監視されるインターネットにどう向きあうか

IIJ Technical WEEK 2013

株式会社インターネットイニシアティブ

セキュリティ情報統括室

根岸 征史

IIJ-SECT
IIJ Group Security Coordination Team

経緯

- 2013年6月から Guardianや WaPoなど複数のメディアを通じて、NSAの監視活動に関する Top Secret資料の内容が多数公開
  → 公開されたのは全体のごく一部で、現在も継続中
- Edward Snowden氏(29) による内部リーク
  → 米国のパスポート失効、スパイ活動法違反で起訴
  → 香港を経由して現在はロシアに一時的に亡命中
- FISAなどの法律にもとづく合法的な監視活動

NSAとは

- 米国の Intelligence Community (IC) を構成する 16 の組織の一つで、主に Signals Intelligence (SIGINT) を担当する情報機関
- 本部はメリーランド州フォート・ミード陸軍基地内
- 人員 約3万人、年間予算およそ1兆円 ($10.8B)
- Five Eyesとの協力 (UKUSA Agreement)

リーク内容 (1)

インターネットおよび電話回線の包括的な監視

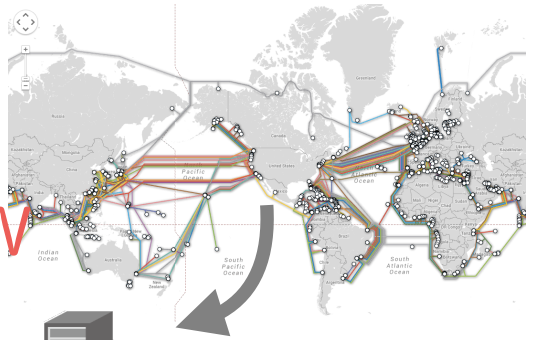
・米国に陸揚げされる海底ケーブルの通信傍受　SSO
・米国外での通信傍受 (Five Eyesなどの協力)　GAO
・インターネットサービス各社からのデータ提供
(Microsoft, Yahoo!, Google, Facebook, Apple等)
・メタデータおよびコンテンツの収集、解析
→ Contact Chaining、リアルタイム検索

Microsoft, Yahoo!
Google, Facebook, etc.

PRISM

FBI

BLARNEY
FAIRVIEW
OAKSTER
STORMBREW
WINDSTOP

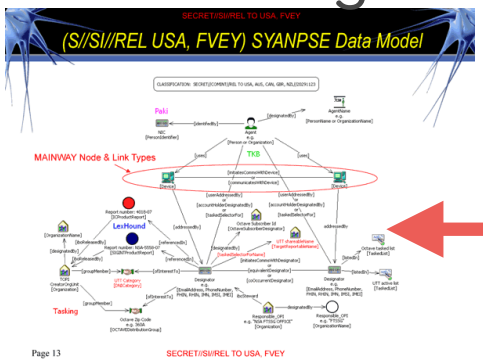


XKEYSCORE

query

query

Contact
Chaining



	DNI	DNR
Metadata	MARINA	MAINWAY
Contents	PINWALE	NUCLEON

NSA自身の発表によると、

「インターネットでは 1日に約1,826PBのデータがやりとりされている。NSAはこのうち約1.6% (約29PB)のデータを監視している。しかしこのうち 0.025%だけが実際に調査対象となっている。つまり全体からみると100万分の4程度にすぎない。」

