HITACHI
Inspire the Next

Hitachi Systems Security Journal

VOL.25

株式会社 日立システムズ

Human * IT

Hitachi Systems security Jounral VOL.25

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

CODE BLUE 2016 レポート

文 = 西方望
撮影 = 斉藤健一

日本発のセキュリティカンファレンスとして2014年にスタートしたCODE BLUEは年々その規模を拡大し、昨年からは2トラックで講演が行なわれるようになった。今年は10月20日と21日の2日間、昨年と同じ新宿の会場にて開催されたが、2トラックなのは変わらないものの、講演数は昨年の20本に対して24本とさらに多くなっている。また、同時に開催されたハッキングコンテストもより広い会場で行なわれるようになり（ただし諸般の都合で予定された3つの競技のうち1つは中止）、より充実の度を増したと言えるだろう。

「e-Estonia：電子国家への叙事詩」
アンナ・ピペラル（Anna PiPeral）氏

開幕の基調講演は エストニアの先進的なIT政策

幕開けとなる基調講演のタイトルは「e-Estonia：電子国家への叙事詩」。スピーカーのアンナ・ピペラル氏は、エストニアの「『e-Estonia』ショールーム担当責任者」だ。エストニアと関わりのある日本人は多くないだろうが、IT関係者であれば、さまざまなIT政策を積極的に推し進めている国として耳にしたことがあることと思う。しかし、具体的にどのような技術がどう使われているのかについて知る機会は少なかった。ピペラル氏は諸外国に対してエストニアのIT政策を紹介する担当者であり、まさに話を聞くにうってつけの人物だ。ピペラル氏によると、エストニアではすでにほとんどの行政サービスがオンラインで受けられるようになっており、コストや時間を大幅に削減できているという。またデータ処理・管理システムとして「X-ROAD」と呼ばれる情報インフラが導入されており、これにより各種情報を容易に相互利用できる。データベースは分散化され、その一貫性はブロックチェーンによって確保されているという点からも、新しい技術を積極的に取り入れていることが分かるだろう。またそのサービスはエストニア一国から、その基盤や技術をEUに拡げつつあるだけでなく、「e-Residency」という海外居住者でもエストニアのIDを取得できる制度もある。これによりエストニアでの起業などが容易となり、日本でもすでに300人ほどが登録しているという。小国であるからこそここまでできる、という側面はあるものの、日本も今後好むと好まざるとに関わらず国家のIT化がより進展していくのは必然であり、それを考える上でも非常に参考となる講演だったと言えるだろう。

では、印象に残った講演を簡単に紹介しよう。本当はもっと取り上げたいところだが、紙幅の都合で3つのみに留めさせていただく。

CGC（全自動ハッキングトーナメント）優勝チームのシステムに迫る

CGC（Cyber Grand Challenge）については本誌Vol.22でも紹介したが、セキュリティの自動化をめざすDARPA主催のコンテストだ。8月のDEFCONで行なわれたCGC本戦の結果、優勝したのはMAYHEMシステムで臨んだチーム

「Cyber Grand Challenge (CGC) : 世界初のマシンだけによる全自動ハッキングトーナメント」
タイラー・ナイスワンダー（Tyler Nighswander）氏

「EXOTIC DATA RECOVERY & PARADAIS」
しもがいと・だい氏

ForAllSecure。今回の CODE BLUE では、優勝チームの一員であるタイラー・ナイスワンダー氏による「Cyber Grand Challenge (CGC) : 世界初のマシンだけによる全自動ハッキングトーナメント」と題する講演が行なわれた。

あまり具体的な内容が知られていなかった CGC だが、さまざまな情報が明らかとなった。例えば用いられたのは既存のバイナリなどではなく、7 つのシステムコールのみからなる専用の実行ファイルだったというのは面白い。これでも Heartbleed のようなぜい弱性も再現できるという。MAYHEM はシンボリック実行とファジングの手法を組み合わせ、ぜい弱性の発見から、エクスプロイト、パッチ当てなどのすべてを自動的に行なう。これだけの複雑な処理がもう自動化できているというのは驚異だ。もちろんナイスワンダー氏も言うようにセキュリティの自動化はまだ始まったばかりだが、未来の可能性を十分に感じることができた。

HDD の不可視領域に Windows XP をインストール !?

