MALWARE REPORT

マルウェアレポート

2018

上半期

安全なネット活用のための

セキュリティ情報

はじめに

本レポートでは、2018年1月から6月までの間（以降2018年上半期）に検出されたマルウェア、および発生したサイバー攻撃事例についてご紹介します。

「1. 2018年上半期マルウェア検出統計」では、2018年上半期に日本国内で検出されたマルウェアについて、2017年と比較して傾向を分析します。また、特に検出数の多い3つのマルウェアについて詳しく分析します。

次に、2018年上半期に特に猛威を振るった脅威の中から「2. 仮想通貨を狙う脅威」、「3. インターネットバンキングを狙う脅威」、「4. Windowsプロトコル SMBの脆弱性を悪用する攻撃」について攻撃の手法と傾向を説明します。

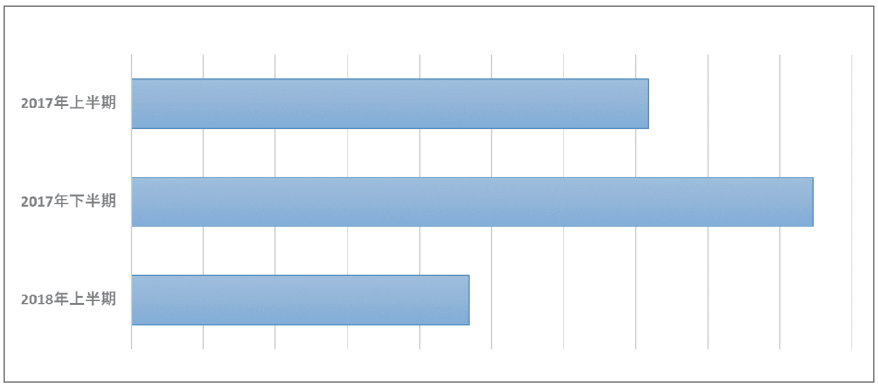
最後に、「5. サイバー犯罪のためのサービス“Crime as a Service”」を取り上げます。ここでは、巧妙化する「サイバー攻撃者のためのサービス」について解説します。

contents

1 2018年上半期 マルウェア検出統計

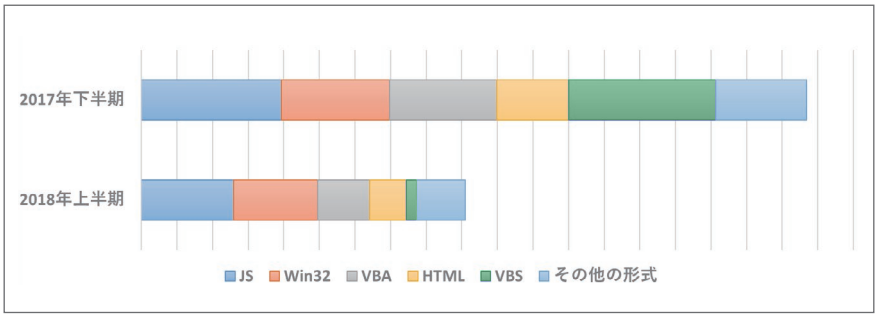
2018年上半期マルウェア検出統計

2018年上半期にESET製品が国内で検出したマルウェアの検出数は、2017年下半期と比べて半減しており、世界全体での検出数も同様に減少しています。 2017年下半期に多く検出された、ダウンローダーを添付したばらまき型メールが減少したことが大きな要因と推測されます。



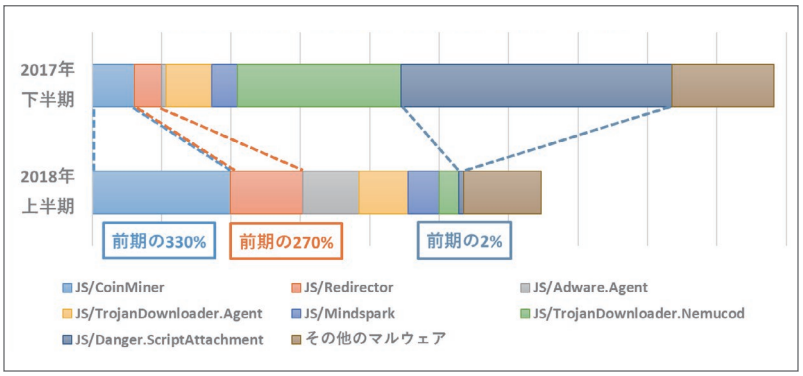
全マルウェアの検出数合計(国内)

形式別でも2017年下半期と比較して軒並み減少しており、とりわけVBScript(グラフ中緑色「VBS」)形式のマルウェアが激減しています。当時流行していたLockyやGlobeImposterのダウンローダーとして使われたために、2017年下半期にはVBScript形式が多く検出されていましたが[1]、2018年に入ってからはあまり観測されていません。



形式別のマルウェア検出数(国内)

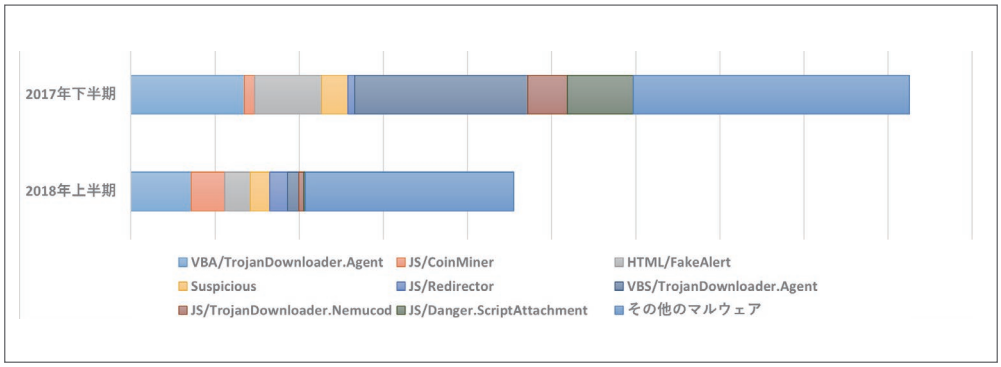
2017年下半期と同様、最も多く検出されたのはJavaScript(JS)形式で作られたマルウェアです。しかしながら、その内訳については様変わりしています。



JavaScript形式・検出名別マルウェア検出数(国内)

2017年下半期と比較して、JS/CoinMiner(グラフ中水色)およびJS/Redirector(グラフ中橙色)の検出数が増加しています。いずれも基本的にはWebサイト上に存在する脅威です。このようなWeb上の脅威が増加している背景として、攻撃の対象がWindows端末だけではなく、さまざまな端末に拡がっていることが考えられます。
メールを経由したマルウェアJS/Danger.ScriptAttachment(グラフ中紺色)はVBScript形式のダウンローダーと同様、当時流行していたマルウェアのダウンローダーとして使われていたために、2017年下半期には検出数が増加していましたが、2018年に入って検出数が激減しています。

JavaScript形式の以外にも多数検出されているマルウェアが存在します。



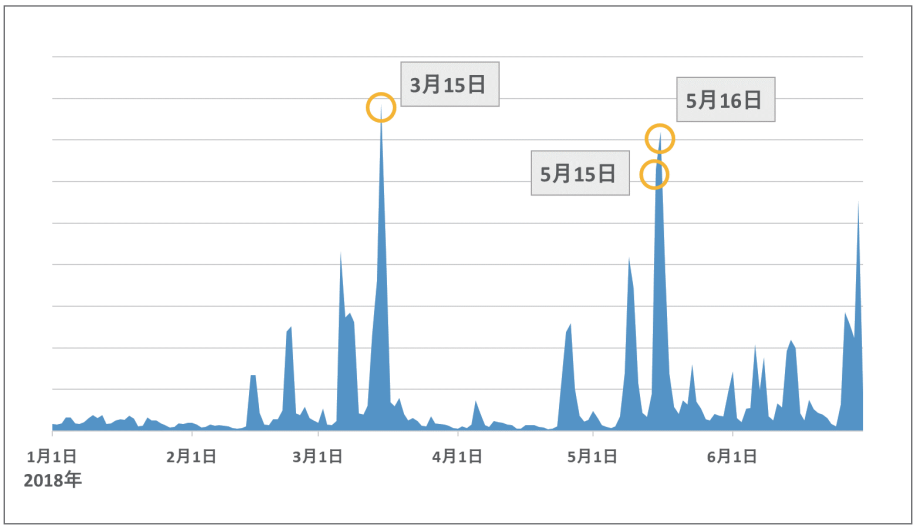
検出名別マルウェア検出数(国内)

2018年上半期に最も検出されたマルウェアは、VBA/TrojanDownloader.Agent(グラフ中水色:2017年下半期2位)です。2018年上半期に検出されたマルウェアのうち、全体の15.3%を占めています。
2位はJS/CoinMiner(グラフ中橙色:2017年下半期12位)です。順位、検出数ともに急上昇しています。2018年上半期に検出されたマルウェアのうち、全体の8.5%を占めています。

3位はHTML/FakeAlert(グラフ中灰色:2017年下半期3位)です。2018年上半期に検出されたマルウェアのうち、全体の6.4%を占めています。
これらの3種類のマルウェアについて、詳しく見ていきます。

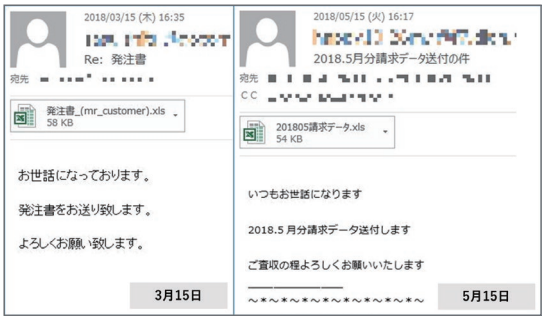
① VBA/TrojanDownloader.Agent

このマルウェアは、Microsoft Office上で利用可能なプログラミング言語のVBA(Visual Basic for Applications)で書かれたダウンローダーです。ファイル形式はMicrosoft Word文書あるいはMicrosoft Excel文書であることが大半です。一般的にメールに添付されることで配布されます。ダウンロードするマルウェアの種類はさまざまですが、この期間の間ほとんどの場合バンキングマルウェアです。バンキングマルウェアに関しては、「3. インターネットバンキングマルウェアを狙う脅威」で詳しくご説明します。

