CLOUD . MOBILE . THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

報道関係者各位

2018 年 9 月 25 日
チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

チェック・ポイント、『サイバー攻撃トレンド：2018 年上半期レポート』を発表
世界規模で見たマイニング・マルウェアの影響が 2018 年上半期に 2 倍に拡大、
クラウド・インフラストラクチャがハッカーの標的になるケースが増加

世界の 42%の組織が仮想通貨採掘攻撃の被害を受けており、
クラウド・インフラストラクチャを狙った第 5 世代の高度なサイバー攻撃*も増加傾向を示す

米カルフォルニア州 サン カルロス - 2018 年 7 月 12 日
ゲートウェイからエンドポイントまで、包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ(Check Point® Software Technologies Ltd. NASDAQ: CHKP）は、**『サイバー攻撃トレンド：2018 年上半期レポート』**を発表しました。このレポートでは、サイバー犯罪者が不正な収益源の開拓を目的に、マイニング・マルウェアを使った攻撃を積極的に仕掛けている傾向が示されています。その一方で、クラウド・インフラストラクチャが標的となる攻撃も増加しています。

2018 年の上半期にマイニング・マルウェアの被害を受けた組織は全体の 42%で、2017 年下半期の 20.5%から倍増しています。マイニング・マルウェアを使うサイバー犯罪者は、被害者の CPU や GPU の処理能力を不正利用し、手持ちのリソースも活用して仮想通貨を採掘できます。エンドユーザの CPU の処理能力は最大で 65%も消費される可能性があります。2018 年上半期に悪用されたマルウェアの上位 3 種は、いずれもマイニング・マルウェアでした。

チェック・ポイントは最近の傾向として、クラウド・インフラストラクチャへの攻撃が増えている事実も確認しています。組織の IT 資産やデータがクラウドへ移行している現状を受け、サイバー犯罪者の意識もクラウドへ向かっているようです。膨大な処理能力の不正利用や利益の増加が狙いです。

『サイバー攻撃トレンド：2018 年上半期レポート』では、マイニング・マルウェア、ランサムウェア、バンキング、モバイルといった主要なマルウェア・カテゴリごとに、サイバー脅威の現状が詳細に解説されています。そうした調査結果は 2018 年上半期の ThreatCloud 脅威インテリジェンスから得られたデータに基づいており、組織を狙うサイバー犯罪者の主要な戦略に焦点を当てた内容になっています。

チェック・ポイントの脅威情報グループ・マネージャを務めるマヤ・ホロウィッツ（Maya Horowitz）は、「今年上半期のサイバー犯罪は 2017 年末に見られた傾向が続いており、犯罪者は水面下で動作するマイニング・マルウェアを活用して収益を最大化させています。また、クラウドのインフラストラクチャやマルチプラットフォーム環境を狙った高度な攻撃の出現も確認されています。そうした展開が速く大規模で複数の経路を利用する第 5 世代の攻撃の発生頻度が高まっていることもあり、組織ではネットワークやデータへの被害を防ぐことができる多層防御のサイバー・セキュリティ戦略を導入する必要があります」と述べています。

*第 5 世代のサイバー攻撃：
第 5 世代のサイバー攻撃とは、モバイル環境、クラウド環境、およびオンプレミスのネットワークを対象に、大規模かつ高速に展開される攻撃を指します。この高度な攻撃は、組織全体をカバーするセキュリティ・アーキテクチャが考慮されていない場合、多大な影響に発展することが考えられます。

2018 年上半期の主なマルウェアの傾向

2018 年上半期に確認された主なマルウェアの傾向は次のとおりです。

● **マイニング・マルウェアが進化：** 2018 年のマイニング・マルウェアは機能が大幅に向上しており、より巧妙で悪質なものへと進化しています。利用できるコンピューティング・リソースの割合を増やし、収益性を高めるという明確な目標のもと、その達成に利用できそうなあらゆるものを標的にするようになっています。また、最近は感染率を高めるために、有名な脆弱性の悪用のほか、サンドボックスやセキュリティ製品の回避という点でも大きな進化を遂げています。

● **攻撃者がクラウドに進出：** 2018 年の上半期だけ見ても、クラウドのストレージ・サービスを対象とした攻撃に、多くの高度なテクニックやツールが使われています。データの外部送信や情報の不正な開示など、クラウドに対する攻撃のいくつかは、公開されているソースコード・リポジトリでログイン情報が参照可能な状態になっていたり、強度の低いパスワードが使われていたりなど、セキュリティ対策の不備に起因しています。マイニング・マルウェアもクラウド・インフラストラクチャを標的にしています。その処理能力を利用して攻撃者により多くの利益をもたらすことが目的です。

● **マルチプラットフォーム対応の攻撃が増加：** 2017 年末までは、マルチプラットフォーム対応のマルウェアはまれな存在でした。しかしオンラインのコンシューマー・デバイスが増加し、Windows 以外のオペレーティング・システムのシェアも拡大していることから、マルウェアのマルチプラットフォーム化が進んでいる状況です。攻撃者は感染した各種のプラットフォームを制御するため、さまざまなテクニックを取り入れています。

● **モバイル・マルウェアがサプライチェーン経由で拡散：** 2018 年上半期には、不正な URL からダウンロードした覚えがないモバイル・マルウェアが別の経路からデバイスに侵入し、気付いたときにはインストール済みだったというケースが確認されています。また、正常なアプリのようにアプリ・ストアで配信されているマルウェアも増加傾向にあります。バンキング型トロイの木馬、アドウェア、高度なリモート・アクセス・ツール（RAT）などがこれに該当します。

