Distributed via @police
http://www.npa.go.jp/cyberpolice/

平成 27 年9月 20 日

Topic

マルウェアに感染した Cisco 社製ルータを探索するアクセスの観測について

「SYNful Knock」マルウェアに感染した Cisco 社製ルータを探索していると考えられるアクセスを観測しました。Cisco 社製ルータを使用している企業や組織においては、管理する機器の感染の有無について確認を実施することを推奨します。

1 Cisco 社製ルータに感染するマルウェアについて

9月 15 日に米国のセキュリティ対策企業が Cisco 社製ルータに感染するマルウェアの詳細情報を公表[i]しました。この公表された情報によると、このマルウェアは Cisco 社製ルータに感染し、攻撃者が外部から遠隔操作可能なバックドアを作成するとしています。また、マルウェアの通信には細工された TCP パケットが利用されることから、同社はこのマルウェアを「SYNful Knock」と称しています。

なお、この情報の公表を受けて、製造元である Cisco 社も注意喚起[ii]を実施しています。

2 マルウェアに感染した Cisco 社製ルータを探索するアクセスの観測について

9月 16 日に米国ミシガン大学の研究者グループは、インターネット上においてマルウェア「SYNful Knock」に感染している Cisco 社製ルータの探索を実施し、同マルウェアと同様の応答を返す 79 台のホストを発見したことを明らか[iii]にしました。

警察庁の定点観測システムにおいても 16 日5時以降、ミシガン大学が管理する IP アドレスから、同グループが公表している探索パケットと同一内容のパケットを観測しています。また、17 日4時以降には、特定の非営利組織[iv]（以下「非営利組織」という。）が管理する IP アドレスからも同様の探索活動を観測しています。ミシガン大学や非営利組織の探索により判明したマルウェアに感染していると考えられるホストの具体的な情報は、制限なしに不特定多数に公開されることはなく、同探索の結果が攻撃に悪用される可能性はないと考えられます。

しかしながら、18 日 21 時から 19 日0時まで間には、ミシガン大学及び非営利組織が管理する IP アドレスとは異なる IP アドレスからの探索活動を観測しました。この新たに観測した IP アドレスはクラウドホスティングサービスを行う企業が管理する日本国以外の特定の国に割り当てられた IP アドレスであり、同サービスを利用している者が探索行為を実施していると考えられます。この探索の目的は不明であることから、マルウェアによって作成されたバックドアを悪用して、ルータに不正なアクセスを試みようとする攻撃者が、探索活動を実施している可能性も考えられます。

---

[i] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html
[ii] http://blogs.cisco.com/security/synful-knock
[iii] https://zmap.io/synful/
[iv] インターネットセキュリティの向上を目的として、攻撃を受ける可能性があるサービスが稼動している IP アドレスの探索等の活動を実施している非営利組織です。探索結果は当該 IP アドレス帯域の管理者等に限定して公開されています。

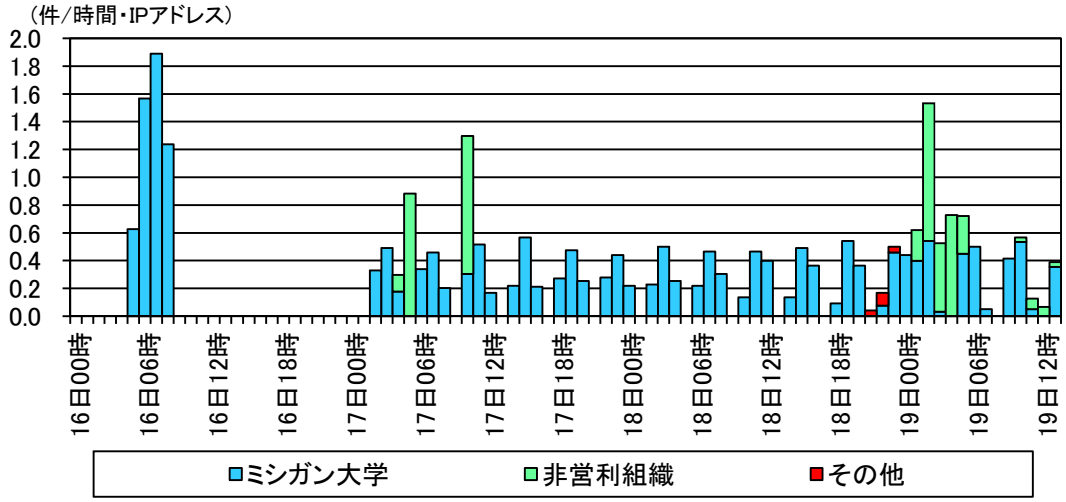

図1　マルウェアに感染したCisco社製ルータを探索するアクセスの発信元組織別の推移状況
（9月 16 日0時 ～ 9月 19 日 14 時）

3 推奨する対策

マルウェアの詳細について公表したセキュリティ対策企業は、感染経路の断定には至っていないながらも、未知の脆弱性が感染に利用された訳ではなく、以下の2点が原因として考えられるとしています。

- ルータの管理者パスワードを初期値のまま運用している。
- ルータの管理者パスワードが何らかの方法で攻撃者に漏洩した。

このことから、ルータ等のネットワーク機器においても、設定しているパスワードや、その管理方法について再度点検を実施することを推奨します。

また、同社はマルウェアに感染しているルータの調査方法等を公表[i]していることから、特にCisco社製ルータを利用している企業や組織においては、同情報を参照して管理する機器の感染有無の確認等を実施することを推奨します。

[i] https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis0.html
https://www2.fireeye.com/WEB-2015-SYNful-Knock.html