マルウェアに関し、ユーザが余り認識していない感染の形態や感染経路について

2019 年 1 月 28 日

駿河台大学　経済経営学部　准教授　八田真行

マルウェアやコンピュータ・ウイルスというと、従来はパソコンが感染するものという感覚が強かった。しかし最近では、Wifi や Bluetooth といった無線通信の一般化や品質向上に加え、高性能なコンピュータの小型化によってスマートフォンやスマート家電が普及し、様々な機器がインターネットに接続しうる IoT（Internet of Things）の時代が到来したため、従来は考えにくかった意外な機器が攻撃者に乗っ取られて悪用される感染形態が増えてきている。

実験も含めれば、ネットワークルータ[1]、モバイルルータ[2]、NAS[3]、プリンタや複合機[4]、いわゆる「見守りカメラ」を含む IP カメラ[5]、冷蔵庫[6]、テレビや DVR、セットトップボックス[7]、ペースメーカー[8]、エアコンやエレベータを含むビル管理システム[9]、自動車[10]、トイレ[11]等で乗っ取りが技術的に可能であることが示された。

機器の種類やメーカーこそ違えどアーキテクチャやファームウェアがほぼ同じ（Android を含む組み込み Linux が大多数）、管理画面のユーザ名やパスワードがデフォルトから変更されず（データベースも存在[12]）、変更されたとしても容易に推測可能なことが多い（様々なオンライン・プラットフォームから流出したパスワードのデータベースが存在）、据え置きや組み込みで直接ユーザの目に触れないことも多いので、脆弱性が発覚してもアップデートが速やかに適用されず、あるいはそもそも更新ができない等の問題があり、IoT 機器のマルウェアによる悪用は今後も増え続けると考えられる。2016 年に登場したマルウェア Mirai [13]やその亜種のように、実験ではなく実世界の無線ルータ等を大量に乗っ取って大規模な悪用を実現したものも出現している。

---

[1] https://www.tomsguide.com/us/russian-router-malware,news-27288.html

[2] https://internet.watch.impress.co.jp/docs/news/1099223.html

[3] https://internet.watch.impress.co.jp/docs/news/1123623.html

[4] https://www.computerweekly.com/blog/Quocirca-Insights/How-printers-can-be-a-launchpad-for-malware-attacks

[5] https://blog.trendmicro.co.jp/archives/14836

[6] https://www.infoworld.com/article/3176673/internet-of-things/your-smart-fridge-may-kill-you-the-dark-side-of-iot.html

[7] https://www.engadget.com/2018/06/12/android-malware-infecting-amazon-fire-tvs-sticks/

[8] https://wired.jp/2018/09/18/pacemaker-hack-malware/

[9] https://www.hackread.com/malware-can-compromise-building-control-systems/

[10] https://www.gnu.org/proprietary/malware-cars.html

[11] https://www.usatoday.com/story/tech/2013/08/06/smart-toilet-hack/2622723/

[12] http://www.routerpasswords.com/

[13] https://en.wikipedia.org/wiki/Mirai_(malware)

乗っ取られた機器は、いわゆるボットネットの一部として他サイトへの攻撃やスパムメールの送信、広告詐欺、仮想通貨マイニング等に使われることが多いが、最近の機器は高性能なカメラやマイク、センサー等を備えていることも多く、今後はユーザがより深刻なプライバシー侵害や物理的被害に晒される可能性もある。グローバル IP アドレスが振られていなくても、UPnP や設定によって LAN 内の機器にポートフォワードされてインターネット側から見えてしまう場合もある。

現在一般的なユーザにはあまり知られておらず、今後周知すべきポイントとして、

1. マルウェアに感染するのはパソコンだけではない

2. （リンクをクリックするなど）ユーザが何かしなくても、いつの間にか感染することがある

3.「たまにネットが重くなる」には要注意

4. 常にアップデートに留意すべき、アップデートが提供されなくなった古い機器は早めにリプレースを

が挙げられる。

1.に関してはすでに言及した。2.に関しては、攻撃者は IP アドレス等を自動生成して総当たりでアクセスしてくるので、ユーザが能動的に何かしなくても知らない間に感染していることはあり得る。管理画面には LAN からのみアクセスできるようにする、パスワードを変更する等の対策を促すことが必須である。ルータ等に関しては、ファクトリーリセットのやり方を理解する必要もあろう。

3.に関しては、マルウェアに感染しても普段は通常通り動作していることが多いが、ボットネットの一部として指令を受け活動しているときには不自然な挙動をすることがあるので注意が必要である。

4.に関しては、例えば比較的新しい Android スマホ等であってもパッチやアップデートが提供されず、危険な Blueborne 脆弱性[14]が放置されていることもあるので、早めのリプレースを促す必要がある。

以上

[14] https://blogs.mcafee.jp/blueborne-vulnerability-prevention