アンラボ・セキュリティレター

# Press Ahn

2016.4　Vol.28

Mac はマルウェアから 100%安全か

Mac 向けセキュリティソリューション **AhnLab V3 365 Clinic** for Mac

# Mac はマルウェアから 100%安全か

AppleのMacは、多くの人にマルウェアから安全だと思われている。しかし実際はWindowほどではないにせよ、Mac向けのマルウェアもマルウェア史の初期から存在し続けていた。それは現在も同じで、Macも安全地帯ではないということだ。

今回のプレス・アンでは、最新Mac向けマルウェアの特徴を分析し、Mac環境を保護する方策を探る。

Appleのマッキントッシュ(Macintosh、以下Mac)に対するユーザーの信頼は厚く、次のような挿絵からも見て取れる。コンピューター使用中感電したキャラに、「コンピューターに異常はないかい？」と聞いたところ「これはMacだから大丈夫」と断言する内容である。


[図1] The Brads- Impossible

その信頼はセキュリティに関しても絶大で、どうやらMacは安全な環境であると思われているらしい。しかし前述のようにMac向けマルウェアは昔から存在していたし、Macの運営環境である「OS X」に移行してから10年間、脅威は持続的に発見されている。もちろんWindowに比べればMac向けマルウェアが少ないのは確かだが、最近発見されるマルウェアの傾向を見るとMacもまたマルウェアの安全地帯ではないことが分かる。最近登場しているMac向けマルウェアの特徴を分析し、Macを保護するソリューションを見てみよう。

## 主なMacマルウェア

現在のMacも多くの進化を遂げた。プロセッサやOSの変化により、[図2]のようにOS環境がOS Xに変更された前後で発見されたマルウェアは異なる。


[図2] Mac向けマルウェア史タイムライン

OS X移行後に登場したマルウェアに関する詳細情報は次の通りだ。

| マルウェア(発見時期) | 特徴 | 備考 |
|---|---|---|
| Renepo<br>(2004) | -システムセキュリティ設定: 低<br>-OS X ファイアウォール解除<br>-ソフトウェアアップデート機能解除<br>-ohphoneX(ボイス及びビデオ共有)、dsniff(暗号スニファ)、John the Ripper(暗号クラック)をダウンロードインストール | -OS X 初のマルウェア<br>-2004/3/3、ニックネーム DimBulbが「Macintosh Underground forum」に参加後、3/13からスクリプトワームに対して掲載し、フォーラムの参加者とマルウェア作成を開始。9/10の掲載バージョンが10/23に外部に知れ渡り、10/24から大炎上したことから作成を放棄<br>-Apple社ではマルウェアではないと否認し、対応せず |
| RSPlug(Dnschanger)<br>(2007.10) | -DNSアドレスを変更してフィッシングサイトに誘導し、金銭的要求 | -使用者に実害を与えた初のOS X向けマルウェア |

