2021年
5月
MAY

MALWARE REPORT

# マルウェアレポート

国内のマルウェア検出状況を解説

キヤノンマーケティングジャパン株式会社

# はじめに

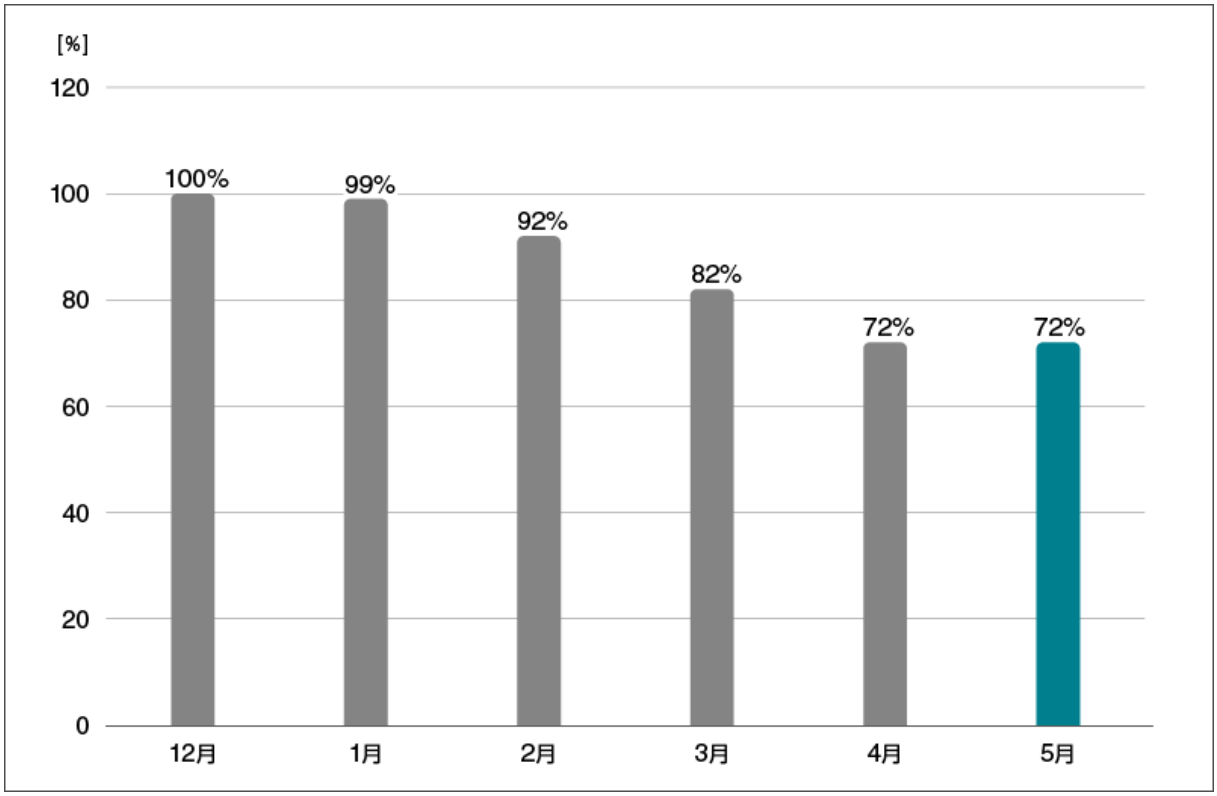
「マルウェアレポート」は、キヤノンマーケティングジャパングループが運営する

「サイバーセキュリティラボ」が「ESET セキュリティ ソフトウェア シリーズ」の

マルウェア検出データを基に国内のマルウェア検出状況を分析し、まとめたレポートです。

# ショートレポート「2021 年 5 月マルウェア検出状況」

2021 年 5 月（5 月 1 日～5 月 31 日）に ESET 製品が国内で検出したマルウェアの検出数の推移は、以下のとおりです。




**国内マルウェア検出数*1の推移**

**(2020 年 12 月の全検出数を 100%として比較)**

*1 検出数には PUA（Potentially Unwanted/Unsafe Application；必ずしも悪意があるとは限らないが、コンピューターのパフォーマンスに悪影響を及ぼす可能性があるアプリケーション)を含めています。

