Press Release

平成30年11月29日

ウェブルート
「最も危険なマルウェア2018」を発表
～今年大きな被害をもたらしている攻撃性のある不正コードやマルウェアとは ～

セキュリティソフトをグローバルで展開し、セキュリティ業界をリードするウェブルート株式会社（本社：東京都港区、 代表取締役社長：伊藤 誉三、以下 ウェブルート）は、企業団体・一般ユーザーのいずれにも有害となるマルウェアや攻撃性のある不正コードを紹介する最新版レポート 「最も危険なマルウェア2018」を発表いたします。脅威は常に進化しており、サイバーセキュリティ関連の教育と防御ツールの必要性はかつてないほどに高まっています。

2018年の最も危険なマルウェアと不正コード

ボットネット & バンキング型トロイの木馬

ボットネットとバンキング型トロイの木馬は2018年に最もよく見られたマルウェアです。中でもEmotetは過去最も流行した悪質なマルウェアであったといえます。

３大ボットネット & バンキング型トロイの木馬型マルウェア：

1. **Emotet**

今年最悪といわれるバンキング型トロイの木馬をもたらすボットネットです。スパムボットネット内にゾンビの数を増やし、クレデンシャル情報の収集を集中して行っています。さらに、ハッカーたちはEmotetで被害者のルーターを自分たちのコマンドのプロキシノードに変えてインフラを支配する、世界的なプラグ アンド プレー (UPnP) モジュールを構築したようです。

2. **Trickbot**

Emotetと類似する攻撃プランを持つマルウェアです。毎日追加されるモジュールが内包されており、ランサムウェアを投下したケースも見られました。

3. **Zeus Panda**

Trickbotに類似した機能をもつマルウェアです。マクロ化したワードドキュメントやエクスプロイト キットを使用するなどユニークな方法で拡散され、遠隔モニタリングやマネージメントサービスさえも損傷しました。

クリプトマイニング & クリプトジャッキング

今年は犯罪者たちの攻撃手段が、クリプトマイニングやクリプトジャッキングへ急激に移行しており、より速く低リスクな方法で仮想通貨が奪われようとしています。被害者のいない犯罪とも言われていますが、ビジネス・一般ユーザーのどちらにも多大な影響を及ぼす可能性があります。

３大クリプトマイニング & クリプトジャッキング型マルウェア：

1. **GhostMiner**

流布方法が不明なクリプトマイニング。Oracle WebLogic 上でエクスプロイトを介して流布されることが一番多かったマルウェアです。

2. **WannaMine**

仮想通貨をターゲットにした新しいマルウェア。Windows management instrumentation (WMI)テクニックでは見つけにくく、除去しづらいという性質を持ち、非常にしつこくたちが悪いと言われています。

3. **Coinhive**

登場当初は害がないように思われていたマルウェアですが、ウェブサイトを攻撃するハッカーたちの定番ツールとなりつつあります。通常のウェブサイトのオーナーでさえ、来訪者にどんな影響を与えるか知らないままCoinhiveを使っているケースが多く存在しています。

Press Release

ランサムウェア

クリプトマイニングの急速な増加により2018年の脅威リストのトップには及びませんでした。しかしサイバー犯罪者にとって、よりターゲットを絞ったビジネスモデルとなりつつあります。セキュリティ保護がされていない遠隔デスクトップ制御（RDP）接続が組織の弱点になり、ランサムウェアの攻撃を受けやすくなっています。

3大ランサムウェア：

1. Crysis/Dharma
「RDP不正侵害」と同調するランサムウェア。進化し続けており、ランサムウェア アズ ア サービス(RaaS)でトップの座を維持し、RDPベクターだけを標的にしています。システム管理者は、週明けの始業時に自社マシンが暗号化されているのに愕然とするが、原因追及ができません。

2. GandCrab
悪意のあるスパム攻撃、エクスプロイト キット、RDPで流布されるたちの悪いRaaS。GandCrabは「.bit」というICANN（Internet Corporation for Assigned Names and Numbers、アイキャン）が承認していないTLD（トップレベルドメイン）を使用し秘密性を高めているというユニークな点が見られました。

3. SamSam
元はJBossのエクスプロイトを介して流布し、RDPに姿を変えて、都市全体（あるいは少なくともその一部)を侵略しています。

総評

ウェブルート サイバー脅威シニアリサーチ アナリスト
タイラー・モフィット（Tyler Moffitt）

今年、サイバー攻撃は以前にも増して急速に変化することで、これまでの防御を回避し、企業にも一般ユーザーにも大きな被害を与えています。保護されていないRDPなどのセキュリティの穴をかいくぐる、フィッシングやエクスプロイトなど実証済みの手法を使う、CPUパワーを利用した仮想通貨の盗難するなど、サイバー犯罪者たちは悪質な方法でシステムの脆弱性を利用しています。企業も個人も常に最新情報を入手し、サイバー衛生の改善・向上に注力し、これらの攻撃を防がなければなりません。

ウェブルートについて

ウェブルートは Smarter Cybersecurity®のソリューションプロバイダです。インテリジェントなエンドポイント保護および脅威インテリジェンス・サービスによって「モノのインターネット」（IoT=Internet of Things／モノのインターネット）のセキュリティを実現。
クラウドベースで予測型の総合脅威インテリジェンス・プラットフォームを活用することによって、コンピュータ、タブレット、スマートフォン、そしてあらゆるデバイスをマルウェアや他のサイバー攻撃から保護しています。高い評価を受けているSecureAnywhere®インテリジェント・エンドポイント保護とBrightCloud®脅威インテリジェンス・サービスは、世界中で数千万台以上のエンドユーザ、企業、エンタープライズ機器を守っています。ウェブルートのテクノロジーは、業界トップリーダーであるCisco、F5 Networks、HP、Microsoft、Palo Alto Networks、RSA、Arubaなどのソリューションに採用され、高い信頼を得ています。本社を米国コロラド州に置き、北米、欧州、アジア環太平洋、日本でビジネス展開しています。
Smarter Cybersecurity®の詳細はウェブサイトhttp://www.webroot.com/jp/ja/ をご参照ください。
公式Facebookページ： https://www.facebook.com/WebrootJapan/
公式Twitterアカウント：https://twitter.com/Webroot_JP

＜本件に関するお問合せ先＞
ウェブルート株式会社
マーケティング部　東田
Email: thigashida@webroot.com

＜報道関係者からのお問合せ先＞
ウェブルート広報事務局（カーツメディアワークス内）
担当：田口・佐藤・ジェレミー
Email: info@kartz.co.jp　Tel: 03-6427-1627