| マルウェア(発見時期) | 特徴 | 備考 |
|---|---|---|
| MacSweeper<br>(2008.1.17) | -常に何かを診断し、購入要求 | -OS X初の偽装アンチウィルスプログラム<br>-KiVVi Softwareで作成し、強制マーケティングに使用したことで公式謝罪<br>-2011/5以降Mac Defender、Mac Protector、Mac Security、Mac Guard、Mac Shieldなど偽装プログラムが大幅に増加<br>-Apple社は同年5月末セキュリティアップデートを行い、偽装アンチウィルスプログラムの削除機能を追加した。この件でAppleCareに約6万件の問い合わせが発生 |
| Olyx<br>(2011.7) | -標的型攻撃推定 | -PortalCurrent events-2009 July 5.rarの中国デモ写真の中にOS Xマルウェア「Current events 2009 July 5」とWindowマルウェアの「Video-Current events 2009 July 5.exe」が潜んでいた<br>-写真をクリックするとマルウェアが実行 |
| Flashback<br>(2012) | -Javaゼロデイ攻撃で配布 | -Java脆弱性(CVE-2011-3544, CVE-2008-5353)利用<br>-3/16に発見された変種は他のJava脆弱性(CVE-2012-0507)を利用<br>-Apple社がセキュリティアップデートを4月に行ったため、約19日間は無防備ゼロデイ攻撃状態<br>-世界で60~75万台のMacが感染されたと推定(米国35万台、カナダ12万台、イギリス8万4千台、オーストラリア4万8千台、韓国130台ほど) |
| Macontrol<br>(2012.3) | -チベット独立活動家を標的攻撃<br>-脆弱性を利用した攻撃 | -特定人、特定の団体を標的にした代表的な事例 |
| Sabpab<br>(2012) | -バックドア機能<br>-Luckycatとの関連性が疑われ | -2012/2にWord文書(MS09-027, CVE-2009-0563)を利用した攻撃<br>-2012/4にJava脆弱性を利用して感染の試み |
| Morcut(Crisis)<br>(2012.7) | -自分を隠ぺいするRootkit機能 | -OS X10.6と10.7で実行可能<br>-2015/7にハッキングチーム流出資料から、同マルウェアがハッキングチームで作成されたことが表明<br>-2016/2に新たな変種発見 |
| Kitm<br>(2013.5) | -標的型攻撃 | -Jacob AppelbaumがOslo Freedom Forumのアフリカ・アンゴラ活動家のシステムから発見<br>-同マルウェアの作成者は、Windowsマルウェアも作成した経歴の持ち主<br>-2013年にIcefog、2014年にCaretoなど、OS Xの標的型攻撃マルウェアを相次いで発見 |
| Cointhief(Coinstealer)<br>(2014.2) | -ビットコイン奪取機能 | -オンライン仮想通貨ビットコインの流行を反映 |
| Wirelurker<br>(2014.11) | -USB接続をモニタリング | -OS Xの外、iOSを標的として作成<br>-ユーザーがアイフォンをMacに繋げると、悪質なアプリがアイフォンにインストールされる手法 |
| Keranger<br>(2016.3) | -ランサムウェア | -サイトをハッキングして、マルウェアを潜ませた改ざんインストールバージョンで感染<br>-感染後、一定時間経過後にデータ暗号化 |

[表1] Mac OS X向けマルウェア

2006年頃までは、OS X向けマルウェアによる被害は小規模に留まっていた。しかし2011/5以降、偽装したアンチウィルスプログラムによる被害が本格化し、2012/4にはFlashbackによる大規模なマルウェア感染が発生した。この件は、これ以上Macがマルウェアから安全ではないということを指し示した事件だった。このような大規模な感染をきっかけに「Macにはマルウェアが存在しない」、「問題ない」と無視を決めていたApple社も、2012/6からは『マルウェアから安全』という文章を訂正するに至った。

2014年と2015年には使用者情報を奪取するバックドア以外にも、不正に金銭的利益を得るためのアドウェア(Adware)や不要なプログラム(Potentially Unwanted Program、以下PUP)が相次いで登場し、Yontoo、VSearchなどのアドウェアは日に数十個ずつ発見されている。

2015/3には中国のQihoo 360から OceanLotus情報を公開した。同マルウェアは中国を対象に作成され、OS X向けマルウェアも含まれていた。

同年9月にはXcode Ghostが発見された。開発ツールのXcode改ざんバージョンを作成して配布したものだが、同バージョンでアプリを開発する場合、マルウェアを含むことになり、数千個以上のアプリが影響を受けている。

2016/3、Transmissionにアップされたプログラムからランサムウェア「Keranger」が潜むハッキングバージョンが発見された。攻撃者はサイトをハッキングしてマルウェアを含むハッキングバージョンをアップロード後に配布した。改ざんされたTransmissionが実行されれば実際にランサムウェア機能を持つGeneral.rtfを実行する。公式サイトで配布されたうえにトルコの認証コード署名があり、Appleのゲートキーパー(Gatekeeper)さえもパスしたため、ユーザーは疑うことなく使用したという。

