

2016年11月18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

企業を狙った未知のマルウェアが前年比9倍に増加**従業員による新種マルウェアのダウンロードは4秒に1回発生****ー チェック・ポイント・セキュリティ・レポート 2016年版を発表 ー**

調査対象企業の80%でフィッシング攻撃が増え影響が拡大、
主な感染経路はメールとソーシャル・エンジニアリング

ゲートウェイからエンドポイントまでの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・テクノロジーズ株式会社（本社：東京都、代表取締役社長：ピーター・ハレット、以下 チェック・ポイント）は本日、「チェック・ポイント・セキュリティ・レポート 2016年版」を発表しました。これにあわせ、チェック・ポイント主催「エンドポイントにおける脆弱性攻撃: SANS 2016 脅威環境調査 (Exploits at the Endpoint: SANS 2016 Threat Landscape Study)」(2016年8月現在)を公表しました。

今回で4回目の調査報告となる「チェック・ポイント・セキュリティ・レポート 2016年版」は、世界中で稼働する25,000を超えるチェック・ポイントのセキュリティ・ゲートウェイの活動を分析し、企業が直面している既知と未知のマルウェア、攻撃傾向、企業内におけるモバイル機器の使用増の影響を報告しています。また、実際にセキュリティ侵害が起きた事例において、組織が受けた影響と、復旧にかかる費用以外のコストに関して具体的なデータを開示しています。進化を続けるサイバー脅威に対し企業が対策を強化するなか、ITリーダーが解決すべき重要課題を明らかにするとともに、鍵となるいくつかの提言を行っています。

また、「エンドポイントにおける脆弱性攻撃: SANS 2016 脅威環境調査 (Exploits at the Endpoint: SANS 2016 Threat Landscape Study)」は、チェック・ポイントとセキュリティ教育研究グループ SANS Institute の研究者らが協力し、世界で活動する300人以上のIT・セキュリティ専門家を対象に調査を行いました。調査内容は、実運用環境において組織が直面する脅威、脅威がインシデントへと発展する原因と経緯、最も影響の大きかった脅威の種類、企業が脅威から身を守る上で最大の課題を明らかにしています。

本日発表のレポートおよび調査はいずれも、ネットワークからエンドポイントまでを網羅した脅威の全容を俯瞰しています。概要は以下のとおりです。

- **未知のマルウェアの急増と進化**：企業を標的とした未知のマルウェアのダウンロード件数は、前年の1時間あたり106件から970件あまりへと、9倍以上に急増していることが判明しました。その主な原因は従業員による、4秒に1回のペースでダウンロードされる新たな未知のマルウェアです。毎月、全体で

1,200 万近くの新種のマルウェアが発見されています。過去 2 年間で新たに発見されたマルウェアの数は、それ以前の 29 年間の合計をすでに上回っています。

- **モバイル・デバイス普及に伴うセキュリティ対策の遅れ**：企業の従業員が デジタル・メディアに費やす時間の 60%はスマートフォンとタブレットの使用によるものであることが判明しています。モバイル・デバイスは、利便性があり生産性を上げる一方で、アクセス面では弊害をもたらします。従業員の 5 人に 1 人が、モバイルマルウェア、または悪意のある Wi-Fi ネットワークを通じて、意図せずネットワーク侵害を引き起こす可能性があります。
- **脅威の大半はエンドポイントが起点**：調査対象企業においてエンドポイントが、侵害の原因となることが最も多く、サイバー防御のうえで最も重要な要素と捉えられます。実際にあった攻撃の多数が、メールを攻撃手段に悪用したものでした。

チェック・ポイントのプレジデントを務めるアムノン・バーレブ (Amnon Bar-Lev) は次のように述べています。「毎分数十億という膨大な数の接続が生まれるなか、世界はかつてないほどグローバルにリンクしています。クラウド、モビリティ、IoT といったイノベーションが、テクノロジーの導入、消費、セキュリティ確保のあり方を変えています。エコシステムに侵入するマルウェアの数は増える一方であり、従来のセキュリティ技術では防ぎきれなくなっています。こうした状況においてリーダー企業であり続けるためには、制御が及ばない見えない未知の脅威の一步先を行き、攻撃を未然に防ぐことが必要です」

上記のレポートおよび調査のいずれも、現在および将来にわたる複雑な IT セキュリティ要件に応えるには、最高レベルのアーキテクチャ導入が最優先と結論づけています。また、高度な脅威対策、モバイル・デバイスの保護、ネットワークのセグメント化が不可欠であることが、共通の見解として確認されました。「チェック・ポイント・セキュリティ・レポート 2016 年版」の全文は <http://www.checkpoint.co.jp/securityreport/>、「エンドポイントにおける脆弱性攻撃: SANS 2016 脅威環境調査 (Exploits at the Endpoint: SANS 2016 Threat Landscape Survey)」は <https://www.checkpoint.co.jp/webinars/sans-2016-threat-landscape-study/> でご覧いただけます。

SANS Institute について

SANS Institute は、1989 年に設立された共同研究教育機関です。サイバー・セキュリティをテーマに 200 を超えるトレーニング・イベントを開催し、ライブ中継およびオンラインを含む 50 コース以上を提供しています。SANS Institute が設立した関連会社の GIAC は、30 以上のハンズオン演習項目を通じてセキュリティ・プロフェッショナルの技術やスキルを検証し、情報セキュリティ認定を付与しています。SANS Institute が設立した独立子会社の SANS Technology Institute は、米国認可の教育機関として、サイバー・セキュリティの修士号を授与しています。 (www.SANS.org)

■チェック・ポイントについて ONE STEP AHEAD

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、あらゆる規模の組織に対応する世界トップクラスのセキュリティ・リーディング・カンパニーです。業界随一の検出率を誇る先進のセキュリティ対策により、お客様のネットワークをマルウェアなどの多岐にわたるサイバー攻撃から保護します。大規模ネットワークからモバイル・デバイスまでを保護する包括的なセキュリティ・アーキテクチャに加え、直感的で使いやすい総合的なセキュリティ管理ソリューションを提供しています。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。

チェック・ポイント・ソフトウェア・テクノロジーズの全額出資日本法人、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 (<http://www.checkpoint.co.jp/>) は、1997 年 10 月 1 日設立、東京都新宿区に拠点を置いています。

©2016 Check Point Software Technologies Ltd. All rights reserved

####

《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

担当 マーケティング 石黒・溝口

Tel: 03-5367-2500 / Fax: 03-5367-2501

Email: info_jp@checkpoint.com

広報代行 共同ピーアール株式会社

担当 中村・小林・上瀧

Tel: 03- 3571 – 5238 / Fax: 03- 3571-5380

Email: checkpoint-pr@kyodo-pr.co.jp