※2016 年 8 月 16 日に米国で発表されたプレスリリースの抄訳です。

2016 年 8 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、世界最大規模のランサムウェア・キャンペーン「Cerber」の複雑な Bitcoin フローを解明

身代金を払うことなく、独自の復号化ツールを開発するための研究者向けの情報も提供

カリフォルニア州サンカルロス発 - 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 Check Point® Software Technologies Ltd.（NASDAQ: CHKP、インターナショナル本社：イスラエル、会長兼 CEO：ギル・シュエッド）は本日、世界最大規模の「Ransomware-as-a-Service（サービスとしてのランサムウェア）」である「Cerber」について、新たな調査レポートを発表しました。レポートでは、この複雑なランサムウェア・キャンペーンの舞台裏を深く掘り下げ、拡大する Ransomware-as-a-Service 業界の実態を明らかにしています。さらに、暗号化されたファイルを、高額な身代金を支払わずに復号化するための研究者向けの情報を紹介しています。

60 ページに及ぶこのレポートでは、チェック・ポイントの脅威情報およびリサーチ・チームと、チェック・ポイントのリサーチ・パートナーである IntSights のサイバー情報チームが、Cerber の技術的な特徴と活動実態について詳しく分析しています。主な内容は次のとおりです。

- **数あるランサムウェアの中でも Cerber の感染率は突出して高く、利益率も高い**
  展開中の攻撃キャンペーンは世界で 160 件以上に及び、年間収益は合計 230 万ドルに上ると推計されます。1 日平均 8 件のキャンペーンが新たに開始されており、2016 年 7 月だけでも、201 の国及び地域で約 15 万件の感染被害が確認されています。
- **Cerber のアフィリエイトは、マネー・ロンダリングの実行役となっている**
  Cerber は、追跡を免れるために仮想通貨の Bitcoin を使用しています。身代金の受け取りには、感染被害者ごとに個別のウォレットを用意しており、身代金（通常は 1 Bitcoin = 現在のレートで 590 ドル）が支払われた場合に限り、被害者に復号鍵を提供します。身代金は、数万個のウォレットを経由するミキシング・サービス（Bitcoin の匿名性を高めるためのサービス）を悪用して Cerber 開発者の元に送られるため、ウォレットを辿って開発者を特定することはほぼ不可能です。最終的に身代金が開発者の元に届いた後、アフィリエイトに成功報酬が支払われます。
- **Cerber は、ハッカー予備軍にサイバー犯罪者への道を開いた**
  Cerber の登場によって、技術的な専門知識のない個人や組織でも、収益性の高いランサムウェア攻撃に参加し、独立したキャンペーンを展開できるようになりました。指令（C&C）サーバや 12 の言語に対応した使いやすいコントロール・パネルが提供されるため、攻撃のためのインフラストラクチャを自分で用意する必要がありません。

チェック・ポイントと IntSights は、2016 年 6 月から、Cerber の複雑なシステムの全体像とグローバルな流通インフラストラクチャを把握するための調査を進めてきました。その結果、被害者の実際のウォレットを再作成し、身代金の支払いや取引を確認して、Cerber が得た収益とそのフローの両方を追跡することに成功しています。またこの調査結果を元に、身代金を支払わずに感染システムを復旧する復号化ツールの開発に道筋を付けることができました。

チェック・ポイントの研究開発担当グループ・マネージャを務めるマヤ・ホロウィッツ（Maya Horowitz）は、「今回の調査活動により、拡大を続ける Ransomware-as-a-Service 業界の動向とグローバルな感染状況という貴重な知見を得ることに成功しました。高度なサイバー攻撃はもはや、国家レベルの攻撃グループや、独自の攻撃ツールを開発できるだけの技術力を持ったグループに限らず、ほとんど誰もが手軽に実行できる行為となっています。この

ような状況下で急激に拡大する Ransomware-as-a-Service 業界に警戒し、適切な対策を講じる必要があります」と述べています。

今回の調査結果の詳細については、レポート『CerberRing: An In-Depth Exposé on Cerber Ransomware-as-a-Service（英文）』（http://www.checkpoint.co.jp/resources/cerberring/）をご覧ください。

チェック・ポイントの脅威情報およびリサーチ・チームは、サイバー攻撃、脆弱性、セキュリティ侵害についての調査を随時実施し、お客様を保護するためのセキュリティ機能を開発しています。チェック・ポイントによるその他の調査結果の詳細については、http://www.checkpoint.com/threatcloud-central/ をご覧ください。

■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　石黒・溝口
Tel: 03-5367-2500 / Fax: 03-5367-2501
Email: info_jp@checkpoint.com

広報代行　株式会社プラップジャパン
担当　高橋・南宮
Tel: 03-4580-9109 / Fax: 03-4580-9135
Email: CheckPoint_pr@ml.prap.co.jp