1E-02

ダークネット観測結果による Hajime の Mirai に対する影響の調査

ファン・アン・ソン†,　中村　康弘‡
防衛大学校 理工学研究科 サイバーセキュリティ工学

1　はじめに

近年、IoT 機器が急速に普及・発展しているが、同時に、それらを標的とする Mirai, Hajime などのワームの活動が活発化している。Mirai はランダムな宛先 IP アドレスを生成してパスワードの辞書攻撃により感染を拡大するとともに、ボットネットを構築して C&C サーバからの指示により DDoS 攻撃を行うワームタイプのマルウェアである。Hajime は Mirai と同じように IoT デバイスへの感染を試みるが、DDoS 攻撃のようなサイバー攻撃の機能は搭載していない。Hajime 感染後は Mirai が感染拡大するためのポートを閉じることで Mirai の感染を妨害すると報告されている。これらのワームは IP アドレスをランダムに生成して感染を拡大しようとするため、未使用アドレスのへ着信する接続要求パケットを観測することで、これらの活動状況を把握することができる。

2　関連研究

Mirai と Hajime については多くの研究や報告がなされている。NICT はダークネットに到着したパケット数の観測結果を報告した [1]。このレポートでは Mirai, Hajime の感染活動が観測された日時と送信者の国別統計を公表した。また、1 日ごとのユニークな送信元アドレス数の増減も報告した。その結果、Hajime の感染数は Mirai の感染数の数倍程度であることを示し、Hajime と Mirai の感染の規模と感染活動が活性化した日が明らかとなった。IIJ-SEC セキュリティレポート 2018[2] は、ハニーポートに到着したパケットを使用して、Mirai, qBot, Hajime の感染活動を調査した。レポートではマルウェア感染活動の傾向を明らかにし、各ポートの送信元 IP アドレスの数を示した。そして、2019 のレポート [3] ではハニーポットで受信したパケットデータを元に、Mirai, Hajime の感染活動状況を調査し、Mirai の亜種の活動状況も調査した。

これらのレポートは Mirai, Hajime の通信特徴を持つパケットの送信元 IP アドレスに着目し、１日ごとのユニークな送信元アドレス数を計測することにより、感染活動を把握する。ただし、この手法では新たに出現する送信元アドレス数と回復した送信元アドレス数を把握することができないため、新規感染数の増減が不明であった。

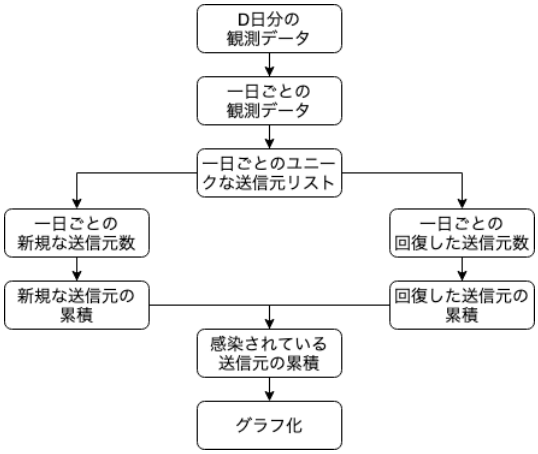

図 1: 処理手順

そこで本研究では、長期間にわたる Mirai, Hajime の新規出現送信元アドレス数と回復した送信元アドレス数を調査することで、Hajime の Mirai に対する影響を明らかにする。

3　調査方法

この報告では、NICT が提供しているダークネット観測データセットのうち、2016 年 1 月 1 日から 2018 年 12 月 31 日までの 3 年間分を用いた。ここで、Hajime からの接続要求パケットは Window Size が 14600 であること、Mirai の接続要求パケットのシーケンス番号は宛先 IP アドレスと同一であること [1] を条件とすることで、感染活動を行なった IP アドレスとその活動日時を調査する。長期にわたる観測結果に対してこの条件を処理を適用することで、その日に新規に感染したアドレス数、接続要求が来なくなることで回復したとみなすことができるアドレス数のそれぞれを調査することができる。

3.1　処理手順

長期にわたる観測結果のデータを用いて、以下の処理を行う。

Step1: D 日分の観測データを一日ごとに分割する。

Step2: 一日ごとのデータに対して、Hajime, Mirai のそれぞれの特徴を持つ接続要求パケットを抽出し、

A Survey of Hajime's Impact on Mirai from Darknet Observation,
†Son Pham Anh, ‡Yasuhiro Nakamura,
Cyber Security Engineering, National Defense Academy

