資料 3−5

第３回 Connected Car 研究会

サイバーセキュリティ目線のConnected Car

LAC
ともに、イキル

2017年3月9日 株式会社ラック
CTO/CISO 西本 逸郎

株式会社ラック

セキュリティでお客様の成長に貢献。　安心・安全な情報社会を実現します。

お客様とともに　社会とともに 安心とともに

商　号	**株式会社ラック** LAC:　LAC Co., Ltd.
設　立	2007年10月1日（ 旧ラック1986年9月）
資本金	10億円
代　表	代表取締役社長　髙梨　輝彦
売上高	連結 369億円（ 2016年3月期）
決算期	3月末日
認定資格	経済産業省情報セキュリティ 監査企業登録 情報セキュリティ マネジメント システム (ISO/IEC 27001)認証取得(JSOC) プライバシーマーク 認定取得

- ✓ http://www.lac.co.jp/
- ✓ sales@lac.co.jp
- ✓ Twitter @lac_security
- ✓ YouTube laccotv
- ✓ Facebook　Little.eArth.Corp or 株式会社ラック

※ ＪＳＯＣ（下記参照）、サイバー救急センター、サイバー・グリッド・ジャパン、が特徴です。

本社
〒102-0093　東京都千代田区平河町 2-16-1
平河町森タワー
03-6757-0111(代表)
03-6757-0113 (営業窓口)

福岡オフィス
〒812-0011　福岡市博多区博多駅前3-9-1
大賀博多駅前ビル5F

名古屋オフィス
〒460-0002 愛知県名古屋市中区丸の内3-20-17 KDX桜通ビル16F

■ JSOC (Japan Security Operation Center)

JSOCは、ラックが運営する情報セキュリティに関するオペレーションセンターです。24時間365日運営。高度な分析官とインシデント対応技術者を配置しています。2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業などに、高品質なサービスを提供しています。

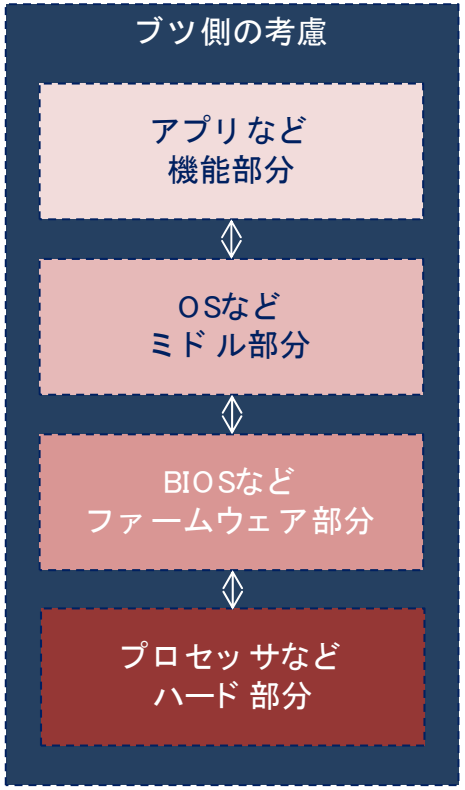
1. おさらい

1）誰がどんな目的で？

脅威の整理

① 人間の意志ではない脅威
　故障、災害や事故などに起因
② 故意の脅威
　（1）外部の攻撃者（直接、成り済まし、間接）
　（2）ＩｏＴ提供者
　（3）ＩｏＴ利用者
　（4）利用部品など
　　→ 設計・テスト・維持・廃棄
③ ビジネス上の脅威
　収益構造、社会問題、風評被害
　悪貨(サイバーデブリ)は良貨を駆逐

代表的な目的
- A. 金銭
- B. 愉快犯
- C. 主義主張や怨恨
- D. 権益拡大



2）攻撃手段？

① ネット から 直接侵入
→ バール壊して, 鍵を 入手など

② 間接的に侵入
（1）メールやWeb閲覧
（2）USBなど
→ Autorun, 他デバイスなりすまし
（3）保守
→ 機器交換, ファームやソフト 更新
（4）製品に組み込み

