SHIELD Security Reserch Center

Hisys Journal

VOL.12

HITACHI
Inspire the Next

株式会社 日立システムズ

Hisys Journal VOL.12

TABLE OF CONTENTS

ダーク・タンジェント インタビュー …… 3

日本における悪質なプロキシサーバー運営業者の摘発事例…… 7

Threat Scope …… 9

●はじめに

本文書は、株式会社日立システムズ セキュリティリサーチセンタが運営するセキュリティ情報サイト、S.S.R.C.(Shield Security Research Center) の公開資料です。本サイトでは、本文書のバックナンバーをはじめ、S.S.R.C. によるリサーチ結果などを随時公開しています。
S.S.R.C. http://www.shield.ne.jp/ssrc/

●ご利用条件

本文書内の文章等すべての情報掲載に当たりまして、株式会社日立システムズ（以下、「当社」といいます。）と致しましても細心の注意を払っておりますが、その内容に誤りや欠陥があった場合にも、いかなる保証もするものではありません。本文書をご利用いただいたことにより生じた損害につきましても、当社は一切責任を負いかねます。
本文書に記載した会社名・製品名は各社の商標または登録商標です。
本文書に掲載されている情報は、掲載した時点のものです。掲載した時点以降に変更される場合もありますので、あらかじめご了承ください。
本文書の一部または全部を著作権法が定める範囲を超えて複製・転載することを禁じます。

主催者が語るDEFCON23の舞台裏や米国セキュリティ業界のトピック

Dark Tangent

ダーク・タンジェント

インタビュー

IoTの普及が加速する中、あらゆるもののセキュリティが問われるようになってきた。そして、この潮流に一役買っているのがBlackHatやDEFCONだ。これらのカンファレンスでは、インターネットと物理世界とをつなぐセキュリティがいち早く注目されていた。今年も自動車の遠隔操作を可能にするハックを始め、衛星によるデータ通信の傍受や、産業用に使われるイーサネットスイッチの脆弱性など、数々の講演が行われた。今回は主催者であるダーク・タンジェント氏に今年のDEFCONや米国のセキュリティ業界のトピックなどについて話を伺った。

●インタビュー＝笠原利香（Rika Kasahara）
●写真＋構成＝斉藤健一（Kenichi Saito）

Q1 BlackHat と DEFCON、それぞれの参加者数について教えてください。

A1 こちらで把握している大まかな数字を言うと、BlackHat はトレーニング受講者を含めて約 1 万人。103 ヵ国の人々が参加してくれました。一方、DEFCON の参加者は 1 万 8000 人ほどになります。

Q2 DEFCON は今年から会場が Paris と Bally's に移りました。参加者の評判はいかがですか？

A2 開催初日、最初の講演を聞くために大勢の人が会場に押し寄せ、3000 名もの人が廊下で立ち往生してしまいました。このままでは参加者から私に大量のクレームが来てしまうと心配したのですが、スタッフがいろいろと対策を講じてくれました。例えば、Paris 側で行われている講演トラックの 1 つを Bally's 側に移動したり、複数ある講演トラックの終了時間をずらしたりするなどして、大量の人が同時に移動することのないようにしてくれたのです。

長年、運営に携わっているスタッフたちですから、誰かに指示される前に、自分たちで考え、行動してくれました。この点については彼らに感謝しています。

●ダーク・タンジェント（Dark Tangent）

本名はジェフ・モス（Jeff Moss）。DEFCON 主催者であり BlackHat の創設者。米国国土安全保障省の諮問委員や ICANN の CSO（最高セキュリティ責任者）などを歴任。長年にわたりハッカーコミュニティと政府機関との橋渡し役を務めている。

Q3 今年はカーハッキングや IoT ハッキングなど、新たなヴィレッジ（ワークショップ）が設けられましたが、この意図などをお聞かせください。

A3 今年から会場のホテルが変更となり、スペースが広くなったことで、いろいろなことにチャレンジできるようになりました。Open CTF の復活などもその一環です。個人的にうれしく思っているのは、テスラ社の CTO（最高技術責任者）である JB・ストラウベル（Straubel）氏が訪れてくれたことです。彼はテスラ社製品のハッキングの講演にゲストとして登場し、脆弱性を見つけてくれるハッカーたちに感謝の言葉を述べてくれたのです。

また、規模は小さいのですが、バイオハッキングに関するヴィレッジが新設されたこともつけ加えたいと思います。私自身も詳細まではわかりませんが、健康や睡眠、運動、人体に埋め込み可能なセンサー、バイオリズムやバイオフィードバック、食品やサプリメントなどに焦点を当てているのだと思います。

