

ウォッちガード、悪意のある仮想通貨マイニングのマルウェアが增加傾向にあると報告



2018年6月29日（金）

ー企業向け統合型セキュリティプラットフォームのグローバルリーダであるWatchGuard (R) Technologiesの日本法人、ウォッちガード・テクノロジー・ジャパン株式会社（本社：東京都港区、代表執行役員社長 谷口

忠彦、以下ウォッちガード）は、四半期毎に作成している「インターネットセキュリティレポート」の最新版（2018年第1四半期）を発表しました。2018年第1四半期の脅威インテリジェンスでは、一般的なLinux/Downloaderの形態を持つマルウェア亜種の98.8%が、拡大するLinuxベースの仮想通貨マイニング（採掘）マルウェアの発信を目的に設計されていたことが判明しました。こうした攻撃は、悪意のある仮想通貨マイニングマルウェアがサイバー犯罪の上位を占めつつある兆候のほんの一例です。本レポートでは、こうした仮想通貨マイニング攻撃の仕組みの詳細を紹介し、中堅／中小企業（SMB）や分散拠点を持つ大企業を標的としたその他の各種のセキュリティ脅威を明らかにしています。

ウォッちガードのCTO（チーフテクノロジオフィサー）であるコリー・ナクライナー（Corey Nachreiner）は、次のように説明しています。「私たちの脅威ラボチームは、悪意のある仮想通貨マイニングが、サイバー犯罪の主力攻撃手段になりつつある複数の兆候を発見し、第2四半期ではさらに増加すると予測しています。ランサムウェアや他の標的型攻撃は、依然として大きな脅威であることに変わりはありませんが、こうした新種の仮想通貨マイニング攻撃は、攻撃者が常に新しい攻撃手法を模索していることを示唆しています。事実、第1四半期にまたしてもマルウェアの約半数が、多様な難読化手法により、従来のシグニチャベースのアンチウイルスソリューションを潜り抜けていることが分かりました。組織がこれらの高度かつ捉えどころのない脅威に対抗する1つの方法として、当社のAPT Blockerなどの標的型攻撃対策機能を実装することが挙げられます。」

ウォッちガードのインターネットセキュリティレポートでは、四半期毎にトップランキングのサイバー脅威に対する深い洞察を提供し、SMBに役立つ防御対策を紹介しています。調査結果は、世界中で運用されている多数のFirebox

UTMアプライアンスから収集されたデータに基づいて作成されています。以下に2018年第1四半期レポートにおける主な調査結果を紹介します：

仮想通貨マイニングのマルウェアが増加。ウォッちガードのマルウェア亜種トップ25に初めて数種類の仮想通貨マイニングのマルウェアが登場しました。Fireboxアプライアンスでは、ダウンロードし、マルウェアペイロードを実行する各種のLinux「ドロッパー」または「ダウンローダ」プログラムを捕捉するLinux/Downloaderと呼ばれるルールを設けています。通常、これらのドロッパーは、広範なマルウェアをダウンロードしますが、2018年第1四半期では、Linux/Downloaderインスタンスの98.8%が同一の著名なLinuxベースの仮想通貨マイニングマルウェアのダウンロード

を試みている結果が出ています。現時点における第2四半期の兆候からして、仮想通貨マイニングマルウェアは引き続きウォッчガードのトップ25リストに残り、四半期の末にはトップ10に入る可能性も出てきています。

Ramnit

trojanがイタリアで復活。ウォッчガードの過去のレポートでトップ10リストにランクインしなかった唯一のマルウェアサンプルは、2010年に初めて登場したtrojanで、2016年に短期間で再度登場したRamnitでした。ウォッчガードが検知したRamnitのほぼすべて（98.9%）がイタリア発であり、標的型攻撃キャンペーンが実施されたものと思われます。Ramnitの過去のバージョンでは銀行情報を標的としていたことから、ウォッчガードではイタリアの方々に対して銀行情報についていつも以上に注意を喚起し、各種の金融口座に多要素認証を適用するようにアドバイスしています。

APACのマルウェアの数が初めて他の地域を上回る。過去のレポートにおいて、報告されたマルウェア数を比較すると、APACはEMEAやAMERに比べて圧倒的に少ない数でしたが、2018年第1四半期では、APACが全体的に最もマルウェアの数が多かったとの結果が出ています。これらの攻撃で大多数を占めたのはWindowsベースのマルウェアであり、98%がインドとシンガポールを標的としていました。

