人質にされるデータたち

トレンドマイクロ株式会社　六宮 智悟
テクニカルサポート本部　リージョナルトレンドラボ・グループ
リサーチ & ソリューション ラボ　担当課長代理
兼 TrendMicro Security Incident Response Team 技術統括責任者

本日、お話する内容

1. 身近な脅威動向とご相談の傾向
2. ランサムウェア（Ransomware）
3. 安全で楽しいデジタルライフのために
4. まとめ

と、先にまとめを。

- デジタルライフは便利で楽しいものである。
- 一方で、悪意ある者にとっても便利なものであるのも事実。
- 脅威は身近に、より巧妙に。
- 残念ながら、対策に銀の弾丸（万能薬）はない。

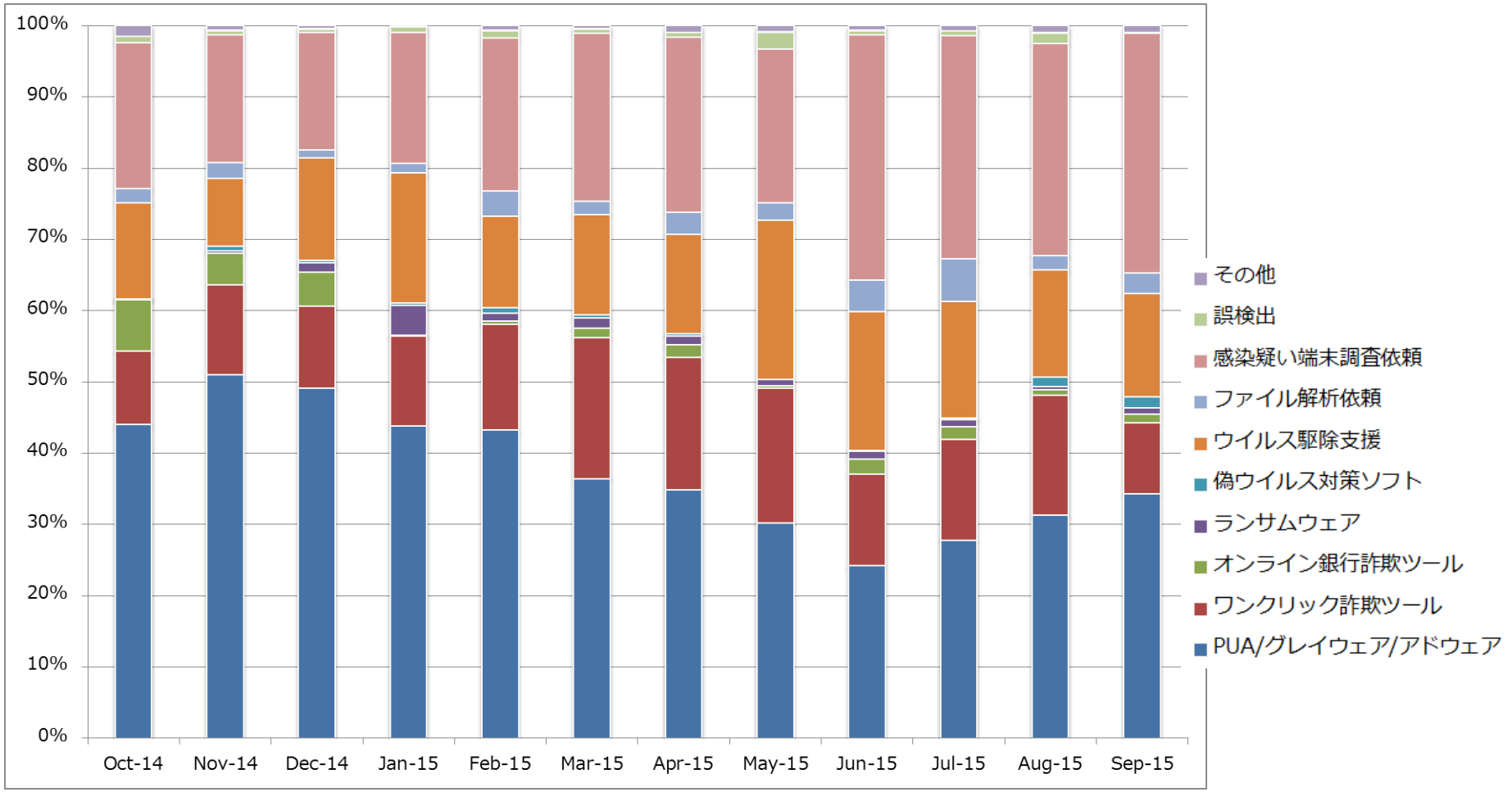
- だがしかし！ひとりひとりが知恵を身につけられたのなら、デジタルライフはもっと楽しいものになる。