データ復旧の専門家である、しもがいと・だい氏による講演タイトルは「EXOTIC DATA RECOVERY & PARADAIS」。HDD には代替領域などとして不可視の部分があるが、しもがいと氏によれば、これは 2TB のディスクで平均 13GB にもなるという。しかしこの領域はアプリケーションや OS はもちろん、データ消去ソフトなどもその大部分にはアクセスできない。ところがファームウェアに細工をすることにより、氏が「PARADAIS」と名付けたこの不可視領域にアクセスが可能になるというデモが行なわれた。ディスクが完全消去されていることをバイナリエディタで確認した上で、その同じディスクの基板を取り替えて PC に接続し起動したところ、なんと Windows XP が立ち上がったのだ。別のファームウェアにすることにより PARADISE 領域から起動したわけだ。もしこれが自由に使えれば、機密データを隠すといった活用もできるが、やはり気になるのは悪用法だろう。氏はデータを完全に不可視にするランサムウェアの例を挙げたが、その他にも可能性はまさに無限大。今後悪用されないことを祈るばかりだ。

エアギャップを越える多彩なアイディアを披露

データを守るための強力な手法が「エアギャップ」だ。ネットワークに接続していない（≒「空気の間隙」がある）コンピューターなら、当然ネットワーク経由の侵入・データを持ち出しは不可能。しかしエアギャップも万能ではない。イスラエルのベングリオン大学のチームはこれを越えるための手法を研究しており、その一員であるイスラエル・ミルスキー氏が、これまでの取り組みも含めたエアギャップ越えのさまざまな可能性を紹介した。今までも同グループの発表した数々の研究成果には感心させられてきたが、あらためてまとめられるとその多彩さには驚く。

「エアギャップのセキュリティ : 最先端の攻撃、分析、および軽減」と題された講演では、PC や機器が発するエネルギーをすべて情報送信に、セ

「エアギャップのセキュリティ：最先端の攻撃、分析、および軽減」
イスラエル・ミルスキー（Yisroel Mirsky）氏

「セキュリティはどれくらいが適量？」
カールステン・ノール（Karsten Nohl）氏

ンサーや入力装置をすべて受信に利用しようとしていると言っても過言ではない。例えば CPU などの温度センサーを受信に使ったり、ハードディスクのノイズで送信したりするなど創意にあふれている。これらのうち実際の脅威となりうるものは少ないだろうが、ハックの根本はやはりアイディアということを再認識させてくれた。

セキュリティとイノベーションのバランスを問う！

締めの基調講演を行なったカールステン・ノール氏は、RFID の解析や携帯電話のプロトコルである SS7 のぜい弱性の発見で知られるセキュリティ研究者であり、最近では世界的に話題となった「Bad USB」で USB メモリの新たな悪用の可能性を示した非凡なハッカーだ。そのノール氏の講演は「セキュリティはどれくらいが適量？」と題し「セキュリティとイノベーションのバランス」をテーマとしたものだ。

セキュリティと利便性はトレードオフの関係にある、というのはよく言われることだが、数知れぬぜい弱性やセキュリティ上の問題を発見してきた一方コンサルタントとしても活躍するノール氏の言葉は非常に説得力がある。私たちはセキュリティを過剰に気にするあまり、現場の生産性を阻害し、イノベーションの芽を摘んでいるのではないか？ぜい弱性などが発見されると研究者は最悪のシナリオを語り、それがメディアで大々的に報じられ、企業はそれに基づいて極端な対応を採りがちだが、実際に被害を生む例は少ない。例えば今年「iPhone の 86%をハック可能なマルウェア」が報じられたが、感染が確認されたのは 1 台だけ。これを恐れて会社へのスマートフォン持ち込みを禁止するというのは馬鹿げている。あるいは昨年報じられた自動車ハッキングにしても実行は非常に難しいものであり、このレベルの問題をすべてあらかじめふさがなければならないのでは、新たな技術は導入できないのではないか。重要なのは「すべてを守る」ことではなくリスクの監視、リスクの管理だ、とノール氏は訴えた。

昨年の CODE BLUE は、基調講演は人工知能によるシンギュラリティやわれわれが目にする情報の真正性についてのものといった、どちらかと言えば「遠く」を見据えていた感があった一方、各講演のテーマは IoT やドローンなど流行のものが目立った。しかし今年は基調講演も今現在の状況や問題という「足元」についてのもので、各講演もセキュリティの自動化や IoT など最新動向を追いつつも落ち着いた印象があり、その意味でもさらに充実したように思う。このようなカンファレンスが毎年開催されるのは実に心強い。セキュリティの重要性、人財不足が叫ばれる中、CODE BLUE の意義は今後もより増していくだろう。