2018 年上半期のマイニング・マルウェア・ランキング

1 **Coinhive（30%）：** ユーザが Web ページにアクセスしたときに、同意を得ることなく仮想通貨 Monero の採掘を行うマイニング・マルウェアです。Coinhive は 2017 年 9 月に登場したばかりですが、すでに世界の 12%の組織が影響を受けています。

2 **Cryptoloot（23%）**：ユーザが Web ページにアクセスしたときに、同意を得ることなく仮想通貨 Monero を採掘する JavaScript ベースのマイニング・マルウェアです。

3 **JSEcoin（17%）**：ユーザが Web ページにアクセスしたときに、同意を得ることなく仮想通貨 Monero を採掘する Web ベースのマイニング・マルウェアです。

2018 年上半期のランサムウェア・ランキング

1 **Locky（40%）**：主にスパム・メール経由で拡散するランサムウェアです。スパム・メールには、Word

ファイルや Zip ファイルに偽装したダウンローダが添付されており、このダウンローダによって、ユーザのファイルを暗号化するマルウェアがインストールされます。

2 **WannaCry（35%）：** 2017 年 5 月の大規模攻撃で感染を広げたランサムウェアです。Windows SMB の脆弱性を悪用するエクスプロイト EternalBlue を利用して、ネットワーク内やネットワーク間で拡散します。

3 **Globeimposter（8%）：** スパム・メールや不正なインターネット広告、エクスプロイト・キット経由で拡散するランサムウェアです。暗号化を実行する際、各ファイルに.crypt という拡張子を追加します。

2018 年上半期のモバイル・マルウェア・ランキング

1 **Triada（51%）：** Android デバイスに感染するモジュール型のバックドアです。ダウンロードしたマルウェアにスーパーユーザの権限を付与することで、そのマルウェアのシステム・プロセスへの組み込みを可能にします。ブラウザに読み込まれる URL を偽装する動作も確認されています。

2 **Lokibot（19%）：** Android スマートフォンを標的とするモバイル・バンキング型トロイの木馬です。ユーザが管理者権限の付与を拒否すると、ランサムウェアへと変貌します。

3 **Hidad（10%）：** 正規のアプリを再パッケージしてサードパーティのアプリ・ストアで公開する Android マルウェアです。OS に組み込まれた重要なセキュリティ情報にアクセスできるため、機密性の高いユーザ・データを窃取されるおそれがあります。

2018 年上半期のバンキング・マルウェア・ランキング

1 **Ramnit（29%）：** 銀行の認証情報や FTP のパスワード、セッション cookie、個人情報を窃取するバンキング型トロイの木馬です。

2 **Dorkbot（22%）：** ユーザが銀行の Web サイトにログインしようとしたタイミングで活動を開始し、Web インジェクションによりユーザの認証情報を窃取するバンキング型トロイの木馬です。

3 **Zeus（14%）：** Windows プラットフォームに感染するトロイの木馬です。多くの場合「Man-in-the-Browser」攻撃やキー入力内容の記録、フォーム入力内容の取得により、金融機関情報を盗み出す目的で使用されます。

ThreatCloud インテリジェンスのベースとなるのは、サイバー犯罪阻止を目的とした業界最大規模の協調型ネットワークです。世界規模の脅威センサー・ネットワークから収集された脅威情報や攻撃動向を配信する ThreatCloud のデータベースには、ボット発見を目的として分析された 2 億 5,000 万件以上のアドレスや、1,100 万件以上のマルウェア・シグネチャ、550 万件以上の不正サイトの情報が登録されています。ThreatCloud は、1 日あたり数百万種類のマルウェアを観察、認識しています。

レポート全文（日本語）は、こちらからダウンロードいただけます。
https://www.checkpoint.co.jp/resources/cyber-attack-2018-mid-year-report/

本リリースは、米国時間 7 月 12 日に配信されたものの抄訳です。

英語のリリース全文はこちらをご確認ください。
https://www.checkpoint.com/press/2018/check-point-research-global-impact-cryptominers-doubles-h1-2018-hackers-increasingly-target-cloud-infrastructures/

日本語のリリース全文はこちらをご確認ください。
https://www.checkpoint.co.jp/press/2018/pressrelease_20180925.html

■チェック･ポイントについて

チェック・ポイント・ソフトウェア・テクノロジーズ（ www.checkpoint.com ）は、世界各国の政府機関や企業など、あらゆる組織に対応するサイバー・セキュリティ・ソリューションを提供する大手プロバイダーです。業界随一の検出率を誇る先進のソリューションにより、お客様のネットワークを、マルウェアやランサムウェアなどの多岐にわたる第５世代のサイバー攻撃から保護します。企業のクラウドやネットワークのほかモバイル・デバイスに保存されている情報を、今日の第５世代のサイバー攻撃を含めてあらゆる脅威から保護するため、第５世代の脅威に対応するマルチレベルのセキュリティ・アーキテクチャを備え、直感的で操作性に優れた総合的かつ一元的なセキュリティ管理システムを展開しています。世界の 10 万以上の組織・企業がチェック・ポイントのセキュリティ製品を利用しています。

《本件に関するお問い合わせ先》

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社　広報代行　共同ピーアール株式会社

担当　マーケティング　横山
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: marketing_jp@checkpoint.com

担当　上瀧・花岡
Tel: 03-3571-5238 / Fax: 03-3571-5380
Email: checkpoint-pr@kyodo-pr.co.jp