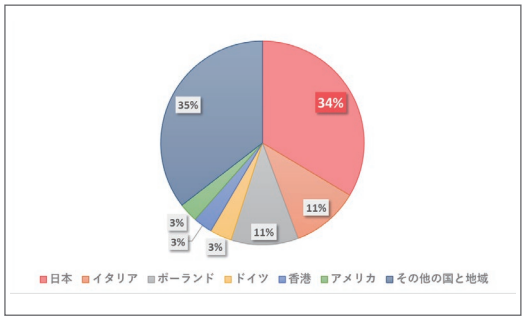


VBA/TrojanDownloaderの国内検出数推移

ご覧の通り、3月15日と5月15~16日(グラフ中○印)の検出数が突出して多くなっています。この期間に、このマルウェアを添付したメールが大量に送信されたことを示しています。メールの文面は、発注書や請求書を装ったものが多く確認されています。



VBA/TrojanDownloaderが添付されたメールの文面

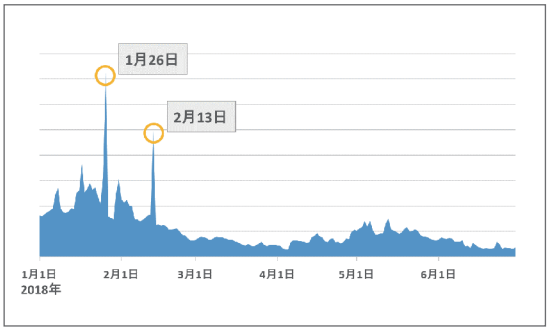


VBA/TrojanDownloader検出数の割合(2018年上半期)

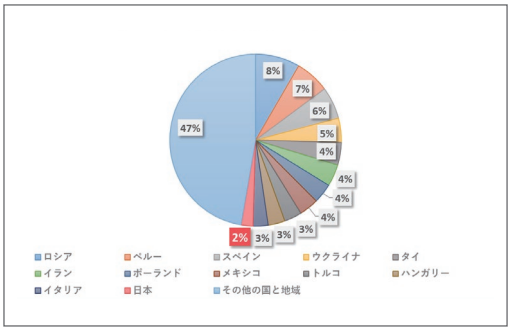
2018年上半期において、VBA/TrojanDownloaderが世界で最も多く検出されたのは日本です。世界全体の検出数のうち34%を日本が占めています。日本において、メールおよびMicrosoft Word文書もしくはMicrosoft Excel文書が多く使われていることが背景にあると考えられます。このような通常の業務で用いられるアプリケーション(ファイル形式)を悪用した攻撃は2017年以前から継続して確認されています。

② JS/CoinMiner

JS/CoinMinerはJavaScriptで記述されたマイニングスクリプトです。マイニングスクリプトは、PCのハードウェアリソース(CPUやGPU)を使って、仮想通貨をマイニング(採掘)します。JS/CoinMinerは通常Webブラウザー上でマイニングを実行します。



JS/CoinMinerの国内検出数推移

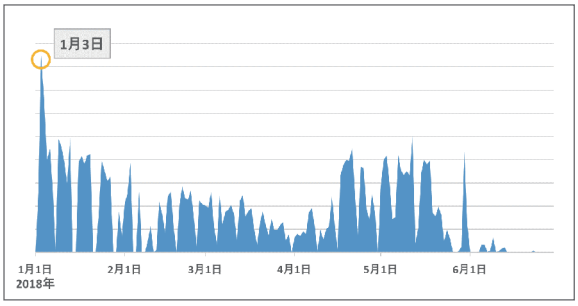


JS/CoinMiner検出数の割合(2018年上半期)

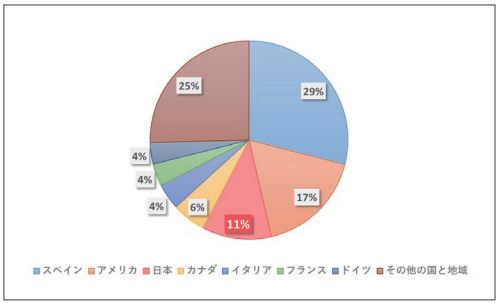
JS/CoinMinerの検出数は、国ごとにあまり大きな差はなく、ほぼすべての国と地域で検出されています。JS/CoinMinerを含むマイニングマルウェア全般については、「2. 仮想通貨を狙う脅威」で詳しくご説明します。

③ HTML/FakeAlert

HTML/FakeAlertは偽の警告文を表示するスクリプトの検出名です。たとえば、「Windowsセキュリティシステムが破損しています」と偽の警告メッセージを表示し、PC修復ツールなどと称したソフトウェアをユーザーに購入させようとします。ユーザーに対する警告メッセージを音声で流すサイトも存在します[2]。

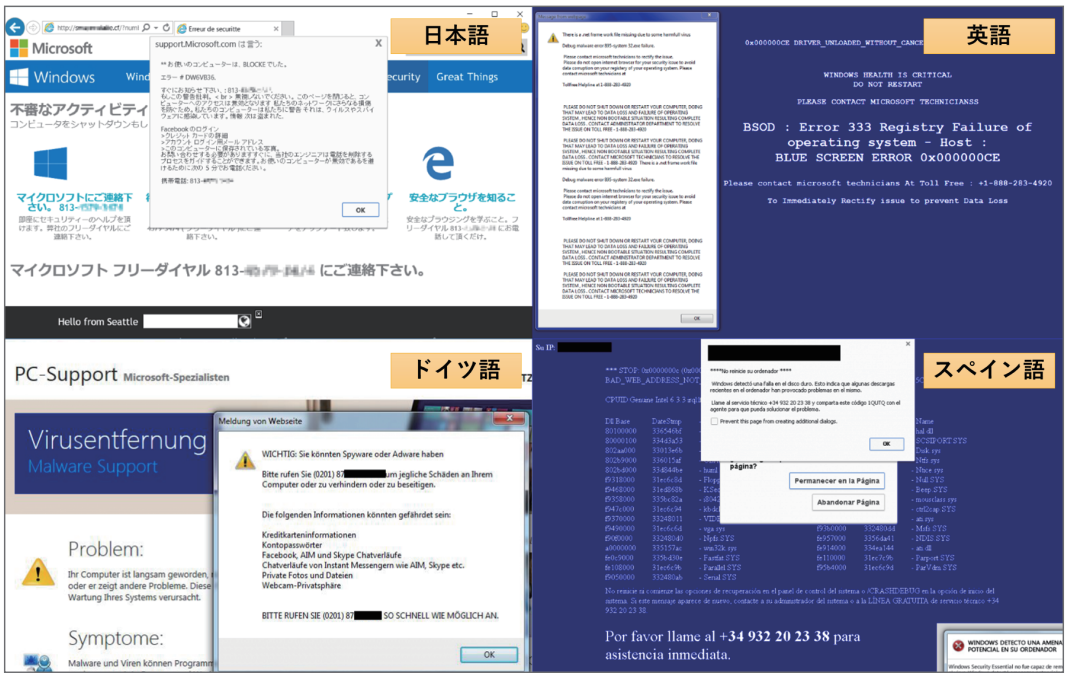


HTML/FakeAlertの国内検出数推移



HTML/FakeAlertの検出数の割合(2018年上半期)

世界で検出されたHTML/FakeAlertのうち、11%を日本が占めています。スペイン、アメリカに次いで多く検出されています。日本を除く検出数上位の国々では、言語構造の似ているゲルマン系の言語(英語、ドイツ語)およびラテン系の言語(スペイン語、イタリア語、フランス語)が多く用いられています。これは詐欺サイトを多言語化する際、攻撃者が自然な文章(あるいは音声)に翻訳できる言語を選んでいることが一因として考えられます。



さまざまな言語で表現された詐欺サイトの例 [3][4][5]

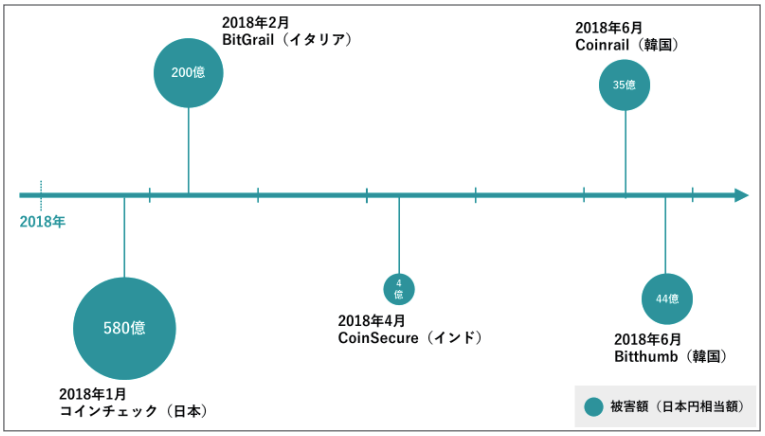
2 仮想通貨を狙う脅威

仮想通貨を狙う脅威

仮想通貨を狙う脅威が世界中で増えています。仮想通貨(暗号通貨)とは、インターネット上で利用される、実物のない通貨のことです。世界中の人と迅速に(数十分の間に)取引を行うことができます。またブロックチェーンと呼ばれる仕組みによって取引の履歴が記録されており、安全性が担保されています。これらの利便性から、仮想通貨の商取引における利用、および投機目的の購入が増加しています。
2017年末、ビットコインをはじめとする仮想通貨の価格が高騰しました。2018年7月現在、ピーク時に対して価格は落ち着いていますが、依然として(2016年以前と比較すると)価格は高い水準にあります。このような価格の高騰を背景に、サイバー攻撃者の関心は仮想通貨に向かっています。仮想通貨をめぐる脅威をいくつかご紹介します。

(1) 仮想通貨取引所に対する攻撃

1つ目にご紹介する脅威は仮想通貨取引所に対する攻撃です。前述したように仮想通貨そのものは非常に信頼性の高い技術を使っていますが、それを取り扱う人、アプリケーション、サーバー等にウィークポイントは存在します。2018年の上半期には、数多くの流出事案が発生しました。