## 最新Macマルウェアの特徴

2012年に発見されたOS X向けマルウェアは約120個で、2013年も似たような水準だった。しかし2014年にはOS X向けマルウェアが約1,000個に急増した。この数値はMac向けマルウェアの絶対多数を占めるアドウェアとPUPをマルウェアに分類するかどうかによって異なるが、2016年の現在もアドウェア、PUPを含めて一日数十個の新たな変種が発見されている。

OS X向けマルウェアの最新の特徴を次のようにまとめた。

### Macユーザーの情報を狙う標的型攻撃

ビジネス現場でもMacユーザーが増え、これらの情報を狙う標的型攻撃が発生している。最初の攻撃ケースは2011/7の「Olyx」だった。2011/7にデモ写真をまとめた圧縮ファイルから、ピクチャファイルに偽装したWindow向けマルウェアとOS X向けマルウェアのOlyxが発見された。WindowやOS Xユーザーが写真を見るためにファイルをクリックするとマルウェアが実行され、標的型攻撃に使用されたのではないかと考えられている。

その後、本格的な標的型攻撃は2012年から確認された。2012/3にチベット独立団体に対する標的型攻撃が発生したが、ここではMacontrolと Sabpabが利用されている。Macontrolの変種マルウェアは、2012/6にウイグル独立団体を攻撃する際にも使用された。

2013/5にはアフリカ・アンゴラ活動家のシステムからKitmマルウェアが発見された。その後2013年 Icefog、2014年 Caretoなど、OS Xを狙った標的型攻撃マルウェアは相次いで登場している。

標的型攻撃マルウェアは、少数の攻撃対象を狙って密かに活動するのでほとんどは発見が遅れてしまいがちだ。

### 脆弱性を突くマルウェア

2012/5には60万台のMacが一度にFlashbackワームに感染する事件が発生した。このような大規模な感染は、同マルウェアがJava脆弱性を利用したために発生したもので、2013年にも多数のJava脆弱性を利用した攻撃が起こっている。これはクロスプラットホーム(Cross platform)攻撃というもので、Java脆弱性を利用すれば一つの脆弱性から多様なプラットホームに対する攻撃が可能となるもの。この手法を利用するとプラットホームごとに適したマルウェアを感染させることができる。Apple社はJava脆弱性を突いた攻撃頻度が多発していることから、Javaを基本アプリケーションから除外した。以後Javaを利用した攻撃は減りつつあるがOS Xのセキュリティホールは持続的に発見され、一部は感染経路に利用されている。