③ 侵入せずに妨害
→ DDoSなど

どんな方法で？
A. 遠隔操作(Backdoor)
B. 自動動作
時限動作やイベント 待ち

どこで？
a. ブツ側
b. サーバー(クラウド)側
管理者を含む
c. 利用者側

3）現状でもみられるサイバーデブリ

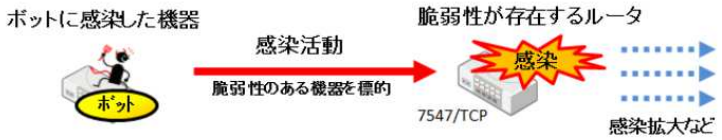
平成28年12月21日
警察庁

海外製ルータの脆弱性を標的としたアクセスの急増等について

平成28年11月期における、インターネット定点観測システムへのアクセス情報等を観測・分析した結果から、ネットワークセキュリティの維持・向上に資する情報を掲載しています。

概要

- 警察庁では、11月26日からCWMP（※1）に使用される宛先ポート7547/TCPに対するアクセスの急増を観測しました。観測したアクセスは、海外製ルータの脆弱性（※2）を悪用して不正なプログラムの実行を試みるものであり、ボットの感染活動と考えられます。



不正プログラム感染活動のイメージ

- ルータ等の機器がボットに感染すると、ボットに感染したルータは、DoS攻撃の踏み台となったり、感染拡大を狙ってさらなる探索を行ったりする可能性があります。ルータ等の利用者はボットへの感染を防止するため、使用している機器の脆弱性の有無等を確認し、ファームウェアのアップデートや適切なアクセス制限を行うなどの対策を実施してください。

@police

平成28年12月21日

海外製ルータの脆弱性を標的としたアクセスの急増等について
（平成28年11月期）

- 海外製ルータの脆弱性を標的としたアクセスの急増
- 宛先ポート27015/UDPに対するアクセスの増加
- SSDPに使用される宛先ポート1900/UDPに対するアクセスの急増
- ntpdの脆弱性（CVE-2016-7434）を標的としたアクセスの観測

宛先ポート7547/TCP及び5555/TCPに対するアクセスにおいては、多数のIPアドレスからのアクセスを確認しています（図4）。

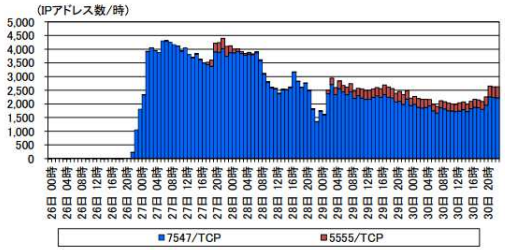


図4 宛先ポート7547/TCP及び5555/TCPに対する発信元IPアドレス数の推移
（H28.11.26～H28.11.30）

1 海外製ルータの脆弱性を標的としたアクセスの急増

インターネット定点観測システムでは、11月26日22時頃から宛先ポート7547/TCPに対するアクセスの急増を観測しました（図1）。

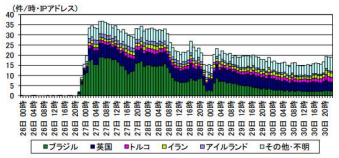
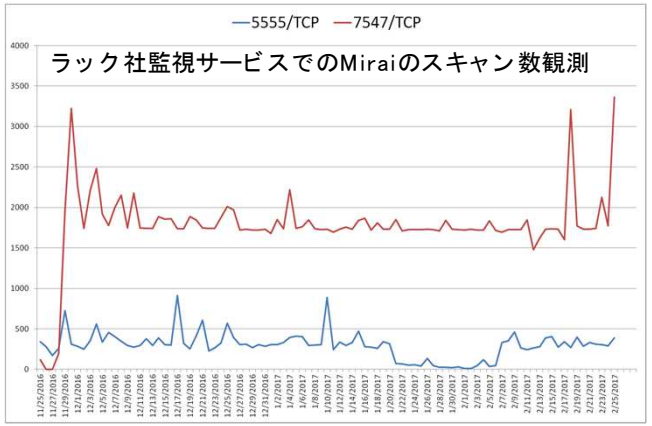
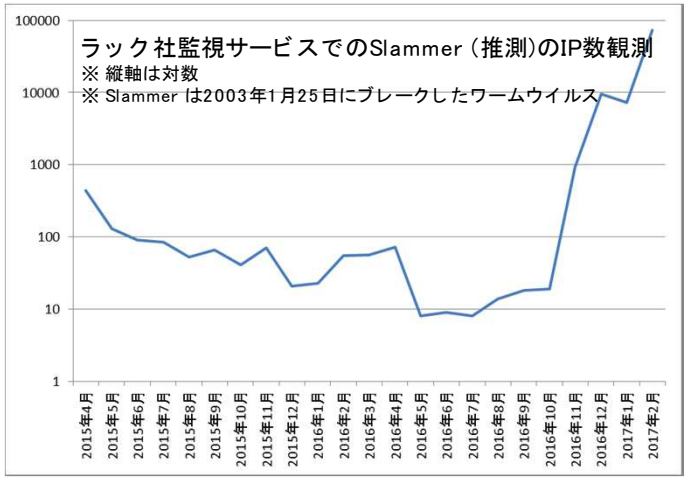


