NEWS LETTER

2018 年 6 月 20 日

Tenable Network Security Japan K.K

データサイエンスチーム「Tenable Research」

業界初※、攻撃側の先行者利益を定量化したレポートを公表

企業の様々な情報資産の脆弱性を手間なく自動で可視化、改善するソリューションを提供する『Tenable Network Security』（以下：テナブル、所在地：メリーランド州コロンビア、代表：Amit Yoran （アミット・ヨーラン）が結成したデータサイエンスチーム「Tenable Research」は、『攻撃側の先行者利益を定量化』したレポートを発表しました。本調査は、2017 年の 3 ヶ月の間に行われた 200,000 件の脆弱性評価スキャンに基づいて、上位 50 の脆弱性を選択し、分析したものです。攻撃側のリードを定量化することは、どの程度の遅れをとっており、そのギャップを埋めるために何をすべきかを判断するための助けになります。※Renaud Deraison が寄稿しているブログの「類をみない調査」から引用しています。

・米国で発表されたプレスリリースの抄訳版：

https://www.tenable.com/press-releases/cybercriminals-have-seven-day-advantage-to-weaponize-vulnerabilities-according-to-new

・日本語版レポートのダウンロードはこちら：https://jp.tenable.com/cyber-exposure/attackers-advantage#download

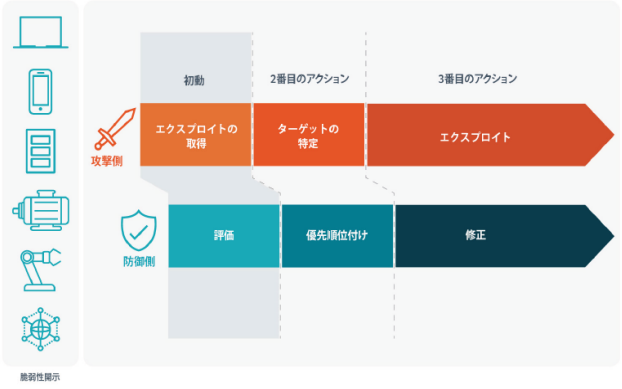
・日本語版解説ページ：https://jp.tenable.com/blog/eliminating-the-attackers-advantage-why-original-research-matters

本レポートでは、特定の脆弱性に関してエクスプロイトが一般に公開された時点（エクスプロイト可用性時間=Time to Exploit Availability：TtE）と、セキュリティチームがシステムで最初に評価する時点（評価時間=Time to Assess：TtA）の差を日数で測定しています。この差分が、防御側と攻撃側双方の初動の差を表します。負の差分は、攻撃側に、防御側が脆弱性を認識・評価するまでに脆弱性をエクスプロイトできる期間があったことを示しています。

■常に先行している攻撃側

◇攻撃側は防御側よりも約 7 日間先行

本調査で、攻撃側は、防御側が脆弱性を初めて評価するまでの差分の中央値（※）は、約 7 日間と判明しました。この間、攻撃側が脆弱性をエクスプロイトする期間が生じていたこととなります。（※）TtE の中央値が 5.5 日であるのに対し、TtA の中央値は 12.8 日と判明し、その中央値の差分は-7.3 日となります。



脆弱性の開示後における攻撃側と防御側の初動の概要

◇攻撃側が有利となったケースは 76%

今回分析した脆弱性のうち、76%が負の差分となりました。このことからも、攻撃側は多くの場合、先行者利益を得ていることが分かります。

◇34%が、脆弱性開示と同日にエクスプロイトが利用可能に

今回分析した脆弱性のうち 34%は、脆弱性が開示されたその日のうちに、エクスプロイトも公開され利用可能となっていました。

◇マルウェアによって広く攻撃の対象にされていた脆弱性は 24%

今回分析した上位 50 の脆弱性のうち 24%が、マルウェア、ランサムウェア、またはエクスプロイトキットによって、際限なく頻繁に出回っているものです。そのうちのさらに 14%が、メディアで取り上げられるほど深刻なものです。サンプルセットに含まれている脆弱性は、Disdain および Terror エクスプロイトキット、Cerber および StorageCrypt ランサムウェア、さらには Black Oasis などの APT グループが FinSpy 監視ソフトウェアをインストールする際にターゲットとされています。

この度の調査では、脆弱性の開示とエクスプロイト可用性までの平均時間を基にすると、TtA の 60%を改善しても、正の差分となる脆弱性は 50%に留まり、TtA を 75%改善して初めて半数以上となる 66%が正の差分となります。

また、スキャン動作に関する分析では、2 日以下の頻度で継続的な脆弱性評価を行っている組織はわずか 25%程度であることも分かりました。

・日本語版レポートのダウンロードはこちら：https://jp.tenable.com/cyber-exposure/attackers-advantage#download

・日本語版解説ページ：https://jp.tenable.com/blog/eliminating-the-attackers-advantage-why-original-research-matters

【米国テナブル社プロフィール】

Tenable Network Security は、総合的なセキュリティのソリューションにより、将来のビジネスニーズに合わせてそのテクノロジーを変革し、企業組織の情報保護に向けた有効的な対策を提供しています。Tenable はセキュリティの脆弱部分を解消し、脅威に優先順位を付け、エクスポージャーと損失を削減します。世界中に 100 万人以上のユーザーと 2 万社を超える法人顧客をもつ Tenable は、裏付けのあるセキュリティ・イノベーションによって企業から信頼を得ています。

【米国テナブル社企業概要】

商号： Tenable Network Security
代表： Amit Yoran アミット・ヨーラン
住所： 7021 Columbia、
Gateway Drive Suite 500 Columbia,
MD 21046

【テナブル社企業概要】

商号：Tenable Network Security Japan K.K.
住所：東京都千代田区丸の内 2-3-2
郵船ビルディング 1 階