2021 年 5 月の国内マルウェア検出数は、2021 年 4 月に引き続いて減少傾向が続いています。検出されたマルウェアの内訳は以下のとおりです。

**国内マルウェア検出数*2 上位（2021 年 5 月）**

| 順位 | マルウェア | 割合 | 種別 |
|---|---|---|---|
| 1 | JS/Adware.Agent | 19.8% | アドウェア |
| 2 | JS/Adware.Sculinst | 13.3% | アドウェア |
| 3 | DOC/Fraud | 6.1% | 詐欺サイトのリンクが埋め込まれた doc ファイル |
| 4 | JS/Adware.TerraClicks | 5.9% | アドウェア |
| 5 | JS/Adware.Subprop | 5.6% | アドウェア |
| 6 | HTML/ScrInject | 3.0% | HTML に埋め込まれた不正スクリプト |
| 7 | JS/Adware.PopAds | 1.9% | アドウェア |
| 8 | PDF/Fraud | 1.6% | 詐欺サイトのリンクが埋め込まれた PDF |
| 9 | HTML/Refresh | 1.3% | 別のページに遷移させるスクリプト |
| 10 | JS/Adware.Chogdoul | 1.2% | アドウェア |

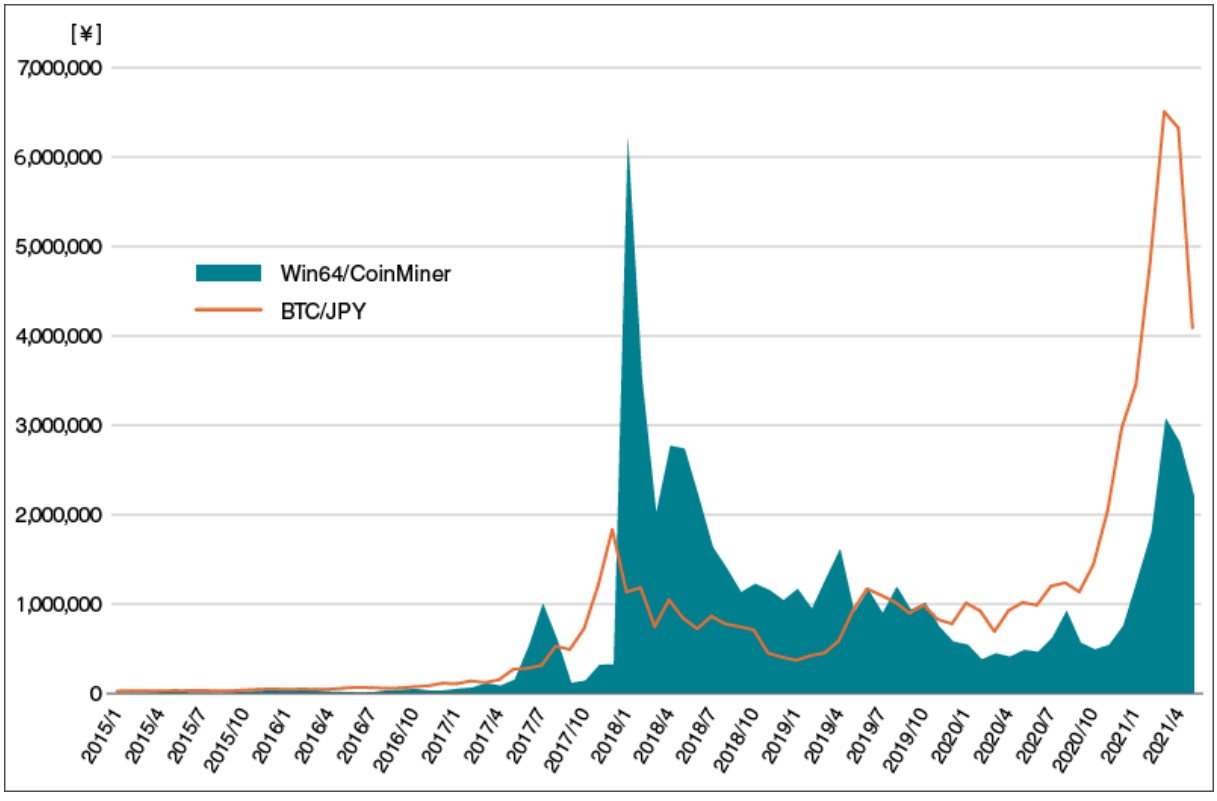
*2 本表には PUA を含めていません。

5 月に国内で最も多く検出されたマルウェアは、JS/Adware.Agent でした。JS/Adware.Agent は、悪意のある広告を表示させるアドウェアの汎用検出名です。Web サイト閲覧時に実行されます。
国内マルウェア検出数上位に複数ある JS/Adware は、国内マルウェア検出数の過半数を占めるほど多く検出しています。