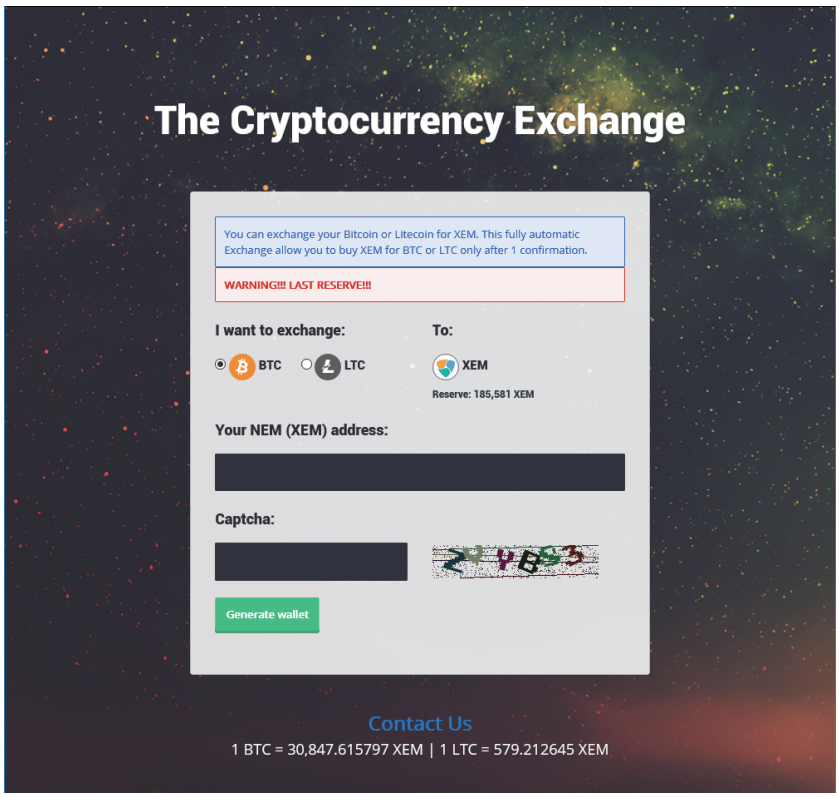


2018年上半期に発生した主な仮想通貨盗難事件 [6][7][8][9]

2018年上半期に発生した中で最も被害額が大きい盗難事件は、コインチェック社から仮想通貨NEMが不正に送金された事件です。外部に不正に送金された仮想通貨は、当時のレートでおよそ580億円に上ります。
コインチェック社は、不正アクセスの原因を従業員端末のマルウェア感染によるものとしています。また、不正送金を防げなかった理由として、仮想通貨をホットウォレット(*)で管理していたことを挙げています[10]。

(*)インターネットに接続された状態のウォレット。対して、インターネットから切り離されたウォレットをコールドウォレットという。

コインチェック社から仮想通貨を盗んだ犯人はその後、資金洗浄を目的としてダークウェブ（Torサイト）に交換所を立ち上げました。同年3月にはすべての盗まれた仮想通貨が不特定多数の相手の手にわたってしまい、現在通貨の追跡は非常に困難な状態です。

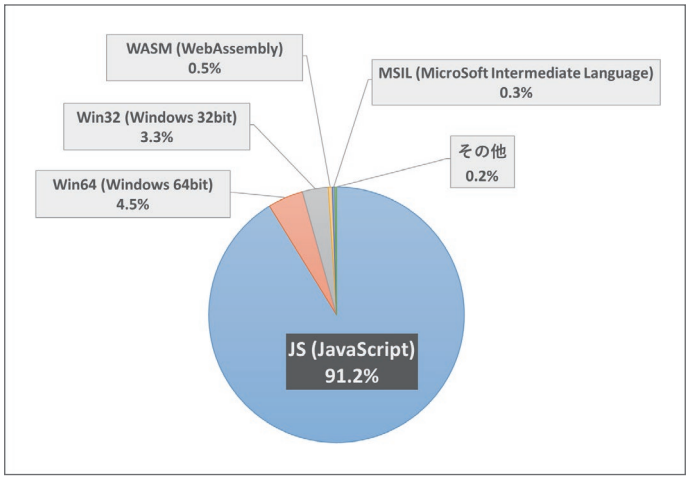


ダークウェブ（Torサイト）の仮想通貨交換所

特定の国や組織の影響を受けない仮想通貨の性質は大きな利点であると同時に、盗まれてしまった場合に取り返すことは困難という問題を抱えています。今回改めて、仮想通貨のリスクが浮き彫りになりました。
取引所の運営者はもちろんのこと、ご自身のウォレットで仮想通貨を管理されている方は仮想通貨の管理には細心の注意を払うようにしましょう。

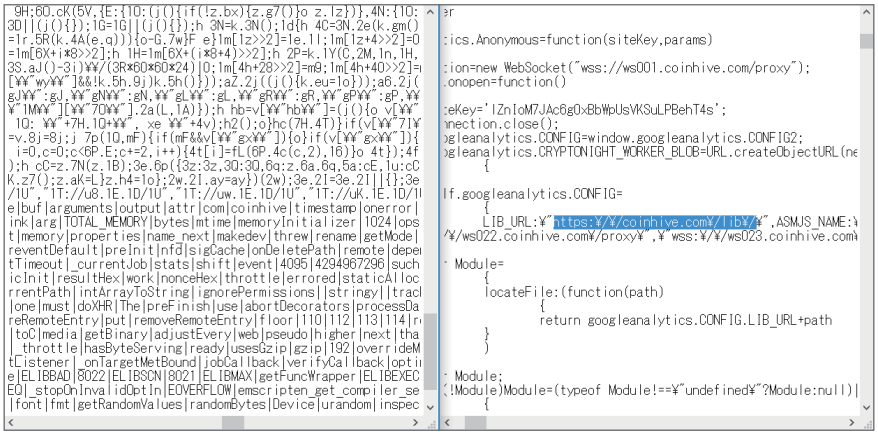
（2）マイニングマルウェア

2つ目にご紹介する脅威はマイニングマルウェアです。
多くの仮想通貨では、一番早く正確に計算できた人に対して、報酬を支払う仕組みが導入されています。このことを、鉱山から金（きん）を採掘することになぞらえて、マイニングと呼びます。他人のCPUやGPUを悪用して、マイニングを行うプログラムをマイニングマルウェアと呼びます。
現在最も多く検出されているマイニングマルウェアはWebブラウザー上で動作するタイプです。
検出されたマイニングマルウェアのうち、90%以上はJavaScript形式（JS/CoinMiner）です。



検出されたマイニングマルウェアのファイル形式別割合(2018年上半期)

検出されたJS/CoinMinerのうち大多数はCoinhiveもしくはCoinhiveを基にしたスクリプトです。Coinhive自体は、Webサイト閲覧者のPCでマイニングを行うことで、Webサイトの運営者が広告の代替となる収益を得るためのサービスです。しかしながら、第三者がWebサイトを改ざんし、Coinhiveを埋め込むことで不正に収益を得る事例が多数確認されています。中には、JavaScriptライブラリのjQueryに偽装しているものや、ブロックフィルターから検出を逃れるため難読化されているものもあります。



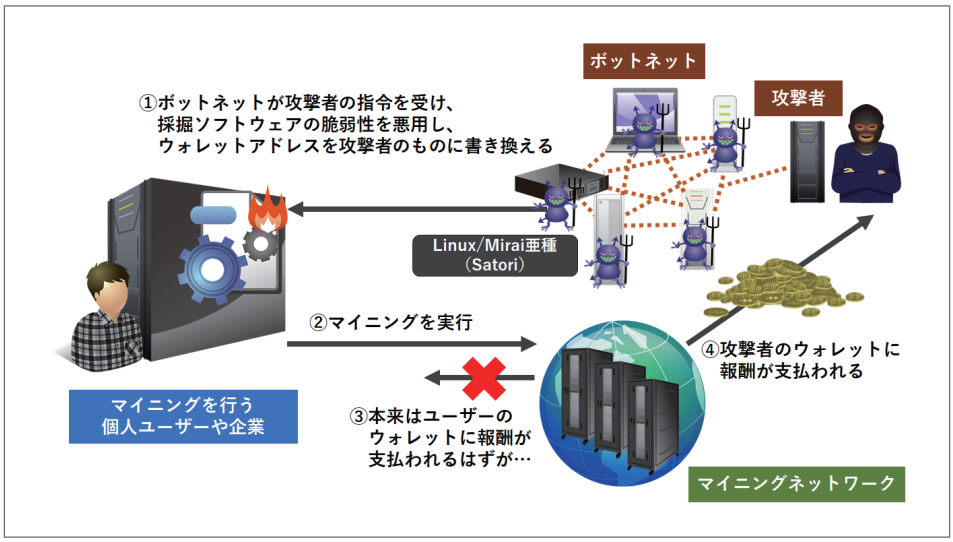
難読化されたマイニングスクリプト(左) / 左のスクリプトの難読化を解除した状態(右)

このようなWebサイトの改ざんは、利用者の信用を失うことになります。
Webサイトを運営されている方は、被害に遭わないためにもサーバーのセキュリティ対策やログの監視方法を今一度見直してください。

(3) ウォレットアドレスを書き換えるマルウェア

3つ目の脅威は、仮想通貨の採掘者を狙う攻撃です。マイニングソフトウェアのウォレットアドレス(採掘された仮想通貨の送信先)を攻撃者のアドレスに書き換えて、収益を横取りする事例を確認しています。

2018年1月にはSatori Coin Robber(ESET検出名:Linux/Mirai)と呼ばれるマルウェアが発見されました[11]。このマルウェアはIoTボットネットマルウェアMiraiの亜種で、Ethereumを採掘するソフトウェアClaymoreの脆弱性を悪用し、設定ファイルのウォレットアドレスを書き換えます。
警察庁から発表された資料によると2018年1月8日以降Claymoreの管理ポートに対するアクセスが増加しています[12]。



ウォレットアドレスを書き換えるマルウェアの動作の流れ

今後、仮想通貨の利用者増加に伴い、仮想通貨を狙った攻撃も増加すると考えられます。仮想通貨は革新的で優れた技術ではありますが、利用者は背後に潜む危険をよく理解する必要があります。

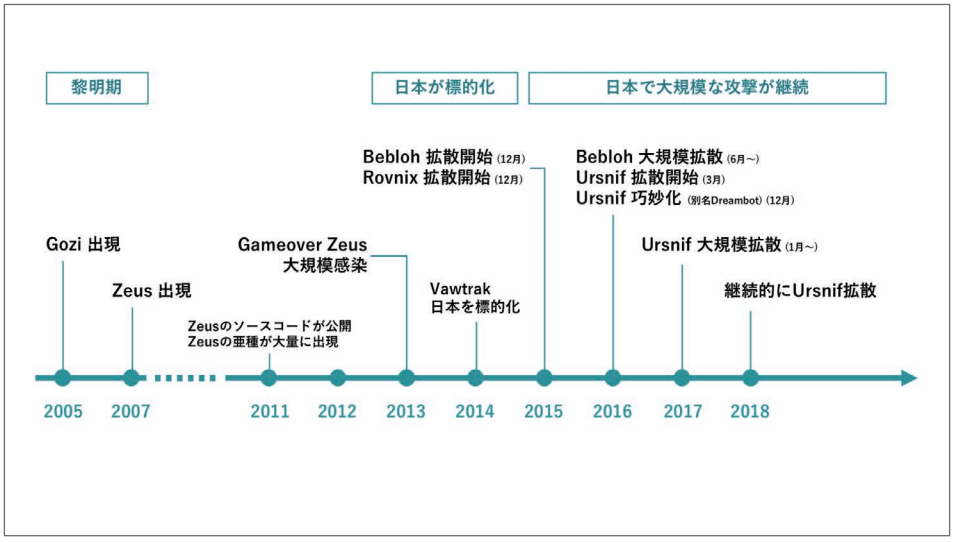
3 インターネットバンキングを狙う脅威

インターネットバンキングを狙う脅威

バンキングマルウェア概況

バンキングマルウェアは、インターネットバンキングの認証情報（ユーザーIDやパスワード等）やクレジットカード情報を窃取します。感染した場合、銀行口座からの不正送金やクレジットカードの不正利用などの被害に遭う可能性があり、警視庁や日本サイバー犯罪対策センターをはじめ他のベンダーからも多くの注意喚起が出ています[13]。