「インシデントレスポンス概論」産学連携セミナー レポート

取材・文＝斉藤健一

産学連携による実践的なセミナー

2016 年 8 月 20 日、東京情報大学において「インシデントレスポンス概論 - マルウェア動的解析 -」と題するセミナーが行なわれた。これは同大学と日立システムズとの産学連携による演習形式の講座で、5 日間にわたる特別セミナーの内容から公開講座用にマルウェア動的解析の部分を編集した内容となっている。

東京情報大学 情報サービスセンター長の布広永示氏によれば、企業と連携することによって、現場で起きている問題を題材とした実践的な講義を行なうことができ、実務レベルで有益なスキルを短時間で習得できるという。2013 年からデジタルフォレンジックやマルウェア解析に関する単位制の講座を開講し、これまで約 100 名の生徒が受講しているというが、布広氏は 2018 年までにその数を 300 名にまで増やしたいと語っている。

日立システムズとしても、人財育成の裾野を広げる取り組みとして協力しているという。社会人であれば CISSP といった資格があるが、学生であれば評価の基準は単位ということとなり、講座の受講や単位の取得がセキュリティ業界への登竜門になると考えているそうだ。

このセミナーが公開講座として開かれたのは今回で 2 回目となる。参加資格が設けられているわけではないが、Windows の基礎的な知識や Linux の基本的なコマンドの理解が求められる。会場には学生と社会人をあわせ約 20 名ほどが集まった。会場はデスクトップ PC が設置された PC 教室で、参加者には演習用の仮想環境がセットアップされたノート PC も貸与される。

セミナーは座学と演習に分かれた構成となっている。午前中は「マルウェア解析概要」と題する講座が行なわれ、午後には「マルウェア動的解析」と題したハンズオン形式の講座や、参加者自身がマルウェアの解析に挑戦する演習が行なわれる。

講座の冒頭で挨拶に立つ東京情報大学 情報サービスセンター長の布広永示氏

講師を務めるのは日立システムズ サイバーセキュリティリサーチセンタの折田彰と関口竜也の両名だ。

マルウェアの動作から調査すべきポイントを知る

マルウェアを解析するには、まずマルウェアの動作を知る必要がある。最初の講義では折田がマルウェアに共通する特徴を挙げ、その特徴から調査すべきポイントを以下のように解説した。

・起動プロセスの調査

マルウェアは実行ファイル（.exe）として起動する場合もあれば、サービスとして起動する場合もある。また、DLL インジェクションなどにより InternetExplorer といった別のプログラムを装うこともあるという。いずれの場合でも Windows の起動プロセス一覧を調べることが重要だという。

講座の会場風景

・ファイル操作の調査

ユーザーがマルウェアのアイコンをダブルクリックして実行すると、自身や関連するファイルを temp フォルダーなど別の場所にコピーすることがある。また、痕跡を消すなどの目的で元のファイルを削除したり、作成日時を変更したり、関連ファイルを隠し属性に変更したりする場合もある。さらに、マルウェアによっては、感染マシンの OS やインストールアプリケーションの情報、バージョン情報を収集し保存するものもある。したがって、ファイルの作成・削除の調査も重要なポイントになるのだそうだ。

・レジストリの調査

マルウェアは感染 PC が再起動されても再び実行できるようにレジストリに変更を加えて自身を自動実行にしたり、感染の発覚を遅らせるためにタスクマネージャーなどのツールを起動させないように設定したりすることがある。また、レジストリ自体にファイルを保存する例もあり、レジストリの調査は必須だという。

・通信の調査

外部ネットワークとの通信も調査すべき点の 1 つだ。マルウェアの中には、Google や Yahoo! をはじめとする Web サイトや感染 PC のグローバル IP アドレスを確認するサイトなどへの接続を試み、接続できなければ動作を終了するものもある。マルウェアによる外部への通信は他にも、C&C サーバー（Command & Control）への接続や新たなマルウェアのダウンロードなどが挙げられる。また、バックドアが設置され、感染 PC の特定ポートを開放し、リッスン状態にすることもあるという。

