくすることや、CPU を 100%占有することも可能となっています。

⑴ 想定されるマイニングスクリプト設置例
① サーバ運用者が広告収入の代わりに Web サイト上にマイニングスクリプトを設置
② 攻撃者により Web サーバが乗っ取られ、攻撃者が収入を得るためにマイニングスクリプトを設置

⑵ クリプトジャッキングの実例
① 2017 年 9 月 The Pirate Bay が 広告の代わりにマイニングスクリプトをテストしていると発表。
② 2017 年 9 月 有料動画配信サイト Showtime にてマイニングスクリプトによりサイト閲覧者の CPU 使用率が 60%となる問題が発生。
③ 2017 年 10 月 ファクトチェックサイト Politifact.com がサーバ設定ミスによりハッキングを受け、マイニングスクリプトを不正に設置されてしまい、サイト閲覧者の PC の CPU 使用率が 100%となる問題が発生。

⑶ 対策方法

対策としては、クライアント側で行う対策と、サーバ及びネットワークで行う対策が考えられます。

〇クライアント対策

① アンチウィルスソフトの導入
② JavaScript 無効化設定
③ マイニングスクリプト対策機能付き Web ブラウザの導入
④ ファイアウォールによるマイニング通信の遮断

〇サーバ対策

① OS/アプリケーションの最新化
② 不要なサービスの停止
③ 定期的なログ分析による改竄検知

〇ネットワーク対策

① 定期的なログ分析によるマイニング通信の検知
② ファイアウォール/Web プロキシによるマイニング通信の遮断
③ WAF/IDS/IPS による不正侵入通信の検知及び遮断

⑷ 参考情報

■CERT-EU

Increased Use of Browser Cryptojacking (CERT-EU Security Advisory 2017-024)
https://cert.europa.eu/cert/newsletter/en/20171115_SecurityBulletins_1.html

■enisa

Cryptojacking - Cryptomining in the browser
https://www.enisa.europa.eu/publications/info-notes/cryptojacking-cryptomining-in-the-browser

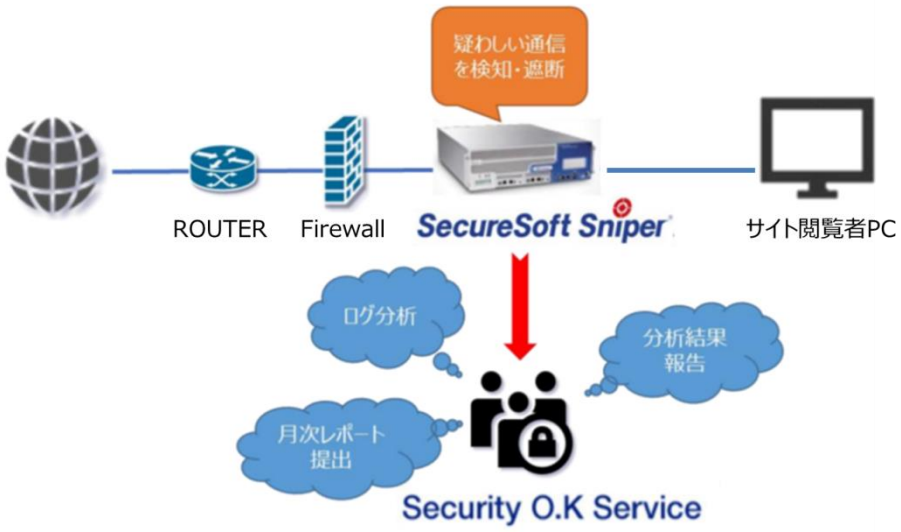
3. IPS とセキュリティ監視サービスを活用した脆弱性対策

今回のような、ユーザーの意図しない通信や、サーバの脆弱性を狙った攻撃通信の検知/遮断には IPS 等のセキュリティ対策機器の設置とセキュリティ監視サービスの導入が効果的です。SecureSoft では、巧妙化する攻撃に対応可能な IPS(SecureSoft Sniper シリーズ)と、不正イベントを 24 時間 365 日監視するサービス(Security O.K Service)を提供しています。

SecureSoft Sniper シリーズ（以下、Sniper）とは、ネットワークを通過するパケットに対して、様々な角度から詳細な分析を行い、攻撃を検知・遮断する事ができる「防御」のための不正侵入検知・防御システムです。

Security O.K Service（以下、S.O.S）とは、最新の相関分析システムとセキュリティアナリストによる高度な分析、迅速なインシデント対応、分析結果を記載した月次レポートの提供によりお客様に安心してご利用いただけるセキュリティ監視サービスです。

システムの脆弱性が確認されバージョンアップなどのシステム更新が必要でも早急に対応できない場合に、Sniper と S.O.S を組み合わせた検出と監視による防御は非常に有効です。
多様化する攻撃に対応する為、セキュリティ監視サービスのご利用をご検討ください。



【図 1】Sniper と Security O.K Service の関連図

■SecureSoft Sniper シリーズ
https://www.securesoft.co.jp/products/
■Security O.K Service
https://www.securesoft.co.jp/security/okservice/

«お問合せ先»

株式会社セキュアソフト

〒150-0011

東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F

TEL 03-5464-9966

FAX 03-5464-9977

sales@securesoft.co.jp