リークコード的な何か

リークした攻撃コードから垣間見る超大国？の攻撃力

2017/08/02　@濱せっく

0xH@jic

本日お話したいこと

- WikiLeaksが定期的にリークしている CIA Vault7の情報
- Shadow Brokers
- 気になった何か

WikiLeaks Vault7

- https://wikileaks.org/vault7/
- https://www.reuters.com/article/us-cia-wikileaks-leak-idUSKBN16F2CZ

WASHINGTON (Reuters) - U.S. intelligence and law enforcement officials told Reuters on Wednesday they have been aware of a CIA security breach, which led to the latest Wikileaks dump since late last year.

The two officials said they were focusing on contractors as the likeliest source of the leak.

Reporting by John Walcott; Writing by Yara Bayoumy

WikiLeaks Vault7

Imperial (2017年7月27日)

- *Achilles*
  - 任意のMac OSXのインストーラ (.dmg)をスクリプトで書き換えて、追加でファイルをインストール
  - 類似マルウェア *Proton*
- *Aeris*
  - 複数のLinuxディストリビューションで動作するCで記述された遠隔操作ツール
- *SeaPea*
  - Mac OSX 10.6/10.7 Rootkit
  - ファイル、ディレクトリ、プロセス、通信の秘匿
  - ツールの起動

UCL / Raytheon (2017年7月19日)

- Raytheon社-CIAとの契約
  - Raytheon Blackbird Technologies社が、CIAの開発部門に対して、観測されているマルウェアについての見解(CIAが攻撃ツールとすべきか)を提供
- 2014年11月21日 – 2015年9月11日の期間、Raytheon社がCIAに提供したマルウェアの調査と攻撃アイデアの報告書

Highrise (2017年7月13日)

- Android 4.0 – 4.3で動作するアプリケーション (手動でインストールが必要)
- SMSメッセンジャーのプロキシ (盗聴的な)
- ユーザーに知られることなく、メッセージ(コマンド)を受信し、情報をコントローラに送信

BothanSpy (2017年7月6日)

- Windows上のSSHクライアントXshellを標的
- アクティブなSSHセッションから以下を盗む
  - SSHクリデンシャル
  - SSH秘密鍵のファイル名
  - 公開鍵のパスワード

OutlawCountry (2017年6月30日)

- Linuxを標的とした通信盗聴ソフトウェア
- Linuxカーネルで動作し、隠し*netfilter*テーブルを作成 (隠しテーブルの知識が必要)
- *netfilter*テーブルに作成したルールは、既存ルールに優先され、管理者からは見えない
- 全ての外部通信をCIA管理サーバーへ送信

Elsa (2017年6月28日)

- Windows端末で有効になっているWiFiを使って、位置情報だけを収集するマルウェア
- 端末はアクセスポイントに接続している必要はない
- 有効になっているWiFiを利用し、近くのAPのBSSID、MACアドレス、強度、時刻だけを定期的に収集・保存

Brutal Kangaroo (2017年6月22日)

- Windowsのクローズネットワークから情報を収集するマルウェアフレームワーク
- 挿入するだけでマルウェアがインストールされるUSBで感染
- 感染端末からの情報収集とC2のセットアップ、感染拡大

Shadow Brokers

- https://twitter.com/shadowbrokerss
- https://github.com/misterch0c/shadowbroker
- 2017年4月のEquation Groupのエクスプロイトリーク以降、パブリックなリークはないが、継続して活動中

気になった何か

- 米政府Intelligenceオフィサーと法律家は、リークを特に否定していない、どころか、気づいているよ的な発言 (政府契約機関が想定されると)
- CIAは、契約企業からマルウェア解析の報告を受けているのではなく、その技法を検証すべきかどうかの報告を受けている
- 実証コードのないリークもあるが、別の攻撃者にアイデアを提供、敵対者には警戒を与える
- CISCOルータの脆弱性コード、ETERNALBLUEは、非常に影響の大きいものであったが、まだまだ氷山の一角 (ではと思われる)