Vol.2017-IOT-36 No.20
2017/3/3

公開情報からみる Mirai

夏目 大伍† 今野 俊一† 水越 一郎‡

†NTT セキュアプラットフォーム研究所 〒180-8585 東京都武蔵野市緑町 3-9-11
‡情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1

Survey of Mirai by OSINT(Open Source Intelligence)

Daigo Natsume† Shunichi Konno† Ichiro Mizukoshi‡

†NTT Secure Platform Laboratories, 3-9-11, Midori-cho Musashino-shi, Tokyo, 180-8585, Japan
‡Institute of Information Security, 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa, 221-0835, Japan

概要：2016 年 09 月 20 日，セキュリティ blog である Krebs On Security が大規模な DDoS 攻撃を受けた．その後，この攻撃はマルウェア Mirai に感染した IoT(Internet of Things)デバイスのボットネットによるものであることが判明した．Mirai はこの攻撃以降も Dyn や Deutsche Telekom への攻撃に利用され，多くの被害を出した．本セッションでは，Mirai 及び Mirai による複数の攻撃事例について公開情報に基づいた調査結果を報告すると共に，その内容についてディスカッションを行う．

キーワード: Mirai, IoT, DDoS, Incident Handling

1. はじめに

IoT デバイスによるインシデントは以前より危惧されていたが [1]，2016 年後半から Mirai 及びその亜種によると推測される攻撃が猛威をふるっている．

本セッションでは，公開情報を用いた分析(OSINT:Open Source INTelligence)によって判明した Mirai の特徴及び攻撃事例について報告し，その内容についてのディスカッションを行う．

2. マルウェア Mirai

Mirai は IoT デバイスに感染し，ボットネット構成するマルウェアである．2016 年 09 月 30 日，Hack Forums にて Anna-senpai と名乗る Mirai 製作者によってソースコードが公開された [2]．このソースコードから，Mirai は C2 サーバと通信し，DDoS 攻撃と，デフォルトの認証情報を使っている脆弱なホームルータや IP カメラといった IoT デバイスのスキャンを行い Telnet ログインすることで，ボットネットに組み込むことがわかっている．

Mirai はメモリにロードされるマルウェアのため，感染したデバイスを再起動することで削除できる．しかしながら，再起動して数分後には再び Mirai にスキャンされてしまうため，Telnet のログインパスワードを変更することも必要である．

3. ソースコード公開による亜種の登場

Mirai のソースコード公開から 5 日後である 2016 年 10 月 05 日，Rapidity Networks の研究者らが IoT マルウェア Hajime を発見した [3]．Hajime は Mirai と同様に 脆弱な IoT デバイスをスキャンし，Telnet ログインすることでボットネットの拡大を行う．これ以外にも Hajime は，Rex や NyaDrop といった他の IoT マルウェアが持つ特徴も取り込んでおり，より洗練されたものになっている．

4. 攻撃事例 1 : Krebs On Security への攻撃

2016 年 09 月 20 日，セキュリティ blog である Krebs On Security が 620Gbps という大規模な DDoS 攻撃を受けた [4]．本件は Mirai による攻撃であることがわかっている． 同 blog は Akamai Technologies によって無償で保護されていたが，同社は他の顧客への影響を考え，ネットワークから同 blog の切り離しを行った．3 日間の停止状態の後，Google の Project Shield の支援を受けて同 blog は復旧した．

5. 攻撃事例 2 : Dyn への攻撃

2016 年 10 月 21 日，Dyn が提供する Managed DNS プラットフォームに対して 2 度の DDoS 攻撃が発生した [5]．攻撃の大半は Mirai ボットネットによるものであることが確認されている．この攻撃の結果，同社のプラットフォームを利用する Twitter, Reddit, GitHub, Netflix, Spotify 等へのアクセス障害が発生した．攻撃は大量の送信元からの TCP と UDP の 53 番ポートを狙った大規模な flood 攻撃であった．Dyn は 10 万台のボットから攻撃を受けたと推測しており，攻撃の規模が 1.2Tbps であるという報告を受けたと述べている．

6. 攻撃事例 3 : Deutsche Telekom への攻撃

現地時刻 2016 年 11 月 27 日の 17 時頃から最低 2 日間 Deutsche Telekom の顧客 90 万人にサービス制限等の影響が発生した [6]．これは Deutsche Telekom の顧客数全体の 4%に相当する．Flashpoint の見解では，本攻撃は Mirai の亜種によるものである [7]．図 1 は発生当時にサービス影響が出たエリアを図示したものであるが．これより，ドイツ全域で影響が出ていたことがわかる．