国内では2000年代後半以降 ZeuS（別名：ZBOT）をはじめとするバンキングマルウェアが次々に流行しました。特に2016年以降はRovnix、Bebloh（別名：URLZone, Shiotob）、Ursnif（別名：Gozi, Papras, Snifula, DreamBot）といったバンキングマルウェアの活動が多く観測されています。2018年上半期は、前年ほどではないものの、Ursnif感染を狙ったばらまき型メール攻撃が多く観測されました。

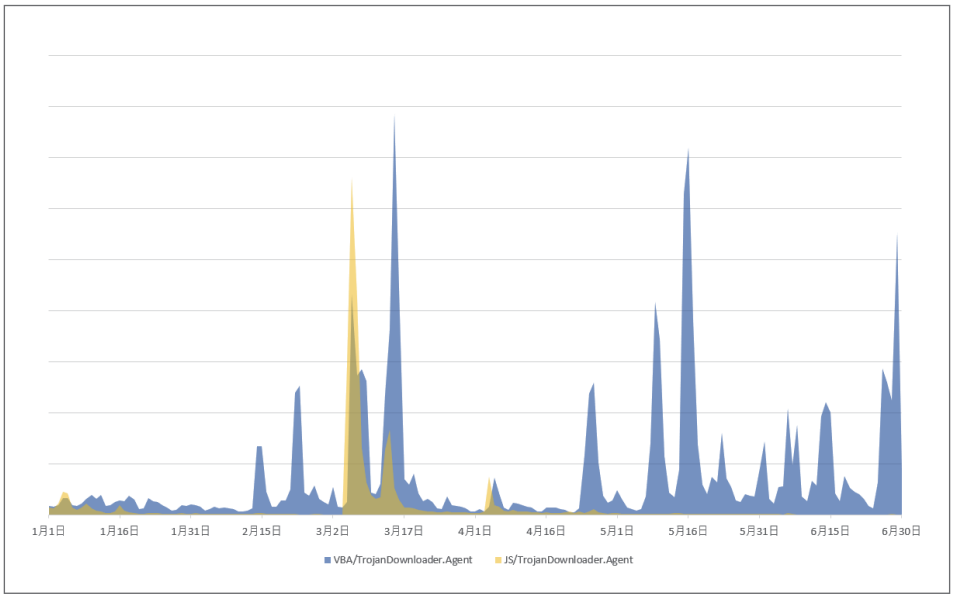


国内の主なバンキングマルウェア関連イベント

2018年上半期に多く観測されたUrsnifの感染手法では、まず数KB～数十KBのダウンローダーを実行させようとします。ダウンローダーを実行すると、いくつかの段階を経てUrsnif本体がダウンロード・実行されます。ダウンローダーには、大きく分けてMicrosoft Officeのマクロを悪用したもの（VBA/TrojanDownloader.Agent）とスクリプトによるもの（JS/TrojanDownloader.Agent）が存在していました。

「VBA/TrojanDownloader.Agent」の検出は3月15日にピークを迎え、その後4月は落ち着いていましたが5月に入ると再度活発化し、5月15日、6月29日に多数の検出がみられました。

一方、「JS/ TrojanDownloader.Agent」の検出は3月5日をピークに、その後は急減少しています。



VBA/TrojanDownloader.AgentおよびJS/TrojanDownloader.Agentの
国内検出数推移(2018年1月−6月)

全体的な傾向として、土日は検出数が少なく、水曜日前後に検出数のピークが現れる傾向があります。 また、日本の年末年始や、火曜〜木曜日に重なる祝日(春分の日、ゴールデンウィーク)に検出数のピークは見られていません。 ここから、攻撃者について、法人を主な標的としている様子がうかがえます。また、攻撃者が日本のカレンダーに従っている、あるいは日本の休日事情を把握している可能性もあります。

Ursnifの攻撃手法

■ Ursnifの侵入経路

2018年上半期に観測されたUrsnif感染を狙ったメール攻撃には、大きく分けて以下の2種類のパターンがありました。

（1） ダウンローダーがメールに添付されているパターン

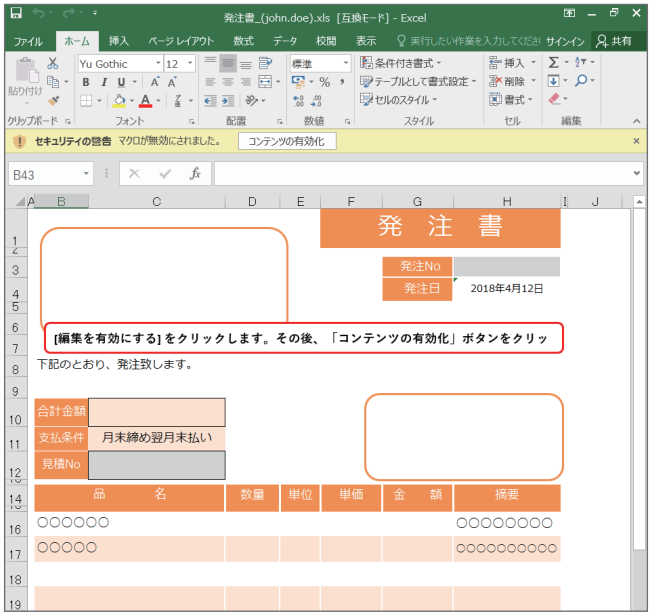
（2） 本文中にダウンローダーのダウンロードURLを記載しているパターン

それぞれのパターンについて説明します。

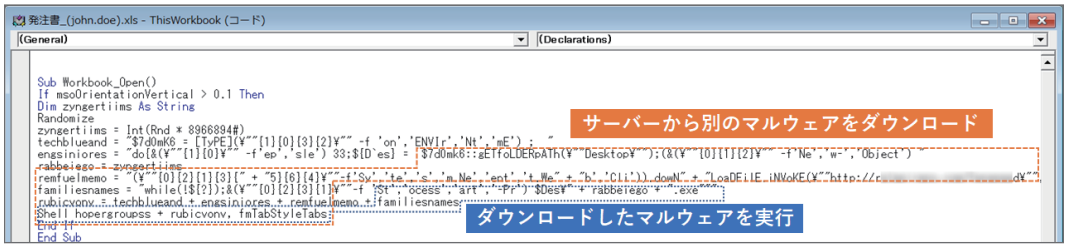
（1）ダウンローダーがメールに添付されているパターン

このパターンでは、Microsoft Officeのマクロ機能を悪用したダウンローダーが主に用いられていました。ESET製品では、このダウンローダーを VBA/TrojanDownloader.Agent として検出します。

VBA/TrojanDownloader.Agent のファイル形式はMicrosoft Word文書やMicrosoft Excel文書です。ファイルを開きマクロを有効化すると、VBA（Visual Basic for Applications）で記述されたコードが最終的にUrsnifをダウンロード・実行します。



メールに添付された悪性のMicrosoft Excelファイル（VBA/TrojanDownloader.Agent）

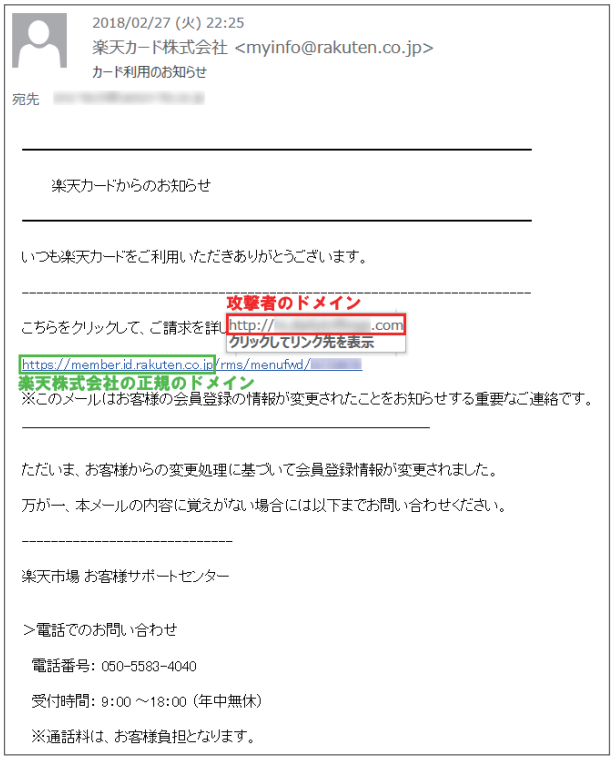


悪性のMicrosoft Excelファイルに埋め込まれたVBAのコード

（2）本文中にダウンローダーのダウンロードURLを記載しているパターン

このパターンでは、Windowsのスクリプト実行機能 WSH（Windows Script Host）を悪用した、JavaScriptで記述されたダウンローダーが主に用いられていました。ESET製品では、このダウンローダーを JS/TrojanDownloader.Agent として検出します。

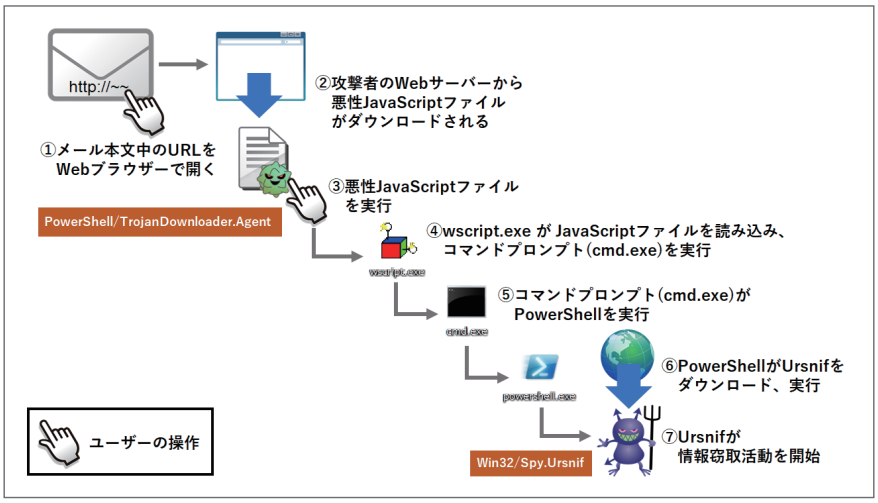
以下の画像は楽天カードを騙ったメールの例です。



楽天カードを騙ったメールの例

本文中のリンクは、一見すると楽天株式会社の正規のドメインのように見えますが、見た目に反して、実際には攻撃者のドメインにアクセスするよう設定されています。

このリンクをクリックすると、悪意あるJavaScriptファイルがダウンロードされます。そしてそのJavaScriptファイルを実行すると、Ursnifに感染します。