今月は、年初から検出が増加している Win64/CoinMiner についてご紹介します。暗号資産（仮想通貨）が再び高騰し、それに伴い CoinMiner の検出も増加しています。CoinMiner は、暗号資産をマイニングするプログラムです。

ビットコイン（BTC）は、2020 年 4 月には 70 万円ほどでしたが 2021 年 4 月には過去最高値の 700 万円を超え 1 年でおよそ 10 倍の価格になりました。その後、5 月 23 日には一時最高値から 50%下落し話題になりました。また、暗号資産の時価総額 2 位のイーサリアム（ETH）は、5 月 12 日に最高値を更新し、その後 23 日には一時 50%以上暴落しました。

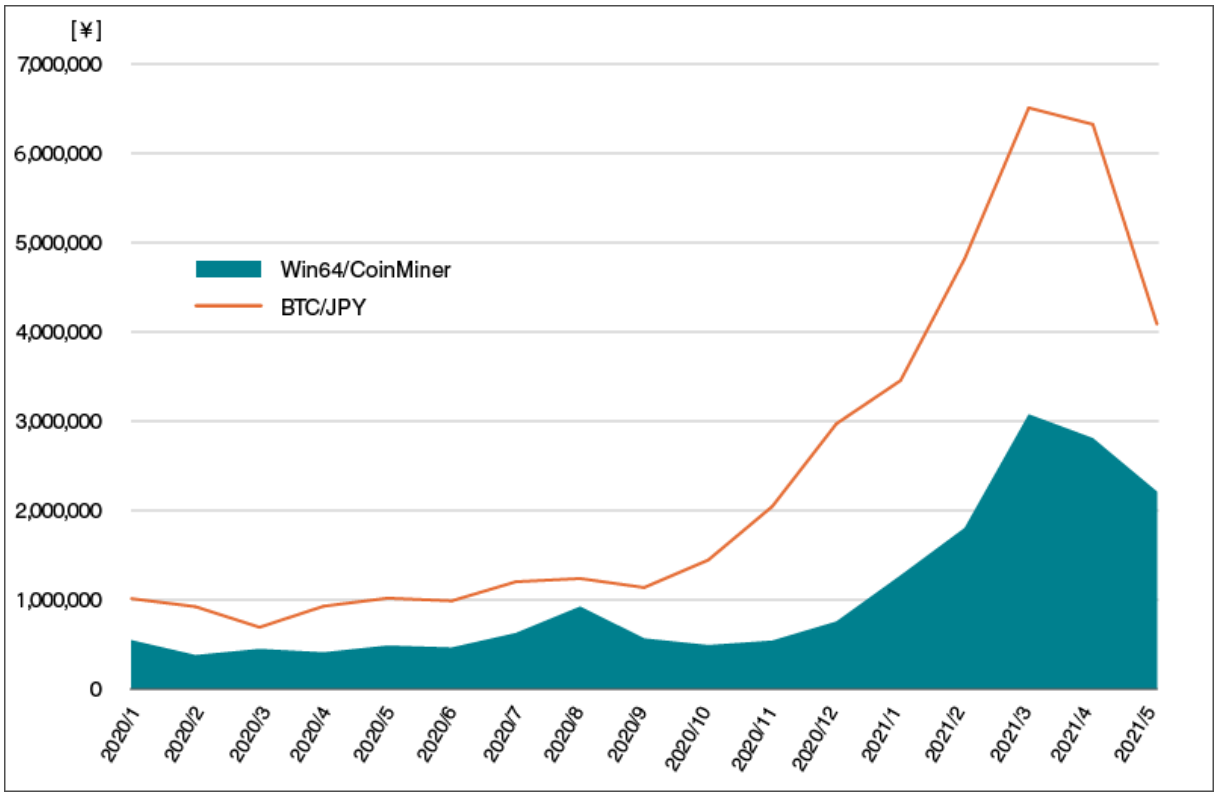
Win64/CoinMiner の検出数は、2018 年の BTC 価格下落を機に減少傾向が続いていました。