マルウェアの動作としては他にも、メールにマルウェア自身を添付したり USB メモリが挿入された時に自身をコピーして感染を拡大させるものや、HDD のブートセクター（MBR）を上書きしたり、ファイルを削除したりするなどの破壊活動を行なうものだ。また、近年のマルウェアには解析を妨害するためにさまざまな機能も実装されているという。例えば、仮想環境では動作しない機能や、デバッガーの起動を検知して動作を終了させる機能、他にもマルウェアのコードをパッカーと呼ばれるツールで難読化してセキュリティ専門家によるコード解析を手間取らせるものなどがある。

講義の終盤ではデモも行なわれ、RAT（Remote Admin Tool：遠隔操作ツール）・文書偽造型マルウェア・バンキングマルウェア・ランサムウェアなどが実際に動く様子が紹介された。参加者の中でマルウェアに触れた人はほとんどいなかったので、脅威を身近に感じる良い機会になったのではないだろうか。

マルウェアの動作をモニタリングする手法が動的解析

午前 2 コマ目の講義は関口が担当し、マルウェ

ア動的解析の手順を紹介した。動的解析とは解析手法の1つ。リバースエンジニアリングによるコードレベルの調査を「静的解析」と呼ぶのに対し、マルウェアを動作させてその挙動を調査するのが「動的解析」となる。静的解析では、難読化されたコードの解読やプログラミングの知識など要求されるスキルは高い。一方の動的解析の場合もWindowsやネットワークの知識などが必要となるが、ツールを使うことにより比較的容易に実施できる。

関口は、動的解析を行なうことでマルウェアの被害範囲の特定、駆除、感染拡大の防止といった対応策を検討できるようになると述べた。

近年、企業などの組織ではメールに添付された数々のマルウェアを受信している。また日々続々と亜種が登場し、アンチウイルスソフトの検知をすり抜けてしまうものも増えている。こういった状況から自組織内でもマルウェアを解析できる技術が必要だといえる。

動的解析の大まかな手順は以下のとおりだ。

（1）表層解析

マルウェアを推察する作業を指す。拡張子やファイル形式の調査、マルウェアに含まれる文字列の抽出、ハッシュ値を取得して既知のものか否か確認、複数のアンチウイルスソフトを使い検知できるか否かなどを確認する。

（2）環境構築

マルウェアの動的解析では実環境から隔離された仮想環境で行なわれることがほとんどだ。もちろん、実環境に影響を与えないための配慮であると同時に、仮想環境であれば、マルウェアに感染させた後でもPCの環境をクリーンな状態に戻すことが容易だからという理由もある。仮想環境は、前述の表層解析で得られた情報を元に構築するが、マルウェアによっては外部へ通信するものもあり、擬似的なインターネット環境を提供する仮想マシンを別途構築する場合もあるという。

（3）動的解析

前述した折田の講義で解説されたマルウェア調査のポイントに沿って作業を進める。具体的に確認・調査を行なうのは、プロセスの状況、マルウェアによって作成・変更されたファイル、レジストリ、外部ネットワークへの通信、Windows APIの呼び出し状況などが挙げられる。

（4）まとめ（レポート）

解析作業で得られた情報をまとめていくが、必要に応じて（1）～（3）の作業を繰り返すこともあるという。

演習ではマルウェアの動的解析に挑戦

午後の講義では、解析に使用するツールの紹介がハンズオン形式で行なわれた。教室に備え付けられたデスクトップPCの画面には、講師の折田がツールを操作する様子が映し出される。参加者はこれを参考に貸与されたノートPCで自分でもツールを操作してみる。紹介された主なツールは次ページの表のとおり。

また、このノートPCにはマルウェアを感染させ実際に解析を行なう仮想マシンの他、DNSやHTTPのダミーのレスポンスを返すインターネットシミュレーション環境も用意されている。

ツール紹介が一とおり終わった後は、参加者がマルウェア解析に挑戦する演習となる。演習に使われる検体は、日立システムズが独自に作成したもので、マルウェアに似た挙動をするが、感染活動などは行なわない無害なものとなっている。

この教材を使ったセミナーが今後も行なわれることを考慮して、今回の記事では演習内容については触れないこととしたい。この記事を読んでマルウェアの動的解析に興味を持った方がいれば、ぜひ参加していただきたい。

演習に取り組む参加者の様子は真剣そのものだったが、なにしろはじめての経験で、講義の内容を理解しているつもりでも、実際に手を動かしてみるとうまく行かず、戸惑う方も多かったようだ。また、演習を通じて得た知識やスキルをどのように維持していくかが難しいと話す参加者もいた。