バンキングマルウェア「Ursnif」感染までの流れ

侵入に使われている3つのアプリケーション（wscript.exe、cmd.exe、powershell.exe）はいずれもWindowsに標準で搭載されている正規のアプリケーションです。Windows PowerShell はコマンドプロンプトより高度な処理を行うことができるため、悪用される事例が増加しています。

■ Ursnifが窃取する情報

Ursnif本体は、ESET製品では Win32/Spy.Ursnif などの名称で検出されます。
Ursnifは以下に示す情報の窃取活動を行います。

- キーボードの入力内容
- スクリーンショット
- Webカメラの動画や音声
- インターネットバンキングサイト、クレジットカードの会員サイト、ECサイト、仮想通貨取引サイトの認証情報（ID、パスワードなど）
- デジタル証明書
- ブラウザーのCookie

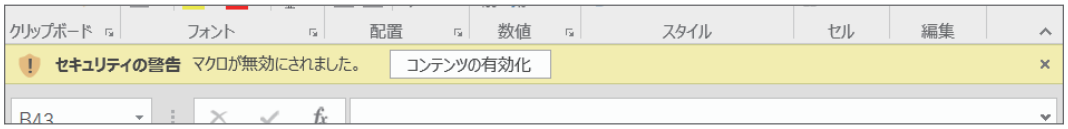
Ursnifへの対処

バンキングマルウェアに感染した場合、感染が発生した時点から発覚、対処までの短時間に不正送金被害に遭う可能性があり、感染の予防（感染リスクの軽減）が重要になります。

Ursnifをはじめとするバンキングマルウェアは、ばらまき型メール攻撃によって感染する事例を多く確認しています。ばらまき型メール攻撃全般への対策を実施することで、Ursnifへの感染リスクを軽減することが期待できます。

■ Microsoft Officeのマクロ機能を制限する

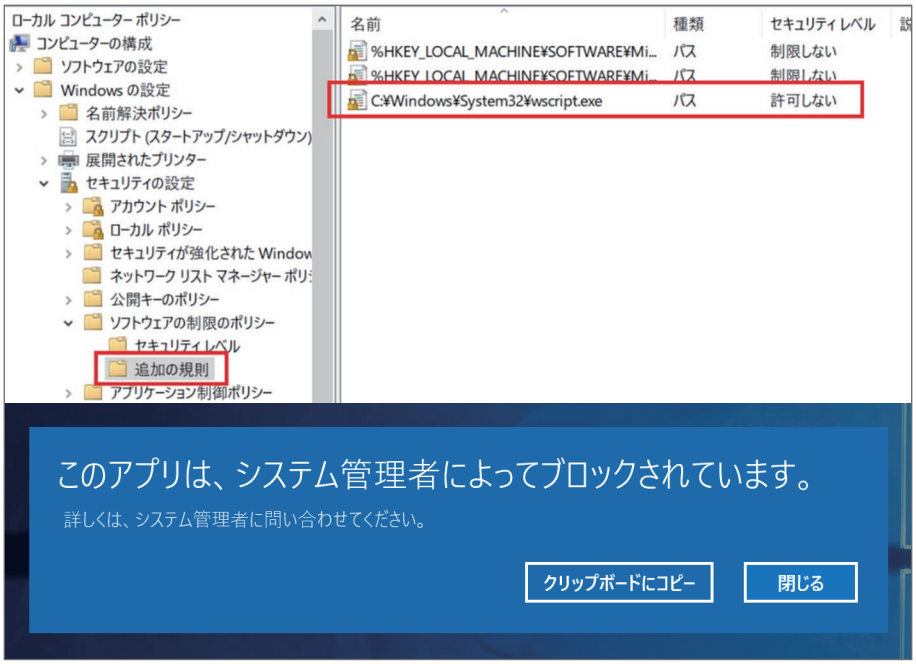
Microsoft Officeの標準設定では、マクロを含むファイルを開いた際に警告が表示されます。また、インターネットから取得したファイルを開いたときは保護ビューでファイルが開かれます[14]。もしこれらの機能を無効に設定されている場合は、Microsoft Officeのマクロ機能は無効、もしくは警告を表示するよう設定し、加えて保護モードを有効に設定しておくことをお勧めします。



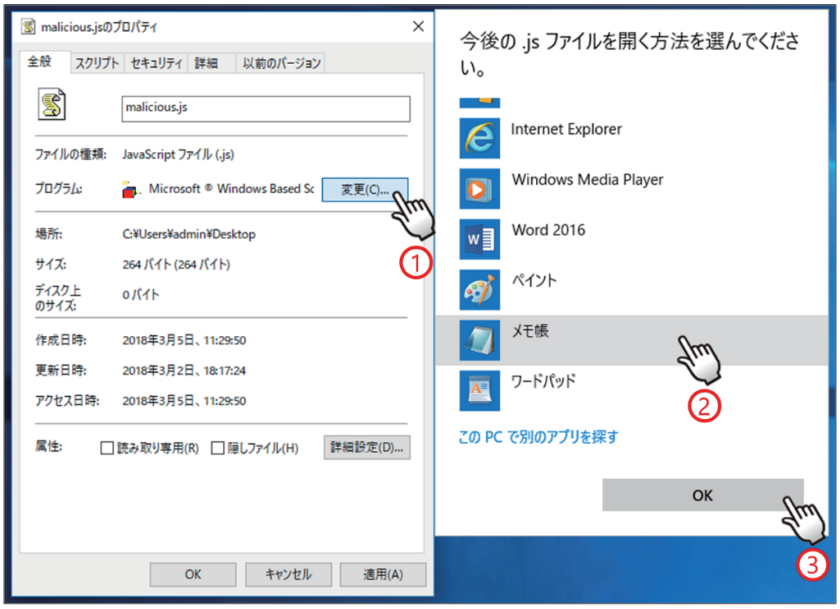
マクロを含むファイルを開いた際の警告

■ WSHによるJavaScript/VBScriptファイルの実行を制限する

Microsoft Officeのマクロ機能と並びよく悪用されるのが、JavaScriptファイル（拡張子.jsまたは.jse）やVBScriptファイル（拡張子.vbsまたは.vbe）です。グループポリシー（ソフトウェアの制限やAppLocker）でwscript.exeやスクリプトファイルの実行を制限する、あるいはスクリプトファイルを開く既定のアプリケーションをメモ帳などのテキストエディタに変更しておくことで、それらのスクリプトが実行されなくなります。Windows上でスクリプトファイルを実行する必要がない場合は、上記のように設定を変更されることを推奨します。
この設定は、Webブラウザー上におけるJavaScriptの実行には影響しません。



グループポリシーによるwscript.exeの実行制限（例）



既定のアプリケーションの設定変更

他にも、オンラインバンキングを利用するPCではメール送受信を行わない、オンラインバンキング以外のドメインへの通信をネットワーク機器で遮断するなどといった対策も有効です。

なお、Ursnifにはスクリーンショットを取得する機能が搭載されているため、ソフトウェアキーボードを利用している場合でも認証情報を窃取される可能性があります。また、ばらまき型メールのほかに、脆弱性を利用したWebページ経由での感染も確認しています。一つの対策に頼らず、複数の対策を実施することが重要です。

バンキングマルウェアの今後

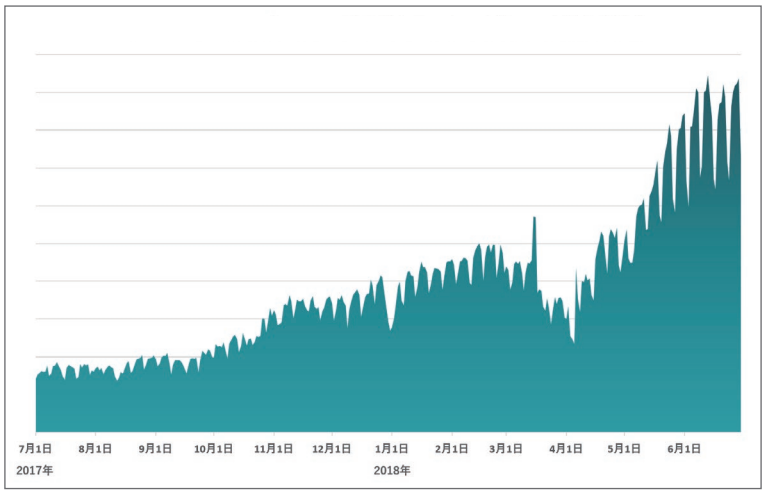
バンキングマルウェアに感染させようとする攻撃は2018年7月現在も引き続き観測されており、今後も続くと考えられます。
また、2018年7月にはVBScriptとPDFを悪用する方法も観測されており、攻撃手法にも変化が見られていますので引き続き注意が必要です。
常に最新の脅威情報をキャッチし、都度対策を講じていくことが重要です。

4 WindowsプロトコルSMBの脆弱性を悪用する攻撃

Windowsプロトコル SMBの脆弱性を悪用する攻撃

WindowsのSMB(Server Message Block:ファイル共有などに使われる通信プロトコル)に関する脆弱性(以下、本脆弱性)を悪用する攻撃が続いています。

本脆弱性に対処するセキュリティ更新プログラムMS17-010は2017年3月の時点で公開されています[15]が、本脆弱性を悪用する攻撃の検出数は増加傾向にあります。