最近ではセンサー類が充実してきており、人間のさまざまな活動が計測可能になってきています。また、1 日に必要なカロリーや栄養素を摂取できると謳う「ソイレント」というドリンクなどもハッカーたちの注目を集めています。こういったことがバイオハッキングの背景にあるのだと思います。

ヴィレッジ運営者の 1 人は、バイオインフォマティックス（生命情報科学）の分野で博士号を持つ人で、ハプティック（haptic：触覚を伝える）ベストというものを紹介していました。ベストには複数のセンサーとモーターが装備されており、周囲の障害物をセンサーが感知してモーターの振動を使ってベストを着ている人に伝えます。この研究を進めていけば、視力を失った人に対してテクノロジーが新たな知覚を提供することにもつながりますから非常にクールだと感じました。

Q4 チャーリー・ミラー（Charlie Miller）氏とクリス・ヴァラセク（Chris Valasek）氏による自動車ハッキングの発表によって、事態

は自動車メーカーの大規模なリコールにまで発展しました。ここ数年の間、彼らは研究を続けていましたが、自動車メーカーは当初、彼らを拒絶していたように見えました。もっと早い時期からハッカーコミュニティの意見を取り入れていればよかったのではないかと思っています。

また、自動車メーカーの現在の姿勢は、十数年前のマイクロソフトの姿にも似ているとも感じました。現在のマイクロソフトはハッカーコミュニティに対して好意的で、指摘のあった脆弱性に対しても迅速に対応していますが、かつてはハッカーコミュニティを敵視していたと思います。このあたりはどのようにお考えですか。

A4 チャーリー・ミラー氏とクリス・ヴァラセク氏の発表に関して、リコールを実施した自動車メーカーは彼らに対して謝辞を述べるべきだったと思います。

ソフトウェア業界とは異なり、自動車メーカーの場合は脆弱性への対応に多額の費用がかかるという問題があります。現在、自動車メーカーはセキュリティに関わる人材を数多く採用していると聞いていますから、今後は企業文化も変わっていくのではないでしょうか。

先ほどのテスラ社の例でお話しすると、コミュニティから脆弱性の指摘が最初にあったのは、1年半ほど前のことです。この時、テスラ社にはまだ対応するセキュリティチームがありませんでした。しかし、現在では CTO 自らが講演に登壇し、迅速なアップデートを約束してくれるまでになりましたから、組織の改善は急速に進んでいるのだと思います。

Q5 最近、米国ではセキュリティツールの輸出規制を強化しようとする動きがあるというニュースを目にしました。この件についてご意見をお聞かせください。

A5 ワッセナー・アレンジメント（Wassenaar Arrangement：以下 WA）のことですね。通常兵器の輸出入管理に関する国際協定で、日本も参加しているはずです。参加国ごとに対応は異なっており、米国でも起草が行われています。商務省はこの統制品目の中に脆弱性検査などのセキュリティツールも含めたい意向のようで、現在国内で議論が行われています。

統制の対象は「軍需品」「汎用品（民生用にも軍需用にも使える品）」、およびその技術ですが、IT の分野では多くのソフトウェアや技術が汎用品に当てはまってしまいます。WA の問題の 1 つは、その品がどういう目的で作られたのかを明確に示さなくてはならないという点です。ただし、この点を明らかにするのは非常に難しいことだと思いますから、結果として弁護士の儲けにつながるだけなのではないかという懸念があります。

また、別の論点もあります。米国では最高裁においてソフトウェアはコンピューターが理解できる「スピーチ」であると認められているのです。ですから、WA は表現の自由にも関係する問題とも言え、この点を協調して議論を起こしている人たちもいます。

仮に草案のまま WA に参加すると、マルウェア研究の分野などにおいて、解析結果の情報や検体を異なる国家間でやりとりすることが規制されてしまいます。WA に基づく輸出入のライセンスを個人で取得すれば可能になりますが、もちろん、現実的とは言えません。

さらに WA の最大の問題は草案に「ゼロデイ」といった定義があいまいな言葉が多く使われている点です。WA の解釈に混乱をきたし、すでに海外への輸出を自主規制する企業なども出てきています。これは経済的にも大きな損失だと言えるでしょう。

Q6 現在においては、ソフトウェアに日々新たな脆弱性が発見され、それを悪用したサイバー攻撃も無数に行われており、人々の生活が危険に晒されています。製造物責任の観点から、今後ベンダーはソフトウェアの信頼性について、より厳しいチェックが要求されることになると思います。一方でベンダーがソフトウェアを開発する際にオープンソースのコードを利用することも多いのが現状です。ソフトウェアの信頼性とオープンソースの利用、この 2 つの要素のバランスはどのようにとったらよいと思いますか。