01. 身近な脅威動向とご相談の傾向

不正プログラム関連

お問い合わせの傾向

- 実数はお伝えできませんが、総数はやや減少傾向



お問い合わせからみる
脅威の流行

- 気付いたらポップアップメッセージが…。
  - PUA (Potentially Unwanted Application)
  - グレイウェア, アドウェア
- ご入会ありがとうございます。
  - ワンクリック詐欺ツール
- 気付いたときには預金残高が 0 円に。
  - オンライン銀行詐欺ツール（バンキング・トロジャン）
- お客様のファイルは暗号化されました。
  - ランサムウェア（身代金型不正プログラム）
- お使いのパソコンがウイルスに感染しています。
  - 偽ウイルス対策ソフト（Fake AV）

身近な脅威で狙われるのは
やっぱり…

手段は様々、狙いはひとつ
金銭

× ~~サイバー犯罪者がサイバー犯罪をやっている~~

○「犯罪者が効率を上げるためにサイバー犯罪をやっている」と思ってもらうほうが自然

ちなみにご相談と言えば…

- パソコンが起動しない！
  - 思い出の写真がぁぁぁ
- 間違えてフォルダごと消しちゃった！
  - 思い出の写真がぁぁぁ
- スマホ水没させちゃった！
  - 思い出の写真がぁぁぁ