これまで紹介してきたように、プログラミング

の知識・経験といった高度なスキルがなくても、動的解析によってマルウェアの挙動を調査することは可能だ。セキュリティ専任者を設けていない組織が多い現状を考えると、システム管理者などが今回のセミナーを通して、実践的な知識を得られることは貴重な機会だといえるだろう。東京情報大学と日立システムズの取り組みには今後も期待したい。

講義で紹介された主なマルウェア解析ツール

ツール名	解析手法	概要	URL
md5deep	表層解析	ハッシュ値を確認するコマンドラインツール ファイルの同一性を調査	https://github.com/jessek/hashdeep
file	表層解析	ファイル形式を確認 アイコンや拡張子の偽装などを調査	https://www.darwinsys.com/file/
Bintext	表層解析	検体に含まれる文字列を確認（バイナリエディタ） Windows API や通信先 URL を調査	(配布終了)
PDF Stream Dumper	表層解析	PDF 形式の解析対象に内包されているデータを確認 不正なスクリプトやシェルコードを調査	https://sandsprite.com/blogs/index.php?uid=7&pid=57
Virus Total	表層解析	オンライン解析サービス ハッシュ値で既存の解析結果を検索できる	https://www.virustotal.com/ja/
UPX	表層解析	UPX 形式のパック・アンパックツール マルウェアをアンパックして解析しやすくする	https://upx.github.io/
Process Monitor	動的解析	レジストリ・ファイル・ネットワークすべてのイベントをリアルタイムに監視	https://learn.microsoft.com/ja-jp/sysinternals/downloads/procmon
Process Explorer	動的解析	高機能なタスクマネージャー 実行プロセスの詳細を調査することができる	https://learn.microsoft.com/ja-jp/sysinternals/downloads/process-explorer
CaptureBAT	動的解析	ファイル・レジストリ・ネットワークの挙動を記録 削除されたファイルの保存などが可能	https://github.com/ph0sec/CaptureBAT-client
Autoruns	動的解析	自動起動の設定を一覧で表示	https://learn.microsoft.com/ja-jp/sysinternals/downloads/autoruns
regshot	動的解析	ファイルシステム・レジストリのスナップショット取得ツール。スナップショット間の差分出力などが可能	https://sourceforge.net/projects/regshot/
API Monitor	動的解析	Windows API の呼び出し状況の確認 プログラムの挙動を推測	http://www.rohitab.com/apimonitor
Wireshark	動的解析	ネットワークに流れるデータのキャプチャー ネットワーク通信データの調査	https://www.wireshark.org/download.html

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

#23 攻撃者の費用対効果を下げるセキュリティ対策

文＝エル・ケンタロウ

犯罪者を狙う犯罪者

英語のことわざに“There is no honor among thieves”というものがある。訳せば「盗人に仁義なし」となり、犯罪社会では裏切られても仕方がないという意味で使われる。セキュリティ企業の Sophos 社が発表した最新レポートによれば、Pahan と呼ばれるハッカーがこれまでターゲットにしてきた一般ユーザーや組織に加え、地下フォーラムなどでサイバー攻撃ツールの売買に関わっている犯罪者たちをも標的にしているという。

このハッカーは Pahan 以外にもさまざまなハンドルネームを使い、サイバー犯罪向けに開発されたソフトウェアの中にマルウェアを仕込み、これらのツールを使おうとする犯罪者への感染を狙っている、とレポートでは報告している。

Pahan の手口は地下フォーラムに Aegis Crypter というアンチウイルス回避ツールを無料で提供すると広告を掲載して人寄せをするが、対象ファイルには RxBot というトロイの木馬が隠匿されており、結果としてダウンロードした犯罪者がこのトロイの木馬に感染するというものだ。現在のところ、Pahan の犯行による感染数など、具体的な被害状況は明らかになっていないとしながらも、レポートでは数百件に上るだろうと推測している。

スキルの低い犯罪者を標的にする仕組みも

また、犯罪者や犯罪者予備軍を標的とした同様の例として、現在では Symantec 傘下の Blue Coat 脅威ラボ（BCECTL）は、他者の Facebook アカウントをハッキングしようとする犯罪者を標的とした CaaS（Crimeware as a Service：犯罪ウェアサービス）の存在を確認していると発表した。CaaS を使えば誰でも簡単にサイバー攻撃が実行できるようになるが、逆にスキルの高いサイバー犯罪者がスキルの低い犯罪者予備軍を狙う罠として使われる可能性があると、BCECTL 責任者のアディティヤ・スード（Aditya Sood）氏は語っている。