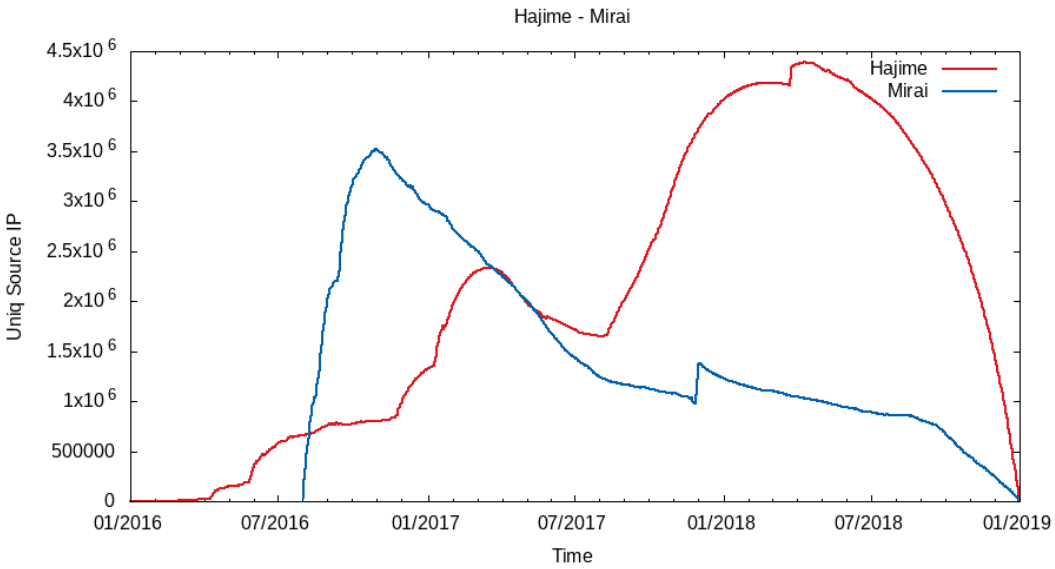

図 2: Mirai, Hajime の感染アドレス数の推移

その送信元アドレスの重複を除いてユニークな送信元アドレスリスト L_i を作成する。

Step3: D 日分の $L_i(i = 1, ..., D)$ から一日ごとに新規に出現した送信元アドレス数 N_i と回復した送信元アドレス数 R_i を求める。

Step4: 新規な送信元アドレスと回復アドレスのそれぞれの累積を TN_i, TR_i を集計する。

Step5: これらの差分により、その日に感染拡大活動を行なっているアドレス数 K_i を求める。

$$K_i = TN_i - TR_i \tag{1}$$

Step6: 得られた K_i をグラフ表示することで実際の感染数の推移を可視化する。

4 結果

Mirai、Hajime に感染されている送信元数の推移を図 2 に示す。Mirai の特徴を持ったパケットは 2016 年 8 月 1 日以前には存在せず、その日から急激に増大した。Hajime の特徴を持ったパケットは 2016 年 8 月 1 日以前にも存在していることが確認できた。図 2 を時間軸方向に見ると Hajime の数が徐々に増えているが、その増加にともなって Mirai の数が急速に減少していることがわかる。これは、Hajime が感染した機器は、Mirai が感染するためのポート番号を閉じることで Mirai の感染が妨害されたためと考えられる。

これらのワームはメモリ上で動作しており、機器の再起動により活動を停止する。このため、同一アドレスから複数日にわたって継続的に感染活動があったアドレスに対して、重複のないアドレス数および活動の継続日数を調査した。その結果、Mirai の特徴を持ったパケットの送信元アドレスの種類数は約 3600 万アドレスで、それぞれのアドレスの平均生存時間は約 38 日間であった。Hajime の送信元アドレスの種類数は約 2500 万アドレスで、平均生存時間は Mirai の約 3 倍の 90 日であった。

5 まとめ

従来の観測報告では 1 日毎の感染数のみに着目していたため、新規に感染した数が明らかではなかった。これは長期にわたってユニークなアドレス数を求めるという負荷の大きい処理を必要とするためである。この研究では特徴量によるフィルタリング処理とユニークなアドレスを抽出する処理を分離することで新規に観測されたアドレスや現れなくなったアドレス等を求めることができるようになった。この結果、Hajime の感染拡大に伴って Mirai の感染数が減少している状況を定量的に捉えることができた。今後、処理のためのメモリ効率等について改善する必要がある。

参考文献

[1] 情報通信研究機構サイバーセキュリティ研究室, NICTER 観測レポート 2018 年, https://www.nict.go.jp/press/2019/02/06-1.html, 2019.

[2] IIJ-SEC・Masafumi Negishi, 2018 年の IoT ボット観測状況と最近の動向, https://sect.iij.ad.jp/d/2019/01/288147.html, 2019.

[3] IIJ-SEC・Masafumi Negishi, 2019 年の IoT ボット観測状況, https://sect.iij.ad.jp/d/2020/02/030029.html, 2020.