ご近所、近親者からの相談第一位

IT企業にお勤めなんですよね、助けてください…

と、前フリが終わったので

02. ランサムウェア

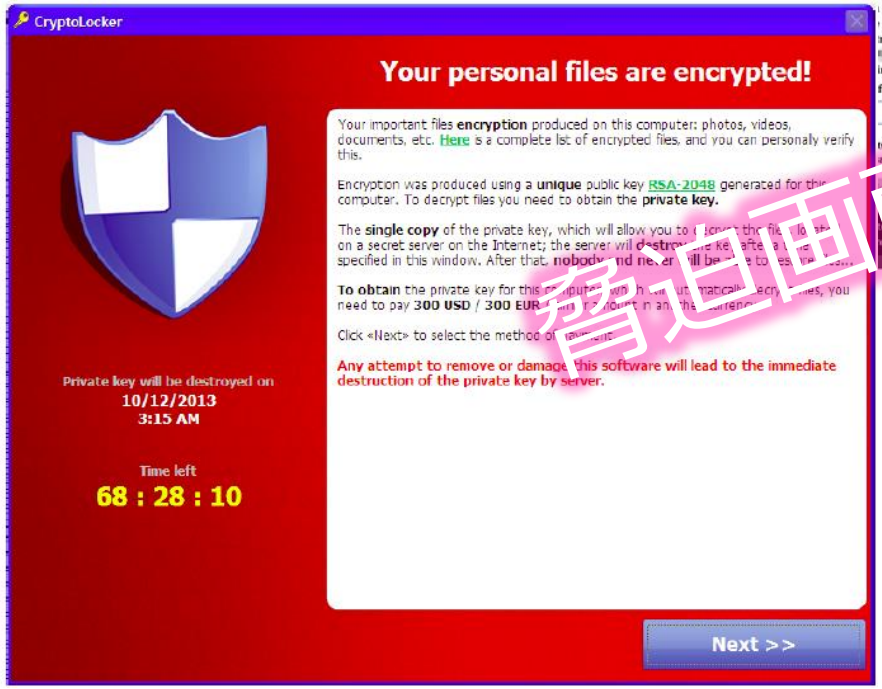
ランサムウェア 

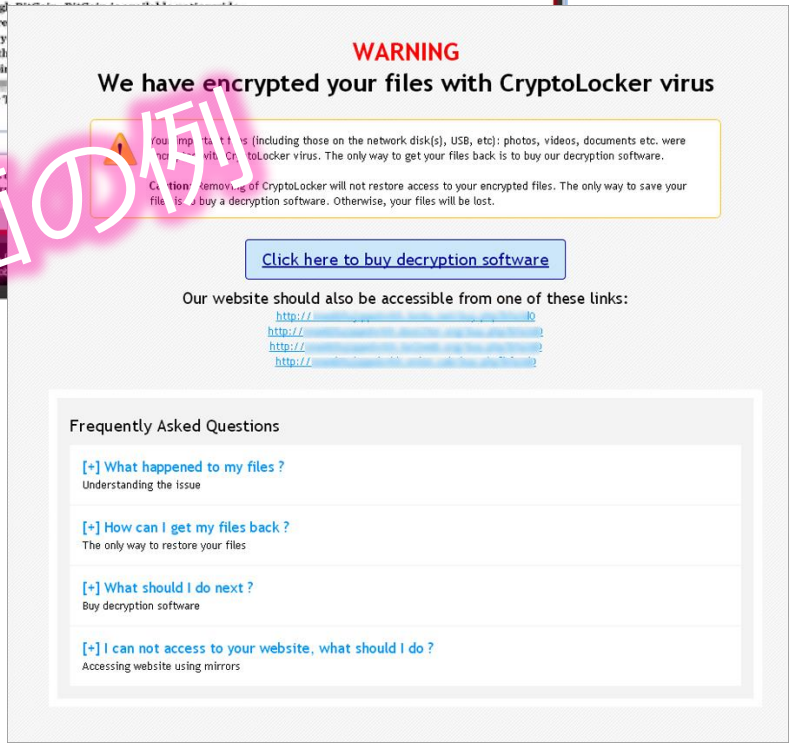
- Ransomware は、
  - 写真などのデータを人質にして、
  - 身代金（RANSOM）を要求する、
  - ソフトウェア（softWARE）です。

データを人質にとる身代金要求ウイルスとは
http://www.is702.jp/special/1807/
「ランサムウェア（Ransomware）」とは？
http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/ransomware/index.html?cm_re=side-_-threatsol-_-ransomware

百聞は一見に如かず

- Demo

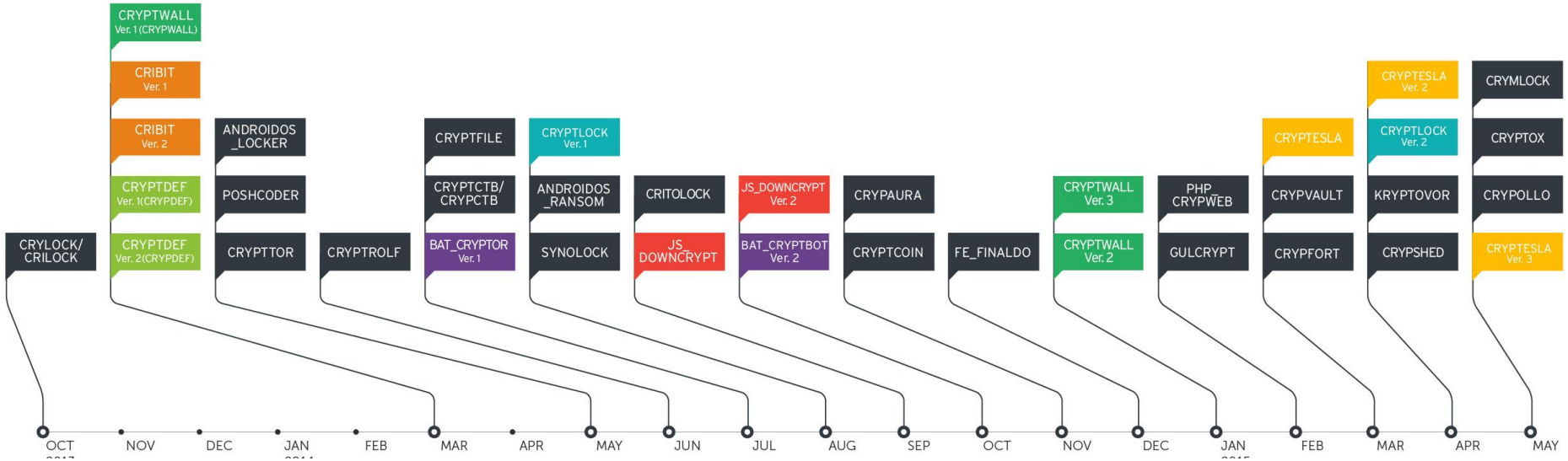




警告画面の例

いつごろから？

- 昔からあったが、2013年頃から再来



トレンドマイクロ セキュリティブログ @ 2014.09.18
多様化するランサムウェア、その手口を解説
http://blog.trendmicro.co.jp/archives/9922

トレンドマイクロ セキュリティブログ @ 2015.06.23
活発化する「Cryptoランサムウェア」
http://blog.trendmicro.co.jp/archives/11739

Google Trend

https://www.google.co.jp/trends/

2012年ごろから徐々に。

日本は2013年頃から。

どこからやってくる？

- ８割程度がメール（注：当社調べ）
  - 添付ファイル、またはスパムでの不正サイトへの誘導
- 最近は…

TREND MICRO トレンドマイクロ セキュリティブログ
POWERED BY TrendLabs
セキュリティ専門家による脅威情報・ニュースをお届けします。