今回発見された事例は以下のとおり。Facebook アカウントのハックを謳う CaaS が罠として用意されており、そこに他者のアカウントをハックしたいと考えるユーザーがアクセスすると「登録用フォーム」へのリンクが表示される。そして、サービス開始のための質問フォームに答えていると、アクセスしたユーザー自身のログイン情報が窃取されるというものだ。

今回のケースがユニークなのは容易に犯罪者を増やす CaaS のようなサービスの存在で、スキルがなくても簡単にサイバー攻撃を実行できるようになるが、一方で犯罪者自身が被害に遭う可能性が高くなる現状が挙げられている点であろう。

報復的サイバー攻撃の是非

犯罪者同士、もしくはハッカー同士の対立はこれまでもあった。例えば、内紛で分裂した Anonymous が他の Anonymous の情報を暴露した例や、さかのぼれば 1990 年代に起こったハッカー間の抗争などだ。一方で、サイバー脅威に対して攻撃的な防衛手段を取るべきとする DDoS 対 DDoS などの論議も以前からそ上に載ってはいるが、法律および倫理的な観点からなかなか議論が進まない現状もある。

日本の電話詐欺と同様、海外では技術サポートを騙った詐欺による被害が拡大している。技術サポート詐欺とは、Web ブラウザーの画面に「あなたのコンピューターはウイルスに感染していま

す。至急以下の電話番号に連絡して対策をしてください」といったメッセージを表示させ、連絡してきたユーザーに対して無駄なソフトウェアを購入させたり、法外なサポート費用を請求したりする詐欺のこと。マイクロソフト社の発表によれば、米国だけでも技術サポート詐欺による被害総額は15億ドルにも上るという。

セキュリティ研究者のイヴァン・クワエトコウスキー（Ivan Kwiatkowski）氏は、自身の両親が技術サポート詐欺の被害に遭ったため、逆に詐欺グループのPCをランサムウェア（Locky）に感染させた経緯をブログで公開している。クワエトコウスキー氏はWebブラウザーに表示された電話番号に連絡して、詐欺グループの技術サポート担当者を自身があらかじめ用意したWindows XPの仮想マシンにリモートログオンさせた。

クワエトコウスキー氏はPCが苦手な老人を演じ、詐欺グループと電話でやりとりしながら、自分のクレジットカードの画像と偽ったランサムウェアを送りつけた。相手の技術サポート担当者は「ファイルを解凍したが画像が表示されない」と告げたが、そのバックグラウンドではランサムウェアがファイルの暗号化を始めていた。

クワエトコウスキー氏は、ランサムウェアによる全ファイルの暗号化が成功したか否かは定かでないと発言しているが、詐欺グループの電話番号もブログで公開しており「時間のある人は電話をかけてソーシャルエンジニアリングをしてみてはどうか」と読者に呼びかけている。

攻撃者の費用対効果を下げる取り組み

クワエトコウスキー氏はブログで、今回の件は報復ではなく、あくまで相手の時間を無駄に使わせることで詐欺行為の費用対効果を下げることが目的だといい、これによって詐欺行為が減ることを望むと語っている。

そして、この費用対効果を下げる取り組みこそがサイバー犯罪・脅威対策において効果的だと考えるセキュリティ研究者も多い。というのも、犯罪行為に掛かるコストが高騰すれば、犯罪者は別の手法に移るからだ。もちろん、全てのサイバー脅威に対して有効というわけにはいかないが、容易に犯罪者を生み出すCaaSなどもいずれは費用対効果が低過ぎれば、市場によって自然淘汰されることになるだろう。

●参考URL

The Hacker Thats Hacking Hackers
http://themerkle.com/the-hacker-thats-hacking-hackers/

A Sneaky Hacker Is Infecting Other Hackers with Malware
http://news.softpedia.com/news/a-sneaky-hacker-is-infecting-other-hackers-with-malware-507946.shtml#ixzz4K6cex5zX

Crimeware-as-a-Service Hack Turns Potential Hackers Into Victims
http://www.darkreading.com/attacks-breaches/crimeware-as-a-service-hack-turns-potential-hackers-into-victims/d/d-id/1326849

How I got tech support scammers infected with Locky
https://blog.kwiatkowski.fr/?q=en/tech-support

Human * IT

人と IT のチカラで、驚きと感動のサービスを。

Hitachi Systems Security Journal VOL.25

株式会社 日立システムズ
本社 〒141-8672 東京都品川区大崎 1-2-1