A6 IoT の普及によってソフトウェアの信頼性への要求はさらに増していくと思われます。自動車や飛行機など人命に関わるものもネットにつながるようになっていますし、例えば家庭にあるスマート家電の不具合によって火災などの事故が発生したとなれば、当然訴訟ということになり、裁判所の判断も加わってくるでしょう。また、これに伴い保険にも注目が集まることになると思います。

また、信頼性とオープンソースのバランスについては、信頼性が損なわれたときの被害の大きさから考慮するのも 1 つの考え方だと思います。10 ドルの被害と 100 万ドルの被害とではソフトウェアの作り方にもおのずと違いが出てくるのではないでしょうか。オープンソースのように誰もがコードを読めるものを利用するのであれば、信頼性を保証しないというスタンスもあると思います。すこし観点はずれますが、マイクロソフトの Windows XP のようにライフサイクルを終え、今後はサポートも行わないし、信頼性も保証しないという例もあります。

笠原：ありがとうございました。来年の DEFCON にも期待しています。

日本における悪質なプロキシサーバー運営業者の摘発事例

APWG eCrime 2015 講演レポート

文＝斉藤健一　協力＝坂東賢太郎

プロキシサーバー運営業者を一斉摘発

昨年 11 月、20 都道府県警の合同捜査本部が複数のプロキシサーバー運営業者（以下プロキシ業者）へ一斉摘発を行った。8 社の業者が摘発を受け、逮捕者は 12 名にのぼった※ 1。さらに、その後の警察の調べで、押収されたサーバーから大量のユーザー ID/ パスワードやフィッシング詐欺に使われたニセサイトのコンテンツなどが見つかったという。新聞・TV 等のニュースでも大きく報じられた事件なので、記憶に残っている方も多いだろう。

本年 5 月、スペイン・バルセロナで開催された APWG 主催の「eCrime 2015」では、この事件の捜査に関わった警察庁の坂東賢太郎氏（現徳島県警）による「A Case Study of Arrests of Criminal Infrastructure Use In Japan（日本で使われる犯罪インフラの摘発事例）」と題した講演が行われた※ 2。今回、坂東氏に協力いただき、講演の内容を紹介することとしたい。

犯罪目的で提供されていたプロキシサーバー

プロキシ（proxy）とは代理の意味。例えば、Web サーバーへのアクセスを中継する HTTP プロキシでは、プロキシサーバーを介することによって、ユーザーは直接 Web サーバーにアクセスすることなく Web のコンテンツを取得できる。一方、Web サーバー側のアクセスログには、プロキシサーバーの IP アドレスが記録される。この仕組み自体には何の違法性もないが、プロキシサーバーは、自身の身元を隠して接続したい犯罪者などに踏み台として使われるという側面もあり、プロキシサーバーのアクセスログが残されていない場合、IP アドレスの追跡が困難になる。

今回の講演で紹介されたプロキシ業者は、直接エンドユーザーと契約するのではなく、中国国内の代理店と契約する事業形態で、中国国内の代理店がインターネットで広告・宣伝を行い、エンドユーザーとの契約を行っていた。

中国国内の代理店は、確認されただけでも約 180 社は存在しており、中には堂々とサイバー攻撃に利用できると宣伝したり、利用者に対して各種攻撃ツールを提供したりするものもあったそうだ。つまり、「匿名でサイバー犯罪を行う」ことを前提にサービスを提供している事業者も存在していたのだ。

こうしたプロキシサーバーは、インターネットバンキングでの不正送金、企業サーバーなどへの DoS 攻撃、金融機関のフィッシングサイトの設置場所、各種会員サービスに対するリスト型攻撃による不正アクセスなど、あらゆる犯罪に利用されており、まさに犯罪インフラといっても過言ではない状態だったという。

また、捜査の過程でプロキシサーバーの所在を調査したところ、日本以外の複数国に設置されていることもわかったといい、警察は一刻もはやく対策を打つ必要性を感じていた。

警察の取り組み

坂東氏によると対策は非常に困難だったとのこと。というのも、プロキシ業者が直接不正アクセスなどの犯罪行為を行っているわけではないの

※ 1　**プロキシ業者が一斉捜索を受けた件をまとめてみた**　http://d.hatena.ne.jp/Kango/20141119/1416424239

※ 2　**Symposium on Electronic Crime Research (eCrime 2015)**
https://apwg.org/apwg-events/ecrime2015/https://apwg.org/apwg-events/ecrime2015/

