Bromium 社共同創業者 CTO, Simon Crosby 氏の 2016 年 6 月 21 日ブログ記事より

A Hat Tip to a White Hat (あるホワイトハッカーへの表敬)
https://blogs.bromium.com/2016/06/21/a-hat-tip-to-a-white-hat/

我々は、セキュリティ・ベンダーには責任があると考えることが重要であると思います。支持できる設計と厳しい評価を支援して、マーケティングメッセージは捨ててください。 Bromium はエンドポイントを設計力でセキュアにするため、仮想化技術に裏付けられた技法を使います。次世代ウイルス対策(AV)のような「かもしれない」ツールは、未知の攻撃がやむ事を望むことができるだけでしょう - しかし、99%のマルウェアは 1 分以内に新しい、未知の形へ変形してしまいます。

これをハイライトするために、我々はロンドンでの InfoSec の参加者に、自前のマルウェアを持ってくるよう呼びかけました。これらが Bromium を回避したならば、彼らは 10,000 ポンドを勝ち取る事になります。二日間の間で、我々は 4,800 以上のサイトを閲覧し、1,500 以上のドキュメントと添付ファイルを開けました。 我々は、脆弱性パッチ未適用の Bromium をインストールしたエンドポイントを 189 の攻撃（そのうち 10 は VirusTotal では認識されていませんでした。）から保護しました。 ある AV ベンダーの研究者は、検知を回避してしまうカスタムメイドのプログラムさえダウンロードしましたが、我々を破ることはできませんでした。

他のベンダーは、未知のマルウェアに対して彼らの製品がどのように動作するのかわからないので、公の場でこうした開示はしないでしょう。

Bromium は信頼に基づいた賭けを要求しません。 弊社の製品は、エンドポイントの攻撃経路を減らす事で、攻撃者側のコストを増加させています。 しかし、我々が良い仕事をしたとあなたがどのように、確信することができますか？ あなたが我々を信頼する必要はないと思います。 毎年、我々は権威がある研究組織によってソースコード・レビューとペン・テストを依頼し、顧客自身も同様のことを行う事を推奨しています。 これまでに実質的な問題は少しも出てきませんでした。

今年は、一歩先に動き、内々に数名の White Hats(*いわゆるホワイトハッカー)の方々と仕事をし始めました。そして、Google の Tavis Ormandy 氏（@taviso）が、MircoVM による隔離を逃れさせる 2 つのバグを認識したと主張した際に我々は驚きましたが、私は内心では、むしろうれしかったです。 Tavis は、最も尊敬される倫理的なペン・テスターの 1 人 - そして、我々は彼に弊社製品を渡すことさえしていませんでした！ 彼は調査結果を喜んで共有してくれ、そして、我々は彼と解決策を協議することに忙しい週を過ごしました。彼は丁寧で、かつ有能 - そして、常に公平で、データに基づいていました。この経験は、White Hats コミュニティとの開かれた関わりも使命の一つとの再確認に繋がりました。
我々は、顧客がパッチを適用するための 30 日の期間のあとで、彼の発見の詳細を明らかにします。一方で、我々が共有できる幾つかの興味深い事実をお伝えします。

- Tavis は、機能の評価用に顧客に送られ、誤ってアップロードされた Chrome の古いバージョンをサポートする機能に関するバグを vSentry 3.1 の初期ビルドで見つけました。バグの連鎖で武装する熟練した攻撃者は、ホストの Chrome ブラウザー上でのコード実行を成し遂げるために、我々のバグを利用することができる状態でした。
- 幸いにも、通常の Bromium のアップデート配信において、Google が新しい版を公開したすぐ後、Bromium Enterprise Controller が”App Packs”を通じて Chrome 保護のアップデートを配信し始めます。 例えば最近の Bromium Chrome App Packs は我々のバグを悪用するのに必要になる既知の問題を修復します。
- 同様の課題が IE 向けの保護の中にも存在しましたが、再び幸いにも、通常の Bromium のアップデートの配信の中で、このバグによる問題を軽減します。
- 我々は InfoSec で使ったマシンが適用済のセキュリティ・ポリシーと設定のため、破られることはないことを確認し、それは現実の運用では一般的な設定になっています。

Bromium にはバグ報告報奨プログラムがまだありません。また、コンテストでの我々の条件は InfoSec で使われた製品バージョンとポリシーの指定がありました。しかし、我々は Tavis に弊社製品に対する重要な貢献から恩恵を受けています。 Bromium は彼に 10,000 ポンドを支払う事にしました。そして、彼はそれをアムネスティ・インターナショナルに寄付すると述べています。それとは別に、彼の本物のプロフェッショナリズムを認識し、また、彼のものすごい「White Hat」の証拠として、私は個人的に Bromium 賞を Tavis の名誉のため、以下に示す先週の為替レートでの約£10,000 相当を寄付に加算する事にしました。我々はきちんとバグ報告報奨プログラムを実行する最良の方法を調査中で、その準備が出来るまでは更なる懸賞金はお払い致しません。