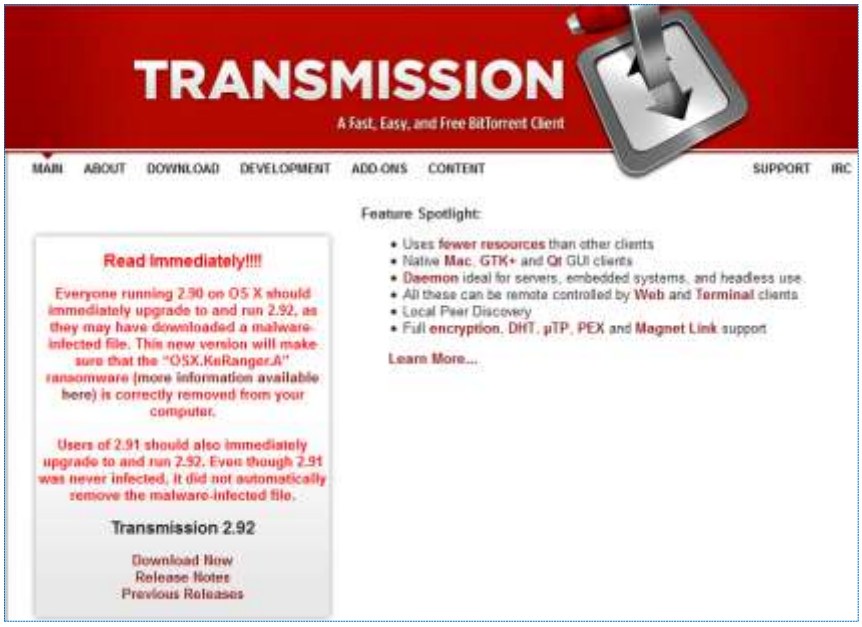
### 境界性プログラム

OS Xでも境界性プログラムが登場した。偽装アンチウィルスプログラムは2011年から登場したが、最近は常駐キーロガー、Keygen、アドウェアなどのプログラムも発見されている。このようなアドウェアは通常多くのプログラムに挿入されてインストールされるが、Javaもアドウェアを含めたまま配布されたことがあり物議を醸した。


[図3] 偽装アンチウィルス製品の感染画面

### 開発者をハッキングするマルウェア

MacのOS XにはApp Storeの検証済みプログラムのみインストールできる。インターネットからダウンロードしたファイルも、確認済み開発者のファイルのみ許可している。だがここまで徹底しても、App Storeにアップされていないプログラムを利用することも多いため、完璧な防御とはいえない。攻撃者は確認された開発者のコード署名をハッキングし、自身のマルウェアに署名する手法を駆使する。実際2013/5のOslo Freedom Forumに参加したアフリカ・アンゴラ活動家のシステムで発見されたKitmや、2016/3/4にTransmissionサイトから配布されたランサムウェアを潜ませたプログラムなどは開発者のコード署名が利用されていた。




[図4] ランサムウェアを潜ませたプログラムを配布したTransmissionサイト

## アンラボ、Mac向けセキュリティソリューションをリリース

このような状況を踏まえると、Mac安全神話は揺らいでくる。アンラボは、Mac OS向けアンチウイルスソリューション「V3 365 Clinic for Mac」を3月にリリースした。本ソリューションはMac OSに最適化され、Mac OS向けの多様なマルウェアに対応できる。セルフプロテクト機能でプロセス及び該当のプロセスで使用するファイルを保護し、パーソナルファイアウォールでネットワークセキュリティも徹底する。PUP、PUS、悪質なサイトを遮断するだけでなくMacに最適化されたインターフェースも提供する。


[図5] V3 365 Clinic for Mac (韓国語バージョン)

Mac誕生後30年余が過ぎた。特にMacはOS Xに移行後、マルウェアが登場してから10年以上経っている。OS X向けマルウェアの未来はどこへ向かうのか。現在Macのマーケットシェアは1割ほどであり、しばらくマルウェアが爆発的に増加することはないと思われているが、これまで比較的マルウェアから安全と思われていたMacユーザーたちもけして安心できない状況だ。OS Xの脆弱性を探る試みも相次いでいるうえ、ランサムウェアが作成されたり組織の情報を狙った標的型攻撃も持続的に報告されている。だがMac向けアンチウィルスソリューションの普及率はまだまだ少ないほうだ。Macが他のOS環境に比べて相対的に安全なのは事実だが、100%安全ではないことを忘れてはならない。

[参考文献]

[1] Pre-OS X Malware (https://macviruscom.wordpress.com/pre-os-x-malware )

[2] Mac はマルウェア感染の心配なし？
(http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=3&seq=19879&columnist=0&dir_group_dist=0 )

[3] Macはマルウェアから自由なるか
(http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=21708&key=&dir_group_dist=0)

[4] APT攻撃、Mac OSもターゲットに (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=20935)

[5] 10 years of Mac OS X malware (www.welivesecurity.com/2014/03/21/10-years-of-mac-os-x-malware)

[6] Mac向けマルウェアの脅威動向 (http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=23326&dir_group_dist=0)

[7] History of Mac Malware (http://www.webroot.com/blog/2015/10/02/history-of-mac-malware/)

[8] http://blogs.technet.com/b/mmpc/archive/2011/07/25/backdoor-olyx-is-it-malware-on-a-mission-for-mac.aspx

[9] http://news.drweb.com/show/?i=2341&lng=en&c=5

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

**アンラボとは**

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)