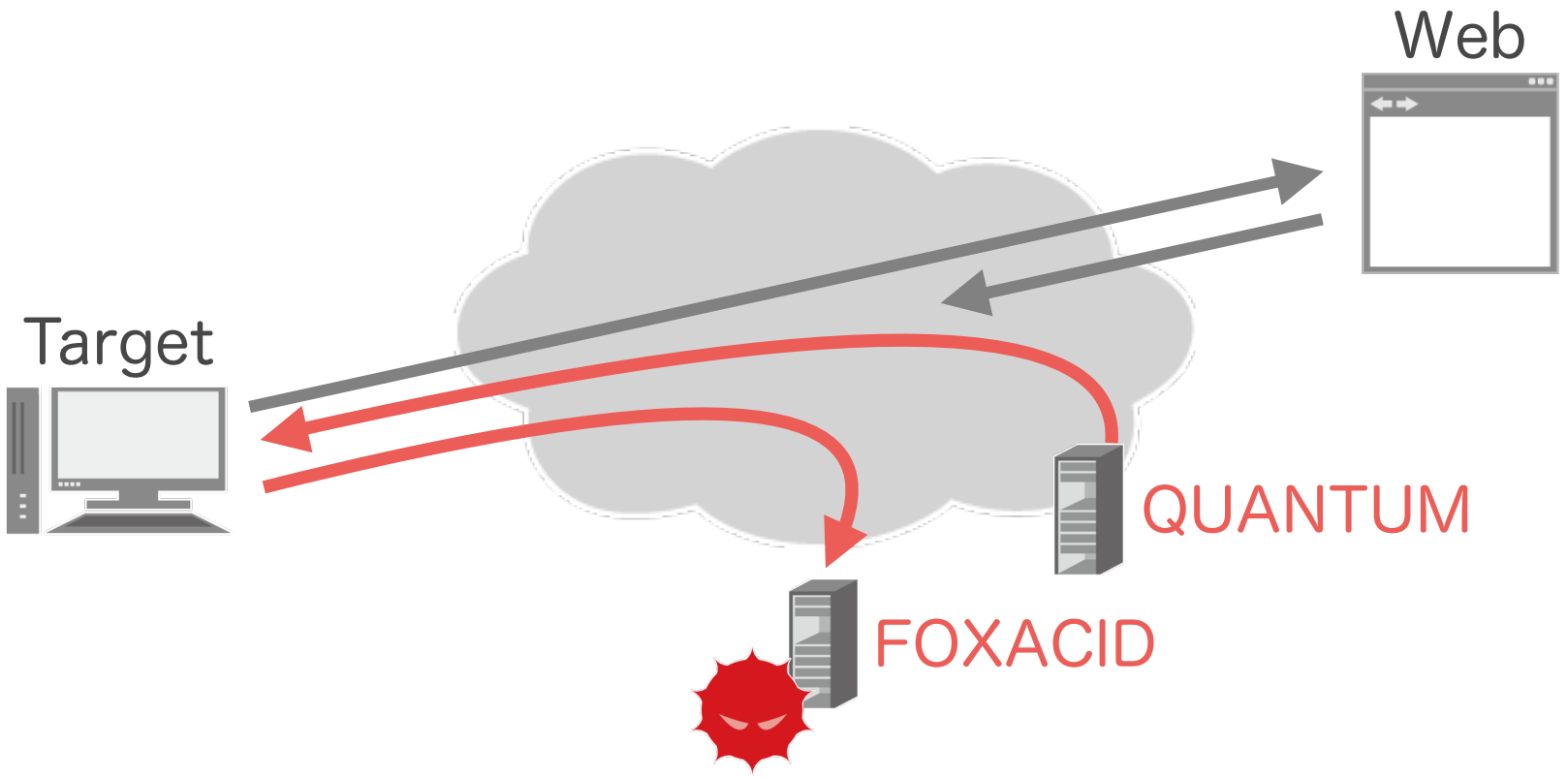
(参考)
Googleの1日のデータ処理量は 2007年に 20PB、2009年に 24PB。AT&Tのバックボーンの 1日のIPトラフィックは 2010年に 19PB。
WSJの報道によると、NSAは米インターネットトラフィックのおよそ75%にアクセスする能力がある?

リーク内容 (2)

米国外における諜報活動、サイバー攻撃

- 各国政府首脳や大使館の電話盗聴、通信傍受　SCS
- 通信会社や石油会社への侵入
- サイバー攻撃作戦の実施 (OCEO)　TAO
- Torユーザへのマルウェア感染

暗号解読、暗号標準策定への関与、バックドア



1. ターゲットが Webにアクセスする
2. 正規のサーバよりも先に QUANTUMが応答する
3. FOXACIDにアクセスを誘導する
4. ブラウザの脆弱性を突いてマルウェアに感染させる

(参考) http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

様々な反応と影響 (1)

米政府、議会、司法

・米議会による調査、追求、法改正
・米政府による積極的な情報公開 (IC on the Record)
・FISCによる情報開示
・NISTによる標準策定の再レビュー

市民

・監視への抗議運動、EFF/ACLUによる訴訟
・プライバシー確保への自衛

様々な反応と影響 (2)

事業者

・インターネットサービス各社による透明性レポート
・メールサービスの停止 (Lavabit, Silent Circle)
・暗号強化、Forward Secrecyへの対応

海外

・国産メールサービスの開発
・自国のセキュリティおよびネット規制の強化
・各国政府から米政府への抗議、説明要求

論点、課題

・テロとの闘い? 合法的な活動?
・目的外利用、暴走
・監視活動の成果、透明性、制限
・他国での諜報活動なんて当たり前?
・自由 vs. セキュリティ vs. プライバシー
・インターネットガバナンス問題

ユーザの自衛策

ユーザとしての態度

・無関心
・やましいことがなければ気にする必要ない?
・やましいことがなくても、公権力が暴走したり
　間違いを犯す可能性はある
→ 自分のプライバシーは自分で守る必要がある

技術的には適切な暗号化がほぼ唯一の対抗策

ネットワークは VPNで暗号化
Webアクセスは HTTPSで暗号化
メールは OpenPGPで暗号化
メッセージは OTRで暗号化
ディスクは LUKS, TrueCryptで暗号化
Torで通信経路を匿名化
パスワード管理は厳重に (パスワード管理ソフト、2要素認証/2段階認証)

まとめ

- ユーザとして
- 事業者として
- XXXXとして

参考資料

NSA files decoded: Edward Snowden's surveillance revelations explained
http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded (Guardian紙によるまとめ)
NSA Spying | Electronic Frontier Foundation
https://www.eff.org/nsa-spying (EFFによるまとめ)
The SSD Project | EFF Surveillance Self-Defense Project
https://ssd.eff.org/
IC ON THE RECORD http://icontherecord.tumblr.com/ (米政府公式サイト)
IC OFF THE RECORD http://nsa.gov1.info/dni/ (パロディサイト)
U.S. Foreign Intelligence Surveillance Court Public Filings
http://www.uscourts.gov/uscourts/courts/fisc/index.html
Stop Watching Us https://optin.stopwatching.us/
Opt out of global data surveillance programs like PRISM, XKeyscore, and Tempora - PRISM Break https://prism-break.org/
Off-the-Record Messaging https://otr.cypherpunks.ca/
Lavabit 事件とその余波、そして Forward Secrecy
http://negi.hatenablog.com/entry/2013/11/05/093606
OTRでオフレコチャット！
http://negi.hatenablog.com/entry/2013/11/09/103401