で、日本の法律による検挙が難しかったからだ。

そこで、警察は ISP に協力を仰いだ。それぞれのプロキシ業者は ISP と多数の回線契約を結び、インターネットに接続していたが、この契約を解除するよう ISP に要請したのだ。これまでは、契約回線の中で犯罪などに利用された特定の回線だけを解約してきたが、これでは別の回線で新たな犯罪が行われてしまい意味がない。そこで、何かしらの犯罪が行われた場合、そのユーザーが契約している回線をすべて解除するように要請したというのだ。

そうしたところ、2012 年以降、ISP は自社の契約約款に基づいて、すべての契約を解除することに協力してくれたのだそうだ。この対応に坂東氏は、勇気ある決断をしてくれたと評している。

こうして、複数の ISP が対策を講じたことにより、悪質なプロキシ業者はインターネットへの接続回線を維持できなくなり、事実上営業が困難になった。

ブロードバンドルーターの脆弱性を悪用してインターネットに接続

しかし、事態は思わぬ方向へと展開する。プロキシ業者の一部が、家庭用に広く普及しているブロードバンドルーターの脆弱性を突いて得た PPPoE のユーザー ID とパスワードのリストを入手、ユーザーにこれを使わせてインターネットに接続するという暴挙に出たのだ（図参照）。

警察は捜査の過程でこの事実を突き止め、日本における悪質なプロキシ業者の取り締まりに乗り出すこととなった。

摘発の概要は記事冒頭でも触れているが、とあるプロキシ業者では、約 20 台の Windows 2003 Server が設置され、それぞれのサーバーにはさらに約 20 台分の仮想化した Windows 2003 Server がインストールされており、合計でおよそ 400 台分のサーバーが提供されていた。もちろん、これらのサーバー OS は違法コピーであり、マイクロソフトの著作権侵害の推定額だけでも 10 億円にも及ぶという。

また、それぞれの仮想サーバー内には、ISP 接続用のツールがインストールされており、ルーターから盗み取った PPPoE のユーザー ID/ パスワードが設定されていた。つまり、中国国内のユーザーがプロキシ業者を通じてインターネットに接続した時点で ISP への不正アクセスとなる。

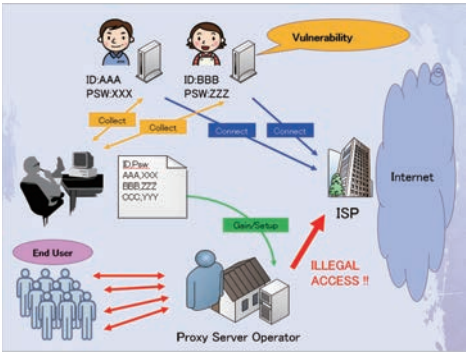

図 摘発を受けたプロキシ業者のネットワークの例
ブロードバンドルーターの脆弱性を突いて得た PPPoE の ID/ パスワードを使ってインターネットに接続。中国国内のユーザーが接続した時点で ISP への不正アクセスとなる（坂東氏のプレゼンテーションスライドより）

なお、このツールには自動的に ISP への接続アカウントを数秒間隔で変更する機能などもあり、まさにサイバー攻撃に特化したものだと坂東氏は指摘する。

さらに、押収したサーバーの調査を続けたところ、53 億もの ID/ パスワードの組み合わせや、785 万もの SNS の個人情報、フィッシングサイトのコンテンツなどが見つかったという。

そして、この摘発以降、リスト型攻撃の発生が劇的に減少し、不正送金の件数も減少したという成果もあわせて発表された。

産官学が連携してサイバー犯罪対策に取り組む JC3

講演の最後には、昨年設立した日本サイバー犯罪対策センター（Japan Cybercrime Control Center：JC3）が紹介された※ 3。

激増するサイバー犯罪の情勢を踏まえ、産官学が連携し、それぞれの組織が持つ知識や経験を集約・分析し、それらの情報を共有していくことで、脅威に対抗していくことを目的に設立された。海外機関との連携も積極的に行い、安全・安心なサイバー空間の実現に貢献していきたい、と坂東氏は語り、講演を締めくくった。