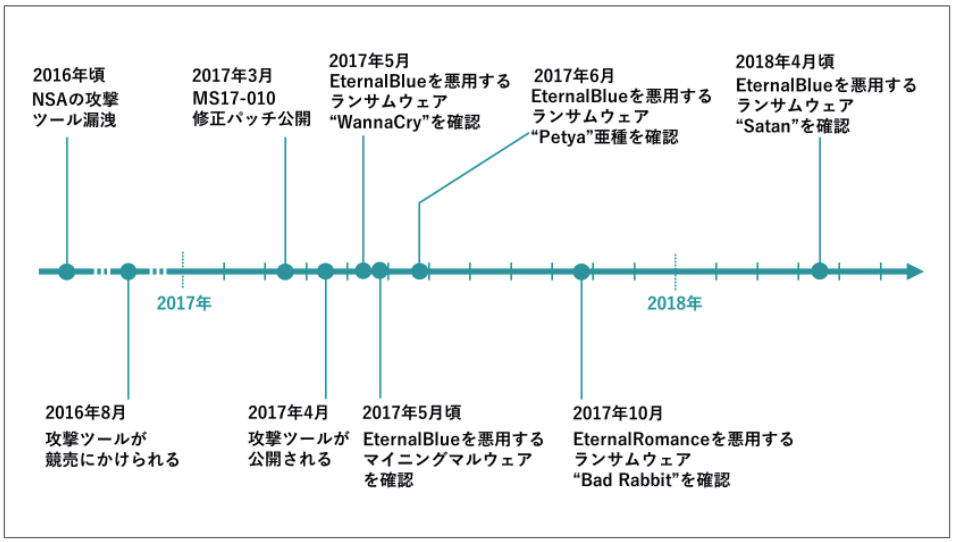


WindowsのSMBプロトコル脆弱性を悪用する攻撃の国内検出数推移(*)
(*)攻撃活動のほかに、脆弱性を検査する目的や研究目的で使用・検出されたものも含まれています。

インターネットに接続されている機器の検索エンジンShodanによると、SMBが利用する445番ポートが開放されている国内のWindows端末は80,000台以上あります[16](2018年8月3日現在)。これらの端末に更新プログラムが適用されていない場合、脆弱性を悪用する攻撃の対象となります。

445番ポートが開放されているWindows端末(出典:Shodan)

本脆弱性を悪用するツール（もしくは機能）として、EternalBlue（ESET検出名：SMB/Exploit.EternalBlue）とDoublePulsar（ESET検出名：SMB/Exploit.DoublePulsar）がよく知られています。
事の発端は2016年、NSA（アメリカ国家安全保障局）が開発したとされる脆弱性攻撃ツール群（EternalBlueおよびDoublePulsarが含まれる）が、Shadow Brokersというハッカー集団によって盗まれた事にあります。
2017年4月には攻撃ツールに関する情報が広く一般に公開され、5月にはWannaCry（ESET検出名：Win32/Filecoder.WannaCryptor）と呼ばれるランサムウェアが大流行します。ほどなくしてWannaCryの脅威は収まりましたが、本脆弱性を悪用する攻撃はその後も続いています。



WindowsのSMBプロトコル脆弱性に関する出来事 [17] [18] [19]

2018年6月には、IoTのWindows端末（Windows Embedded OSが搭載された端末）もDoublePulsarの影響を受けることが研究者によって示されました[20]。今後も、本脆弱性に対する攻撃は続くと予想されます。

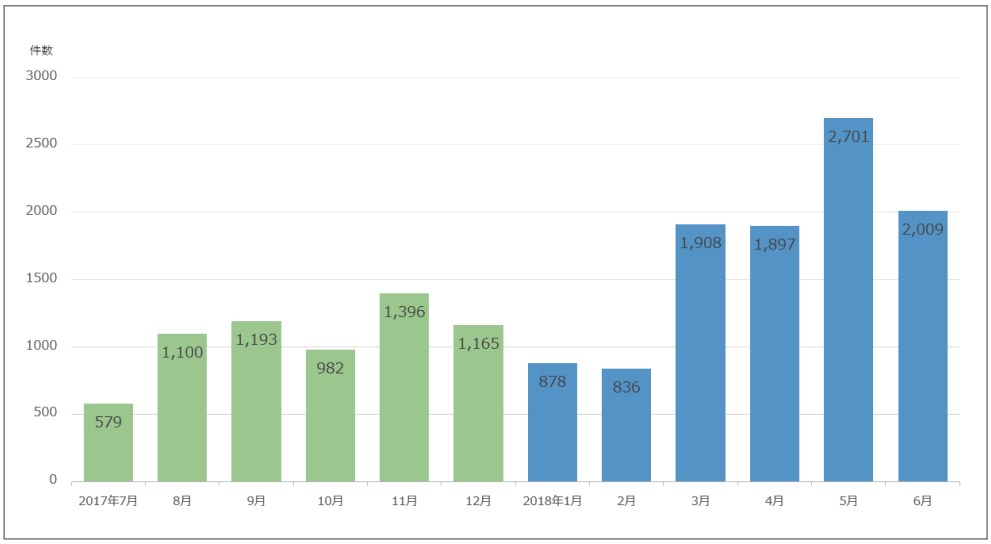
今一度、攻撃の影響を受けるすべてのWindows OSに修正プログラム（MS17-010）が適用されているか確認されることを推奨します。

5 サイバー犯罪のためのサービス “Crime as a Service”

サイバー犯罪のためのサービス “Crime as a Service”

今やインターネットは、オンラインショッピングや航空券の予約、SNSを利用したメッセージや写真の共有など、私たちの生活にとってなくてはならない生活基盤となっています。
その一方で、サイバー犯罪は増加傾向にあり、フィッシングメールやランサムウェアなど、さまざまな方法で攻撃が行われています。

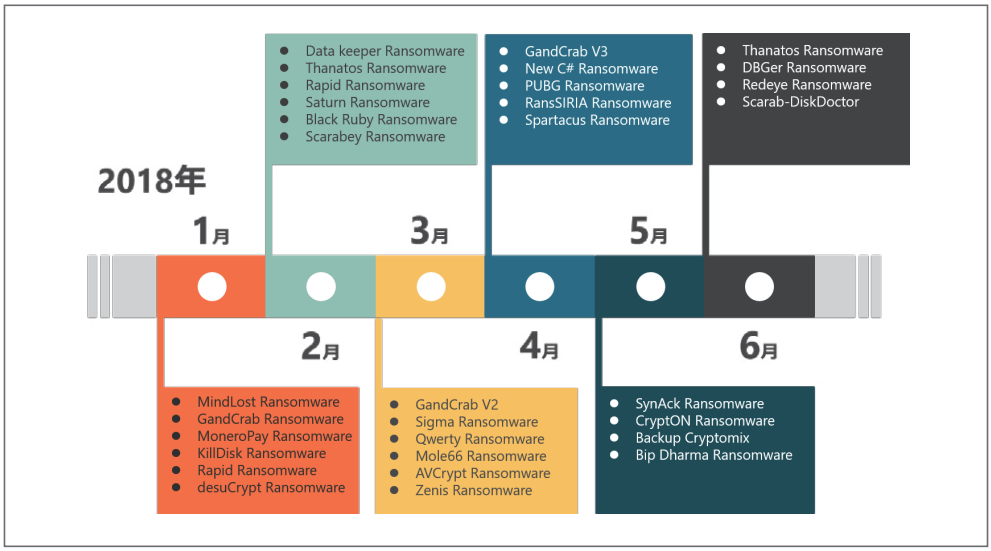
以下のグラフは、フィッシング対策協議会が発表したフィッシングの報告件数(2017年7月～2018年6月)です。



フィッシング報告件数
出典:フィッシング対策協議会 2018/06フィッシング報告状況 フィッシング報告件数 [21]

2018年6月のフィッシング報告件数は2,009件で、5月に比べ692件減少したものの、昨年に比べ増加傾向にあります。

また、2016年から2017年にかけて猛威を振るったランサムウェアは、減少していると言われているものの、以下の図のように依然として新しいランサムウェアが定期的に発見されています。



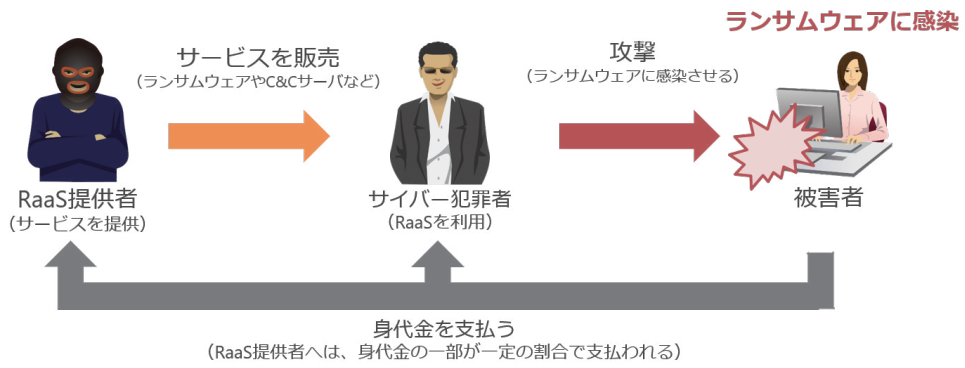
2018年1月から6月に新しく見つかったランサムウェア

このように、フィッシングメールの増加や新しいランサムウェアが継続して見つかっている要因の1つとして「Crime as a Service(CaaS)」の存在が挙げられます。

CaaSは、サイバー犯罪に使われるマルウェアやC&Cサーバーを「必要なときに」、「必要な分だけ」、「サイバー犯罪者のために」提供するサービスです。

CaaSには、「Ransom as a Service(RaaS)」と呼ばれるランサムウェア(ファイルを暗号化し身代金を要求するマルウェア)を販売するサービスや「Phishing as a Service(PhaaS)」と呼ばれるアカウント情報(ユーザー名、パスワードなど)を盗むための偽Webサイトを簡単に作成できるサービス、「DDoS as a Service(DaaS)」と呼ばれるDDoS攻撃を行うためのボットネットを販売するサービスなどがあります。

たとえば、RaaSは、ランサムウェアを感染させ身代金を得ようとするサイバー犯罪者に対して、感染に必要なプログラム(ランサムウェア本体やダウンローダー、C&Cサーバーなど)を販売しています。サイバー犯罪者は、このRaaSサイトからサービスを購入することで、サイバー犯罪者自身がランサムウェアを開発する必要がなく、容易に攻撃を行うことが可能です。