検索:

サイバー攻撃 | サイバー犯罪 | モバイル | クラウド | ソーシャル | 脆弱性

ホーム » 不正プログラム » ランサムウェア拡散を狙うWeb改ざん、国内サイト70件以上で被害を確認

ランサムウェア拡散を狙うWeb改ざん、国内サイト70件以上で被害を確認

投稿日: 2015年10月30日
脅威カテゴリ: 不正プログラム, サイバー犯罪, 脆弱性, TrendLabs Report
執筆: セキュリティエバンジェリスト 岡本　勝之

トレンドマイクロでは、2015年10月29日以降、70件以上の国内Webサイトで改ざんが発生していることを確認しました。今回確認した改ざんサイトは、すべて脆弱性攻撃サイトへ誘導し、最終的に暗号化型ランサムウェアを拡散させることが目的であるものと判明しています。トレンドマイクロではすでに関係機関に通報し対処を図っておりますが、同様の改ざん被害が継続する可能性もありますので、一般に向け注意喚起いたします。

今回改ざん被害を確認した 70件以上のサイトは、中小企業、各種学校や地域の団体、個人ページなど多岐にわたっています。インターネット利用者が改ざんサイトへアクセスした場合、脆弱性攻撃サイトへ誘導されます。すべての改ざんサイトからは 1つの脆弱性攻撃サイトへの誘導が確認されており、同一の攻撃者による改ざんであるものと推測されます。

ウイルスバスター クラウド 30日間無料体験版

ウイルスデータベース

関連記事

- 台湾の機関を狙う標的型攻撃を確認。Microsoft Wordに存在したゼロデイ脆弱性「CVE-2014-1761」を利用
- 5月最終週に日本を襲った２つのWeb経由攻撃：「VAWTRAK」と「AIBATOOK」
- 「DOWNAD」：2014年第2四半期、最も多くスパムメールを送信した不正プログラムに
- 「Angler Exploit Kit」を利用してPOSシステムを事前調査する不正プログラムを確認

http://blog.trendmicro.co.jp/archives/12434

実行してしまったら？

- 痛すぎる
  - 駆除そのものはそれほど難しくないが…
  - 暗号型は身代金を払わない限りデータの複合は絶望的
  - 支払ったからといって助けてもらえないかも
  - マウント済みネットワークドライブのデータも暗号化されてしまって大参事（主に企業）
- ついでに情報も盗まれるケースも
  - 情報を盗取する他の不正プログラムをダウンロードして個人情報等を収集

トレンドマイクロ セキュリティブログ @ 2015.03.24
情報窃取型不正プログラムと連携するランサムウェア「Cryptowall 3.0」
http://blog.trendmicro.co.jp/archives/11149

日本語対応

日本語で脅迫するランサムウェアを初めて確認 @2014.03.27
http://blog.trendmicro.co.jp/archives/8801
日本語対応したCryptoランサムウェアを国内で確認 @2015.04.27
http://blog.trendmicro.co.jp/archives/11378

ビジネスモデル

- 組織化、分業化が進んでいる
  - Web サイトで申し込み
  - フリーで作成（スモールスタート可能）
- アフィリエイトモデル
  - 成功報酬型
- Bitcoin での支払

03. 安全で楽しいデジタルライフのために

やはり攻撃者が有利な状況

ランサムウェアに限りませんが、

知彼知己　百戦不殆

不知彼而知己　一勝一負　＜イマココ

不知彼不知己　毎戦必殆

敵を知り己を知れば

- **対策に銀の弾丸はない**
  - 修正パッチを適用する（脆弱性対策）
    - 特に Adobe Flash や Java
    - もちろん OS やブラウザ なども
  - ウイルス対策ソフトは最新の状態で利用
  - メールの添付ファイルを安易に開かない
  - メール内のリンクも安易に開かない
  - 大切なファイルはバックアップしておきましょう
- **必ずしも怪しくない**
  - 見るからに怪しいメールだけではない
  - いかにも怪しいサイトだけではない

04. まとめ

改めまして、まとめです。

- デジタルライフは便利で楽しいものである。
- 一方で、悪意ある者にとっても便利なものであるのも事実。
- 脅威は身近に、より巧妙に。
- 残念ながら、対策に銀の弾丸（万能薬）はない。

- だがしかし！ひとりひとりが知恵を身につけられたのなら、デジタルライフはもっと楽しいものになる。

TREND MICRO™

Securing Your Journey to the Cloud

Enjoy your digital Life !!

Thank you ☺

TREND MICRO™