**Win64/CoinMiner の国内における検出状況と BTC 価格/日本円[*3]の推移**
**（2015 年 1 月～2021 年 5 月）**

*3 BTC 価格/日本円の価格は CryptoCompare のデータを使用

しかし 2021 年暗号資産の価格の高騰に伴い、Win64/CoinMiner の検出数が再度増加しています。




**Win64/CoinMiner の国内における検出状況と BTC 価格/日本円[*3]の推移**
**（2020 年 1 月～2021 年 5 月）**

Win64/CoinMiner には、トロイの木馬として検出される場合と PUA（望ましくない可能性があるアプリケーション）として検出される場合があります。このため検出数の増加には、クリプトジャッキングの増加だけでなく、自身でマイニングを行う人の増加、収益を得るための手段としてマイニングを利用するアプリケーションの増加なども考えられます。

自身でマイニングを行う場合などでは問題ありませんが、クリプトジャッキングが行われている場合は検出されることが望ましいと考えられます。クリプトジャッキングでは、正規のマイニングソフトが悪用されていることも多くあります。このため PUA の検出を無効にしていた場合は、気付かないうちにマイニングが行われている可能性もあります。ESET などのセキュリティソフトでは、PUA の検出を有効化し検査することで、秘密裏に実行されている CoinMiner を発見できる可能性があります。今一度、確認することを推奨します。

ご紹介したように、Win64/CoinMiner の検出が増加しています。
公開サーバに侵入されマイニングマルウェアが設置される事例や 4 月のマルウェアレポートでも紹介した QNAP 社製の NAS の脆弱性を悪用し、マイニングを行う事例も報告されています。今後、暗号資産の価格がどのようになるかは不明ですが、マイニングの収益が期待されるような場合は、CoinMiner の検出数も多くなると考えられます。

---

■常日頃からリスク軽減するための対策について
各記事でご案内しているようなリスク軽減の対策をご案内いたします。
下記の対策を実施してください。

**1. ESET 製品の検出エンジン（ウイルス定義データベース）を最新にアップデートする**
ESET 製品では、次々と発生する新たなマルウェアなどに対して逐次対応しております。
最新の脅威に対応できるよう、検出エンジン（ウイルス定義データベース）を最新にアップデートしてください。

**2. OS のアップデートを行い、セキュリティパッチを適用する**
マルウェアの多くは、OS に含まれる「脆弱性」を利用してコンピューターに感染します。
「Windows Update」などの OS のアップデートを行い、脆弱性を解消してください。

**3. ソフトウェアのアップデートを行い、セキュリティパッチを適用する**
マルウェアの多くが狙う「脆弱性」は、Java、Adobe Flash Player、Adobe Reader などのアプリケーションにも含まれています。
各種アプリのアップデートを行い、脆弱性を解消してください。

**4. データのバックアップを行っておく**
万が一マルウェアに感染した場合、コンピューターの初期化（リカバリー）などが必要になることがあります。
念のため、データのバックアップを行っておいてください。

**5. 脅威が存在することを知る**
「知らない人」よりも「知っている人」の方がマルウェアに感染するリスクは低いと考えられます。マルウェアという脅威に触れてしまう前に「疑う」ことができるからです。
弊社を始め、各企業・団体からセキュリティに関する情報が発信されています。このような情報に目を向け、「あらかじめ脅威を知っておく」ことも重要です。

※ESET は、ESET, spol. s r.o.の登録商標です。Windows は、米国 Microsoft Corporation の、米国、日本およびその他の国における登録商標または商標です。

---

引用・出典元

■マルウェア情報局『2021 年 4 月 マルウェアレポート』
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware2104.html

■JPCERT/CC Eyes | JPCERT コーディネーションセンター公式ブログ『仮想通貨マイニングツールの設置を狙った攻撃』
https://blogs.jpcert.or.jp/ja/2021/05/xmrig.html

Canon

キヤノンマーケティングジャパン株式会社