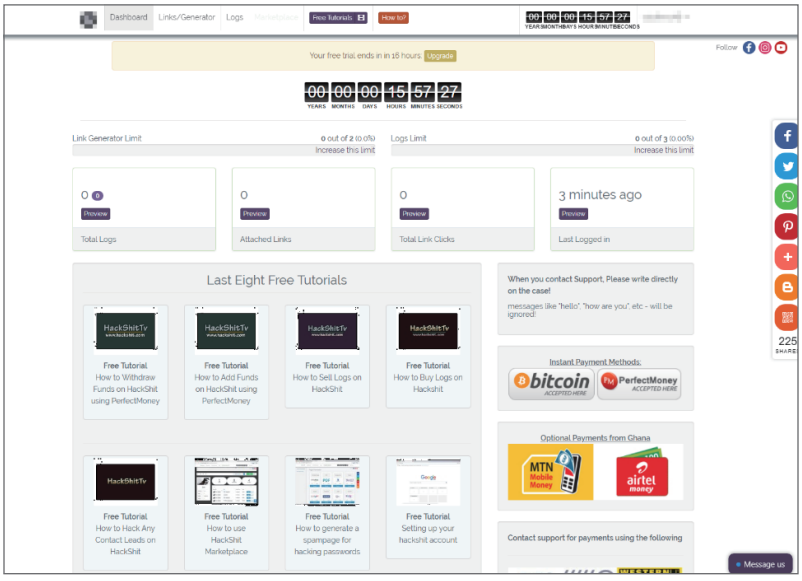
RaaSの概要

また、PhaaSでは、AppleやMicrosoftなどのアカウント情報（ユーザー名、パスワード）を騙し取ろうとするサイバー犯罪者に対して、実在する企業やサービスに見せかけた偽のWebサイト（偽のログイン画面など）を簡単に作成するプログラムやサーバーなどを販売しています。
サイバー犯罪者は、このPhaaSサイトで実在する企業やサービスに見せかけた偽のWebサイトを作成し、フィッシングメールなどを使って、偽のWebサイトへ誘導することで、簡単にアカウント情報（ユーザー名やパスワードなど）を盗み取ることが可能です。また、盗み取ったアカウントは、PhaaSサイト上で販売することができます。

従来、マルウェアの作成やフィッシングサイトの構築を行うには、プログラムやネットワークといった専門的な知識が必要でした。しかし、CaaSからマルウェアやフィッシングサイト、ボットネットを購入することで、誰でも簡単に攻撃を行うことが可能です。CaaSは、今までサイバー犯罪を行う上で障壁となっていた技術的な壁を下げる役割を果たしています。

このようなランサムウェアやフィッシングサイトをサービスとして販売するCaaSサイトは、ダークウェブやディープウェブ上に多数存在しています。

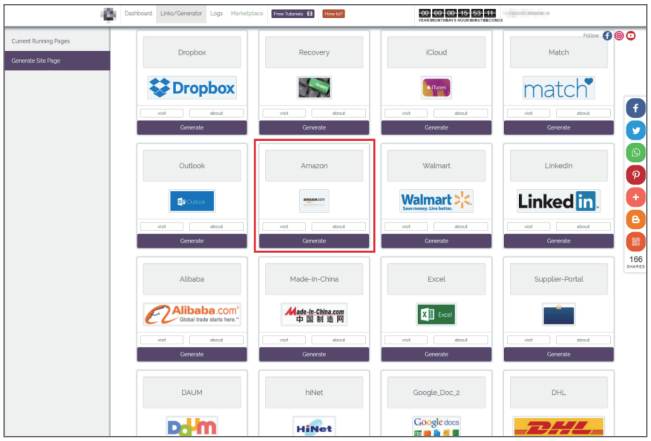
以下の画面は、AppleやGoogleのアカウント情報（ユーザー名・パスワード）を騙し取るWebサイト（フィッシングサイト）を簡単に作成することができるPhaaSサイトです。このPhaaSサイトは昨年発見され、現在（2018年7月現在）でもサービスを提供しています。



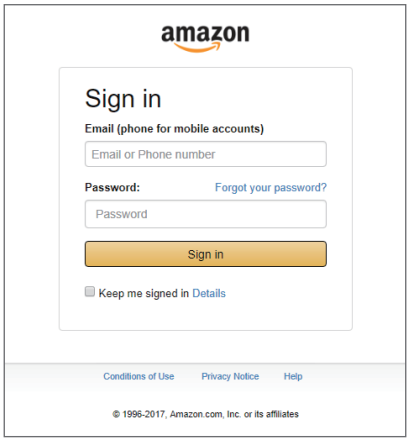
PhaaSサイトの設定画面

このPhaaSサイトの特徴は、AppleやMicrosoftなどのアカウント情報(ユーザー名、パスワード)を騙し取る偽のログインサイトを簡単に作成できる点です。
サイバー犯罪者は、PhaaSサイトの設定画面からボタンを数回クリックするだけで、実在の企業を装った偽のログインサイトを作成できます。

たとえば、サイバー犯罪者がアカウント情報(ユーザー名、パスワード)を盗み取るためにAmazonのログイン画面を装った偽のログインサイトを作成したい場合、PhaaSの設定画面にあるフィッシングサイトの一覧から作成したい企業やサービスの項目を選択します。そして、[作成]ボタンをクリックするだけで、以下のような本物そっくりのログインサイトを簡単に作成することができます。



作成可能な偽ログインサイト(フィッシングサイト)の一覧画面



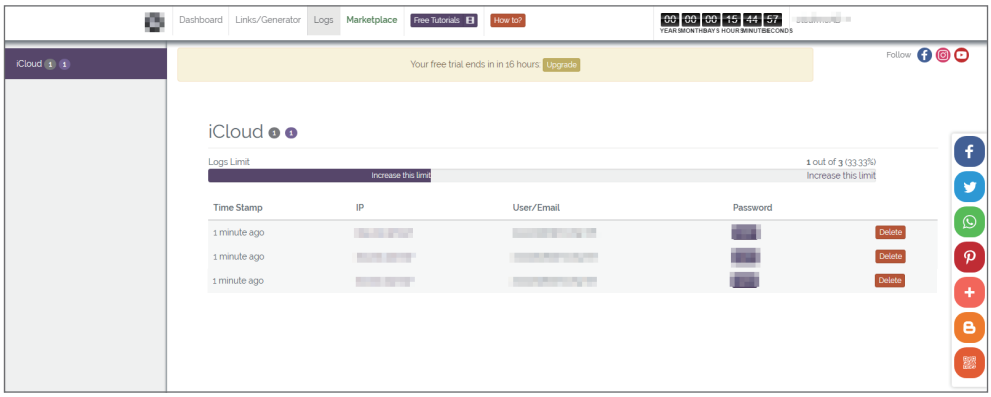
PhaaSサイトで作成したAmazonの
偽ログインサイト(フィッシングサイト)画面

現在、このPhaaSサイトで作成できる偽のログインサイトは、AppleやMicrosoft、Google、Amazonなど約50社以上に上ります。

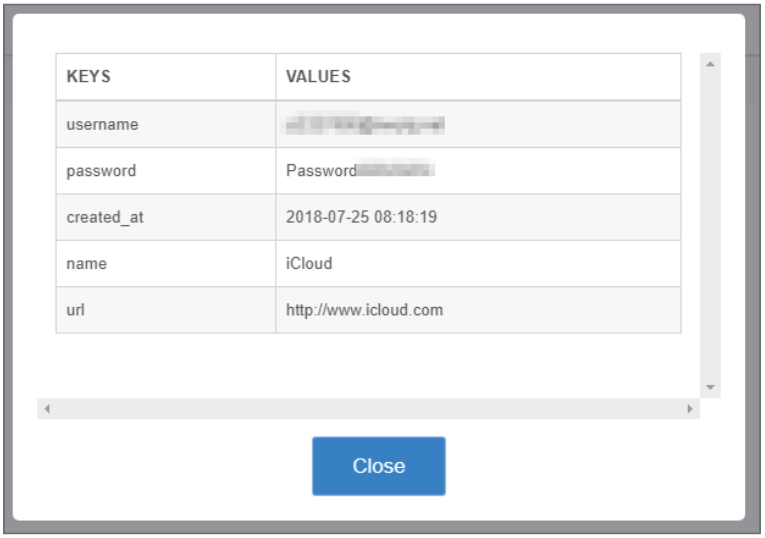
このPhaaSサイトで作成された偽のログインサイトは、PhaaSが提供するクラウドサーバー上に設置され、フィッシングメールの誘導先サイトとして使われます。

たとえば、ショッピングサイトや銀行などを装った電子メールに、このPhaaSサイトから作成した偽ログインサイトのURLを記載し、攻撃対象へ送信します。
攻撃対象(フィッシングメールの受信者)が、本当の企業から送信されたメールだと勘違いし、電子メールに記載されたURLを開くと、PhaaSサイトで作成した偽のログイン画面が表示されます。
そして、表示されたログイン画面にユーザー名・パスワードを入力すると、ユーザー名・パスワードなどのアカウント情報がPhaaSサイトのサーバーに記録されます。
サーバーに記録されたアカウント情報(ユーザー名、パスワード)は、PhaaSの管理画面から簡単に閲覧できるため、このアカウント情報を使って他の攻撃(アカウントの乗っ取りなど)に利用できます。

このPhaaSサイトでは、盗み取ったアカウント情報は、以下のような画面で確認することができます。

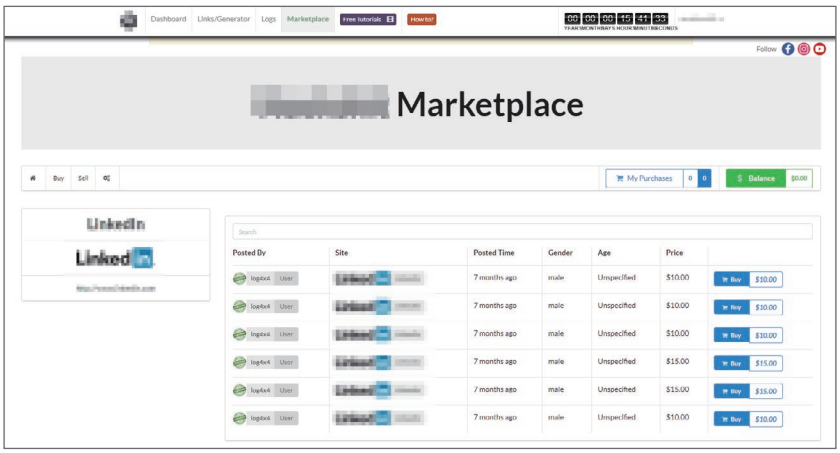


偽のWebサイトから収集したアカウント情報の一覧画面



偽のWebサイトから収集したアカウント情報の詳細画面

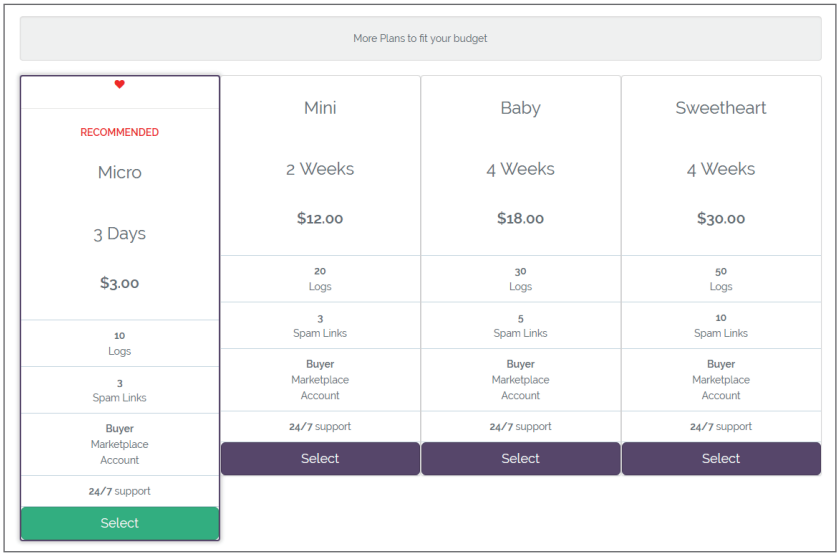
また、このPhaaSサイトでは、盗み取ったアカウント情報を売買しやすいように、PhaaSサイト内にアカウント情報を売買する機能も実装されています。
たとえば、以下の画面では、PhaaSサイトを使って盗み取ったソーシャルネットワークサービスのアカウント情報が10ドルで販売されています。PhaaS利用者（サイバー犯罪者）は、このようなサービスを利用して盗みとったアカウント情報をビットコインなどのお金に換金することができます。