図1 宛先ポート7547/TCPに対するアクセス件数の発信元国・地域別推移
（H28.11.26～H28.11.30）

https://www.npa.go.jp/cyberpolice/topics/?seq=19747





４）悪貨(サイバーデブリ)が生み出される理由

① 開発者側 (ブツ/サーバー)

（1）技術がない
（2）気が付かない
（3）端から やる気がない
（4）EOL
（5）倒産・ 事業撤退
（6）事業売却
（7）そもそも犯罪目的

② 利用者側(ブツ/端末など)

（1）気が付かない
（2）設定しない
（3）故意に
（4）そもそも犯罪目的

2. 課題

１）セキュリティへの考慮事項

① 脆弱性管理と真正性の管理
　汎用化，高機能化部品を含め

② 機能の実装だけでも済まない
　セーフティとセキュリティの実装

③「悪意」への考慮が鍵
　どのレベルまでの考慮が必要か？

④ ゲートウェイ(ファイアウォール)
　外向き制御(出口対策)が必須

⑤ 悪貨を駆逐する策

悪貨の駆逐に関して(初回の資料から)

① 関連サービスの充実 → 良貨で席捲
② 車検,取締り　　→ 悪貨の駆逐

悪貨の駆逐には「暴く力」が欠かせない。そのため,特に車検や取締りの変革は大きな影響を与えるのでは？
① Car関連コード(プログラム)
　→ Connected車検・取締りなど
② 関係者サイド
　→ 配布コードや体制など

ご参考 弊社の取り組みや参考情報

① 弊社の取り組み
（1）ホワイトハッカーを活かした攻撃者目線でのペネトレ
（2）JSOCを活かした車載ネットワークの監視・分析研究
② 考慮すべき社会動向（攻撃者の動向）
テクノロジーやサービスの高度化は攻撃者も活用する。
― AWS→計算コスト減
― SDR→無線ハックコスト減
― フェムトセル
→モバイル回線ハックコスト減
― CAN・LINなどのマイコン
→車載ネットワークへの攻撃テストコスト減
③ 今後の課題
（1）最低限，自動車，部品，インフラ，セキュリティ関係者が協調する必要あり
― 意外と，ECUサプライヤーは要かも
― 攻撃者の動向やプロファイリング力（暴く力）
（2）全てをオープンにする必要はないが，ブラックボックスだから安全ということにはならない。
― 少なくとも中の人には弱いところが丸分かり

【参考情報】

① ジープチェロキーのリモートハック
Kaspersky.lab: Black Hat USA 2015： ジープのハッキングの全容が明らかに
https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/

② コルベッティ＋保険会社ドングルのリモートハック
WIRED: Hackers Cut a Corvette's Brakes Via a Common Car Gadget
https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

③ 日産LeafがVINだけでリモートから状態が分かって一部コントロールもできる。
ThreatPost: Nissan Car Hack Allowed Remote Access
https://threatpost.com/nissan-car-hack-allowed-remote-access/116469/

④ トヨタはコネクテッドカーで車両状態のログを収集する
http://techon.nikkeibp.co.jp/atcl/mag/15/400480/111800046/?rt=nocnt

ご清聴, ありがとうございました。

LAC ともに、イキル

株式会社ラック
http://www.lac.co.jp/
sales@lac.co.jp