全マルウェアの約半数が従来のアンチウイルス（AV）ソリューションを回避。ウォッчガードのUTMアプライアンスでは、レガシーのシグニチャベースの検知技術と最新のプロアクティブな振る舞い検知ソリューションであるAPT Blockerの両方を用いてマルウェアを防御しています。APT Blockerでマルウェア亜種が捕捉された場合、レガシーのAVシグニチャでは検知できなかったことを意味します。第1四半期のすべてのマルウェアの46%がゼロデイマルウェア（従来のシグニチャベースのAVを回避したマルウェア）でした。このような高度なレベルのゼロデイマルウェアは、犯罪者が引き続き難読化技術を用いて従来のAVサービスを機能不全にしており、振る舞いベースの防御機能の重要性がさらに高まっていると言えます。

Mimikatzが米国を標的にし、アジア太平洋地区ではほぼ被害なし。機密情報を窃取するMimikatz Windowsマルウェアがウォッчガードのトップ10マルウェアリストに数四半期ぶりに登場しました。検知されたマルウェアの3分の2が米国でAPACでは0.1%未満でした。おそらくAPACでは日本など、複雑なダブルバイトの文字を使用している国があり、パスワードも特殊な記号が使用されていることが起因していると思われます。

インターネットセキュリティレポートの完全版では、激増しているGitHub 1.35 Tbps DDoS攻撃の詳細、並びに四半期におけるトップランキングのマルウェアおよびネットワーク攻撃の分析、そしてSMBに役立つ主な防御戦術を報告しています。

今期の結論は、匿名化された世界中で運用されている40,000台近くに及ぶウォッчガードのUTMアプライアンスから収集されたFireboxのデータに基づいています。これらのアプライアンスは2018年第1四半期で、累計2,300万以上のマルウェア亜種を防御し（1デバイス628件）、また1,000万以上のネットワーク攻撃を防御しています（1デバイス278件）。

インターネットセキュリティレポートの担当チームおよびSecplicity.orgによる最新ポッドキャスト「The 443 Security Simplified」<https://www.secplicity.org/category/the-443/>（英語のみ）に是非アクセスして下さい。本ポッドキャストでは、毎週最新のハッキング、攻撃、侵害に関する手法やテクニックについて分析しています。また、最新の脅威情報、攻撃手法を紹介し、企業の防御対策に役立つ実用的な知見を提供します。

レポート全文は以下よりダウンロードできます。

<https://www.watchguard.com/wgrd-resource-center/security-report>

(英語) *日本語レポートは後日公開予定。

また、攻撃の種類、地域、日時ごとにリアルタイムで脅威の知見を提供するウォッчガードの脅威ランドスケープはこちらよりご覧になれます。 (英語のみ)

<https://www.secplcity.org/threat-landscape/>

【WatchGuard Technologiesについて】

WatchGuard (R) Technologiesは、業界標準ハードウェア、ベストオブブリードセキュリティ、ポリシーベースの管理ツールを独自アーキテクチャにより統合したビジネスセキュリティソリューションを提供するグローバルリーダとして、全世界の企業にエンタープライズクラスのセキュリティソリューションを提供しています。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッчガード・テクノロジー・ジャパン株式会社は、多くのパートナーを通じて、アプライアンス製品、ネットワークからエンドポイントまでの脅威検知とセキュリティの「可視化」及びセキュリティとネットワークの「運用管理」など拡大するニーズへのソリューションを提供しています。詳細は <http://www.watchguard.co.jp> をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向はTwitter (@WatchGuardJapan)、Facebook (@WatchGuard.jp)、をフォローして下さい。また、最新の脅威に関するリアルタイム情報やその対策法はSecplcityJPまでアクセスして下さい。

SecplcityJP : <https://www.watchguard.co.jp/security-news>

WatchGuardは、WatchGuard Technologies, Inc. の登録商標です。その他の商標は各社に帰属します。

【本プレスリリースに関するお問合せ】

ウォッчガード・テクノロジー・ジャパン株式会社

〒106-0041

[東京都港区麻布台1-11-9 BPRプレイス神谷町5階](#)

マーケティング担当：角田・堀江

Tel : 03-5797-7205

Fax : 03-5797-7207

Email : jpnsales@watchguard.com

URL : <https://www.watchguard.co.jp>

Generated by ふれりりプレスリリース

<https://www.prerele.com>