2017 年 6 月 30 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、世界規模で急速に感染を広げる Petya ランサムウェアの追跡調査を実施

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、6 月 27 日に発生した世界規模のサイバー攻撃に関する追跡調査の分析結果を発表しました。ウクライナの中央銀行や政府機関、民間企業を中心に世界中で被害が出ています。

今回の攻撃は、個別のファイルではなく MBR(マスタ・ブート・レコード)を暗号化するランサムウェア、Petya の亜種が配布された可能性があります。攻撃の詳細原因はまだ特定されていませんが、多くの研究者は、ウクライナの会計ソフトウェアプロバイダである M.E.Doc が侵害され、そのシステムを悪用しソフトウェア更新メカニズムを介して攻撃を配布していたと指摘しています。なお、現時点で M.E.Doc は否定しています。

マルウェアがネットワークに侵入すると、ネットワーク全体を感染させるためにマルウェアが横方向に展開します。SMB の脆弱性やアクティブなセッションを悪用し、クレデンシャル（認証情報）の窃取および別のマシンへファイルを配布する手段としてファイル共有などワーム的な活動を特徴としています。

チェック・ポイントでは、今回のマルウェアについて次の 2 点を確認しています。1 つは、CVE-2017-0147 の脆弱性を悪用するエクスプロイト EternalBlue（WannaCry が使用したのと同じエクスプロイト）を利用して、ネットワーク内での感染拡大を試みる点。もう 1 つは、マルウェアのバイナリにリソースとして埋め込まれた別の実行可能ファイルを使用し、認証情報を窃取する点です。後者の実行ファイルは DLL で、%TEMP% ディレクトリにドロップされ、rundll で実行されます。このツール自体は Mimikatz と呼ばれる既知のオープンソース・ユーティリティと同様に、マシンのメモリからハッシュ、パスワード、その他のセキュリティ関連の有益な情報を窃取する機能を備えています。

盗取されたクレデンシャルは、Petya の DLL をターゲット・ホストにファイル転送する際に使用されます。このペイロードは、SMB プロトコルの TRANS2 SESSION_SETUP リクエスト・パケットで、4096k のチャンクとして送信されます（リクエストごとに 1 チャンク）。ペイロードは、「24db007a」を鍵にして XOR エンコードされています。ターゲット・ホストに転送されたファイルは、Windows の正規ツール群 Sysinternals に含まれる PsExec を使用してリモート実行されます（PsExec も、元のマルウェア・バイナリに埋め込まれています）。

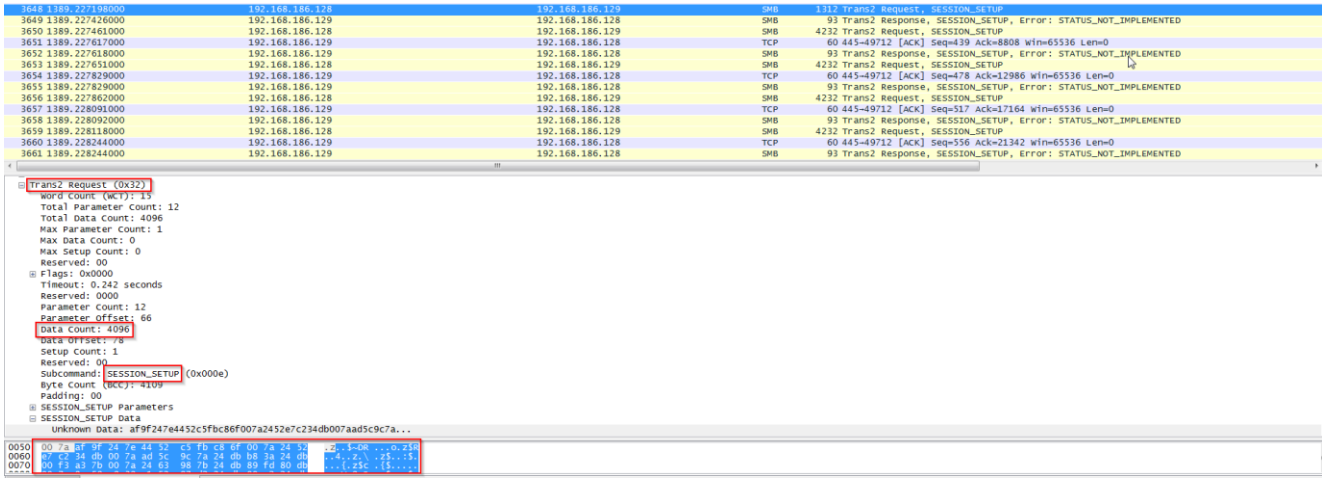


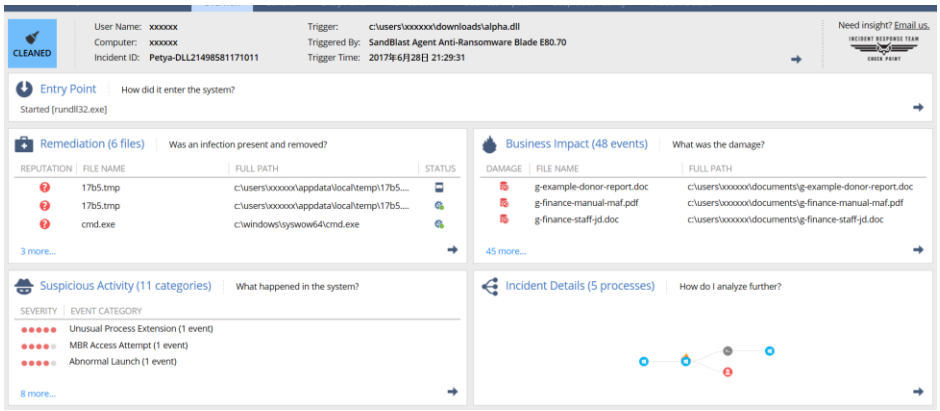
図 1: Petya が転送するペイロード・チャンクの例

チェック・ポイントは、継続調査しブログを更新していく予定です。Sand Blast Agent をはじめとする以下のソリューションは、Petya と Loki Bot に対応しています。

- Sandblast： http://www.checkpoint.co.jp/products/sandblast-network-security/
- Sandblast Agent： https://www.checkpoint.co.jp/products/endpoint-sandblast-agent/
- Anti-Bot Software Blade： https://www.checkpoint.co.jp/products/anti-bot-software-blade/
- IPS： https://www.checkpoint.co.jp/products/ips-software-blade/

＞ランサムウェア攻撃を防御するための詳細情報 （製品評価のお問合せ）

SandBlast Agent のフォレンジック機能による Petya 分析結果については、こちらをご覧ください。



■チェック･ポイントについて　　WELCOME TO THE FUTURE OF CYBER SECURITY

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。

####

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