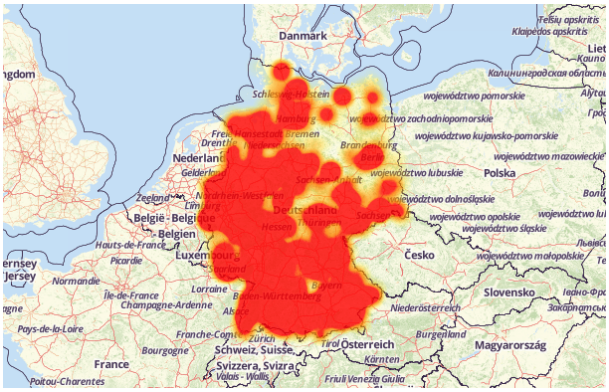

図 1　Deutsche Telekom のサービスが
使えなくなった地域[6]

Deutsche Telekom の発表 [8]によれば，何者かがルータの遠隔保守機能の脆弱性 [9]を利用して，Deutsche Telekom が顧客に提供する Speedport ルータをマルウェアに感染させようとしたが，Speedport ルータはこの脆弱性を有していなかったため，攻撃は失敗した．しかしながら，攻撃が契機となり，Speedport ルータが機能不全状態になる等の影響が発生した．

本件に関して Deutsche Telekom は以下の対応を行ったと述べている [8].

- フィルタを書いて Speedport ルータの遠隔保守ポート宛の通信をブロック
- ルータ製造企業にソフトウェア改修を依頼し，これを発生日当日のうちに影響を受けたデバイスに対して配布
- 影響の有無に関わらず，Speedport ルータの全モデルのチェックを実施

7. Mirai 製作者の正体

Mirai ボットネットから攻撃を受けた Krebs On Security が，2017 年 01 月 18 日に Mirai 製作者である Anna-senpai と名乗る人物の正体に関する調査記事を掲載した [10]．様々な情報を組み合わせた結果，Anna-senpai と ProTraf Solutions という DDoS 保護サービスプロバイダの経営者に関連があることがわかった．ProTraf Solutions は，競合する DDoS 保護サービスプロバイダに対して DDoS 攻撃を実施し顧客を奪い取るということも行っていた模様である．

8. ディスカッションポイント

これまで，公開情報を元に Mirai の特徴と攻撃事例を紹介した．これより，Mirai は脆弱な IoT デバイスをボットネットに組み込み，これを利用した攻撃を行うことで多大なる被害を出してきたことがわかる．また，ソースコードの公開により複数の亜種が生まれている．このような点を踏まえ，以下の点を議論したい．

- IoT デバイスが備えるべき要件(低価格な IoT デバイスに対してどこまでセキュリティ対策を施すか)
- IoT ボットネットからの攻撃の影響を最小限にとどめるためには，どのような防御策をとるべきか
- ソースコード公開に悪意があるかどうかをどのように判断するか，悪意があった場合にどう対処するか
- 真偽不明ではあるが、仮に調査記事が真実だったとした場合に、製作者の正体とその意図をどううけとめるか

謝辞

本研究は科研費(15H03385)の助成を受けたものである．

参考文献

[1] J. Queenan, "When the 'Internet of Things' Attacks," 29 8 2014. [Online]. Available: http://www.wsj.com/articles/when-the-internet-of-things-attacks-1409331700. [Accessed 30 01 2017].

[2] B. Krebs, "Source Code for IoT Botnet ‘Mirai’ Released," 01 10 2016. [Online]. Available: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/. [Accessed 30 01 2017].

[3] S. Edwards and I. Profetis, "Hajime: Analysis of a decentralized internet worm for IoT devices," 16 10 2016. [Online]. Available: https://security.rapiditynetworks.com/publications/2016-10-16/hajime.pdf. [Accessed 30 01 2017].

[4] B. Krabs, "KrebsOnSecurity Hit With Record DDoS," 21 09 2016. [Online]. Available: http://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Accessed 30 01 2017].

[5] S. Hilton, "Dyn Analysis Summary Of Friday October 21 Attack," 26 10 2016. [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. [Accessed 30 01 2017].

[6] P. Paganini, "More than 900k routers of Deutsche Telekom German users went offline," 28 11 2016. [Online]. Available: http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html. [Accessed 30 01 2017].

[7] J. Costello, "New Mirai Variant Leaves 5 Million Devices Worldwide Vulnerable — High Concentration in Germany, UK and Brazil," 29 11 2016. [Online]. Available: https://www.flashpoint-intel.com/new-mirai-variant-involved-latest-deutsche-telekom-outage/. [Accessed 30 01 2017].

[8] Deutsche Telekom, "Answers to attack on routers of DT customers," 28 11 2016. [Online]. Available: https://www.telekom.com/en/media/media-information/archive/13-answers-to-attack-on-routers-445148. [Accessed 30 01 2017].

[9] kenzo2017, "Eir’s D1000 Modem Is Wide Open To Being Hacked.," 07 11 2016. [Online]. Available: https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/. [Accessed 30 01 2017].

[10] B. Krebs, "Who is Anna-Senpai, the Mirai Worm Author?," 18 01 2017. [Online]. Available: https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/. [Accessed 30 01 2017].