PhaaSサイトで売り買いされているアカウント情報

このようにPhaaSサイトでは、偽Webサイトの作成から盗み取ったアカウント情報の管理、販売といったサイバー犯罪者が犯罪を行う上で必要な機能がサービスとして提供されています。

また、PhaaSサイトを利用する費用の面でも、工夫が行われています。
このPhaaSサイトの利用金額は、8つのプランに分かれており、プランごとに利用できる期間や偽サイトの作成数、騙し取ったアカウント情報（パスワードなど）を記録できる数などが異なります。
たとえば、最小のプラン（Micro）では3ドルで3日間PhaaSサイトを利用できますが、偽サイトの作成は3つ、アカウント情報（ユーザー名、パスワードなど）の記録は10アカウントまでに制限されています。
一方、最大のプラン（Master）では、250ドルで3か月間PhaaSサイトを利用でき、偽サイトの作成は10,000個、アカウント情報は無制限で記録することができます。



PhaaSサイトの料金表

そのため、サイバー犯罪者は、自身の利用目的に合ったPhaaSを購入することができます。

以上のようにPhaaSサイトでは、サイバー犯罪を行う上で必要な機能が実装されており、複数のサービスメニューから自身にあったメニューを選択することができます。また、プログラミングなどの特別な技術を必要とせず、比較的簡単に利用できることから犯罪者にとって、とても魅力的なサービスと言えます。

今回は、PhaaSを中心にCaaSをご紹介しましたが、ダークウェブやディープウェブ上には、ランサムウェアを販売するRaaS（弊社マルウェアレポート2018年5月で紹介[22]）やDaaSなどのサービスが多数存在しており、頻繁に機能追加や改善が行われています。
そのため、CaaSは、今後も引き続き、新しい機能が追加され、サイバー犯罪者に利用されるものと予想しています。

当然ながら、正当な理由なしにマルウェアを作成・保管する行為やアカウント情報を盗み出す行為は犯罪です。興味本位でこのようなサービスを利用されることがないようご注意ください。
また、今回ご紹介したPhaaSなどを使ったフィッシングの被害に遭わないためには、以下のような対策を行うことが重要です。

- 電子メール本文のリンクはクリックしない
- IDやパスワードを入力する前にURLを確認する
- パソコンやモバイル端末にウイルス対策ソフトを導入する
- OSやソフトウェアに最新の更新プログラムを適用する
- フィッシング協議会などのサイトを定期的に閲覧し、フィッシング詐欺の手口を確認する
- 少しでもおかしいと感じたらサービス事業者へ問い合わせる

もし、被害に遭った場合でも、落ち着いて行動し、サービス事業者への連絡やアカウントの停止などを速やかに行ってください。また、少しでも不明な点がある場合は、各都道府県の警察に設置されているサイバー犯罪相談窓口に相談することをお勧めします。

引用・出典元

1 | ランサムウェアのダウンローダーを数多く確認 | キヤノンITソリューションズ
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1712.html#anc_03

2 | Microsoftの技術サポートを装った詐欺サイト | キヤノンITソリューションズ
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1707.html#anc_03

3 | Support Scam – was Chiptuning mit Microsoft zu tun hat | ESET
https://www.welivesecurity.com/deutsch/2016/04/06/support-scam-chiptuning-mit-microsoft-zu-tun-hat/

4 | Tech Support Scams: Top of the Pop-Ups | ESET
https://www.welivesecurity.com/2015/10/07/tech-support-scams-top-pop-ups/

5 | Support scams now reign in Spain | ESET
https://www.welivesecurity.com/2017/02/20/support-scams-now-reign-spain/

6 | コインチェック、580億円相当の仮想通貨「NEM」なぜ消失 | ITmedia
http://www.itmedia.co.jp/news/articles/1801/27/news017.html

7 | Coinsecure, not so secure: Millions in cryptocurrency stolen, CSO blamed | ZDNet
https://www.zdnet.com/article/coinsecure-not-so-secure-millions-in-cryptocurrency-stolen-cso-branded-as-thief/

8 | イタリアの取引所から約200億円分の仮想通貨「Nano」流出　「全額補償は不可能」とCEO | ITmedia
http://www.itmedia.co.jp/news/articles/1802/13/news050.html

9 | 韓国の世界6位の仮想通貨取引所でハッキング、35億円流出 | Forbes JAPAN
https://forbesjapan.com/articles/detail/21698

10 | 仮想通貨NEMの不正送金に関するご報告と対応について | Coincheck
https://corporate.coincheck.com/2018/03/08/46.html

11 | Art of Steal: Satori Variant is Robbing ETH BitCoin by Replacing Wallet Address | Qihoo 360 Technology
http://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/

12 | 仮想通貨採掘ソフトウェア「Claymore（クレイモア）」を標的としたアクセスの増加等について | 警察庁
https://www.npa.go.jp/cyberpolice/detect/pdf/20180312.pdf

13 | 不正送金等の犯罪被害につながるメールに注意 | JC3 日本サイバー犯罪対策センター
https://www.jc3.or.jp/topics/virusmail.html

14 | 保護ビューとは | Microsoft
https://support.office.com/ja-jp/article/%E4%BF%9D%E8%AD%B7%E3%83%93%E3%83%A5%E3%83%BC%E3%81%A8%E3%81%AF-d6f09ac7-e6b9-4495-8e43-2bbcdbcb6653

15 | マイクロソフト セキュリティ情報 MS17-010 - 緊急 | Microsoft
https://docs.microsoft.com/ja-jp/security-updates/securitybulletins/2017/ms17-010

16 | Windows operating systems with port 445 open | SHODAN
https://www.shodan.io/report/R0p5ASdT

17 | New WannaCryptor-like ransomware attack hits globally: All you need to know | ESET
https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/

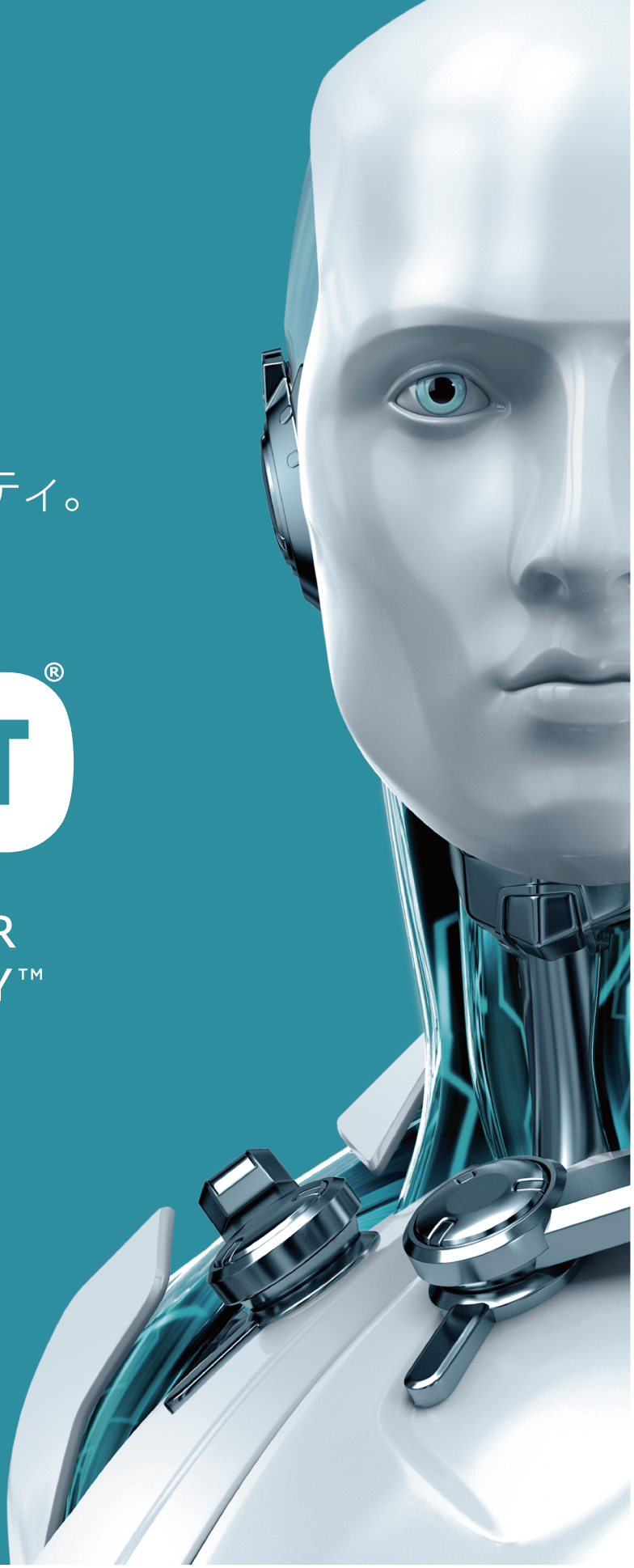
18 | One year later: EternalBlue exploit more popular now than during WannaCryptor outbreak | ESET
https://www.welivesecurity.com/2018/05/10/one-year-later-eternalblue-exploit-wannacryptor/

19 | Bad Rabbit: Not-Petya is back with improved ransomware | ESET
https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/

20 | Patching DoublePulsar to Exploit Windows Embedded Machines | Capt. Meelo
https://capt-meelo.github.io/pentest/2018/06/26/patching-doublepulsar.html

21 | 報告書類 2018/06 フィッシング報告状況 | フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/201806.html

22 | ランサムウェアを販売するRansomware as a Service (RaaS) | キヤノンITソリューションズ
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1805.html#anc_03



強くて軽い。
妥協なきセキュリティ。

ENJOY SAFER TECHNOLOGY™

Canon キヤノン ITソリューションズ株式会社

〒140-8526 東京都品川区東品川2-4-11 TEL. 03-6701-3475

MWJ18081000MUR-621