※ 3 **一般財団法人 日本サイバー犯罪対策センター** https://www.jc3.or.jp/

ハッカーやセキュリティにまつわるニュースを独自の視点から捉える時事コラム

Threat Scope

#10 企業の商取引を狙った詐欺が急増

文＝エル・ケンタロウ

Ubiquiti Networks 社が 4670 万ドルもの詐欺の被害に！

さまざまなシステムにログインする際、ID/ パスワードの他にセキュリティコードなどを入力する 2 段階認証は、Google をはじめ Facebook、Twitter など多くの Web サービスで採用され、一般にも認知されるようになってきた。

しかし、FBI（米国連邦調査局）によると、企業取引においても同様に認証の強化が必要だとされる事件が相次いで発生しているという。

ネットワーク関連機器の製造販売で知られる Ubiquiti Networks 社は、証券取引委員会に提出した四半期決算報告書の中で、4670 万ドルの企業詐欺の被害に遭ったことを公表した。現在、捜査が進行中だとして詳細は開示されていないが、セキュリティ・ジャーナリストであるブライアン・クレブス（Brian Krebs）氏は自身のブログにおいて、Ubiquiti Networks 社の被害は、FBI が 2013 年に警告を発した MITE（Man-In-The-middle-Email）攻撃、もしくは BEC（取引メール侵害：Business Email Compromise）と呼ばれる詐欺によるものだ、と見解を発表している。

企業の経営層を標的にしたフィッシング詐欺

これらの攻撃は個人を標的としたフィッシング詐欺と似ているが、標的は主に企業の経営層であり、その手口もはるかに高度だといえる。一般的なフィッシング詐欺とは異なり、標的が絞り込まれているためメールが大量に送信されることはなく、スパムフィルターなどでの検知も難しいと、クレブス氏は指摘している。

さらに、これらの企業詐欺の多くは、従来の標的型攻撃と同様に標的となる人物の調査を周到に行った後に攻撃へと移っており、メールの文章だけを見て詐欺目的なのか否かを判断するのは難しいとしている。

標的にマルウェアを感染させる標的型攻撃と比べ、技術面においては稚拙だと思われがちなこれらの詐欺行為だが、アカウントの乗っ取りなどよりもリスクが少なく、かつ得られるものが大きいため、攻撃者にとっては費用対効果の大きい手法である、とクレブス氏は述べる。

多くの場合、詐欺に使われるのは国際取引だ。国際的な犯罪となるため、捜査機関の国家間での協力が不可欠となり、犯人の摘発も難しくなることを攻撃者は熟知しているのだ。そして、その手口は、取引担当者だけでなく組織の代表を騙り、経理担当者などに送金指示を出す事例などが確認されている。

また、アカウントを乗っ取るパターンの詐欺とは異なり、攻撃者が銀行と直接やりとりするのではなく、あくまで被害者自身が正規の商取引と思い込み、攻撃者が用意した取引口座へ送金を行っているために、銀行側での不正取引検知のプロセスも回避できる。

さらに、このような詐欺行為の過程で侵害したサーバーからメールを抽出し、標的となる企業が行っている通常取引の状況や役員の出張予定などを把握し、そこから送金につなげられる情報を抜き出して、詐欺のシナリオに反映する事例もある、とクレブス氏は語っている。

企業取引も認証を強化するよう FBI が警告

このような被害は 2013 年ごろから増えていることから、FBI は同年 12 月にプレスリリースを

発表。企業取引においてもメールのみでのやりとりに注意するように指摘し、メールだけに頼らず電話など他の通信チャンネルの利用や、メールアカウントへのデジタル署名の付加などを促している。

今回の Ubiquiti Networks 社の被害額は突出しているが、FBI のインターネット犯罪苦情センター(IC3) の統計によると、2013 年 10 月から 2014 年 12 月の間で IC3 に報告があった被害状況は、米国被害企業数 1198 社、被害総額 1 億 7970 万ドル、非米国被害企業 928 社、被害総額 3520 万ドルで、合計すると 2 億 1500 万ドルもの被害が発生しているという。

最近では、流ちょうな日本語を使った標的型攻撃メールが増加していると話題になっている。このことからもわかるとおり、攻撃者の視線の先には日本が見据えられている。日本の企業においても、サイバーセキュリティの一環としてこれまでの商取引のプロセスを早急に見直す必要があるだろう。

●参考 URL
- **Tech Firm Ubiquiti Suffers $46M Cyberheist**
  http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/
- **'Man-in-the-E-Mail' Fraud Could Victimize Area Businesses**
  https://www.fbi.gov/seattle/press-releases/2013/man-in-the-e-mail-fraud-could-victimize-area-businesses
- **FBI: Businesses Lost $215M to Email Scams**
  http://krebsonsecurity.com/2015/01/fbi-businesses-lost-215m-to-email-scams/