平成 28 年 11 月 29 日

リフレクター攻撃の踏み台となる機器の探索行為と考えられるアクセスの増加等について

（平成 28 年 10 月期）

- リフレクター攻撃の踏み台となる機器の探索行為と考えられるアクセスが増加
- 宛先ポート 4786/TCP に対するアクセスを観測
- D-Link 社製ルータの脆弱性を標的としたアクセスを観測

1 リフレクター攻撃の踏み台となる機器の探索行為と考えられるアクセスが増加

インターネット定点観測システムでは、10 月中旬から LDAP[i]に使用される宛先ポート 389/UDP に対するアクセスの増加を観測しています。観測したアクセスの発信元 IP アドレスのうち、インターネットに接続された機器等の調査を行なっている組織以外からの、探索と考えられるアクセスの増加を観測しています（図1）。

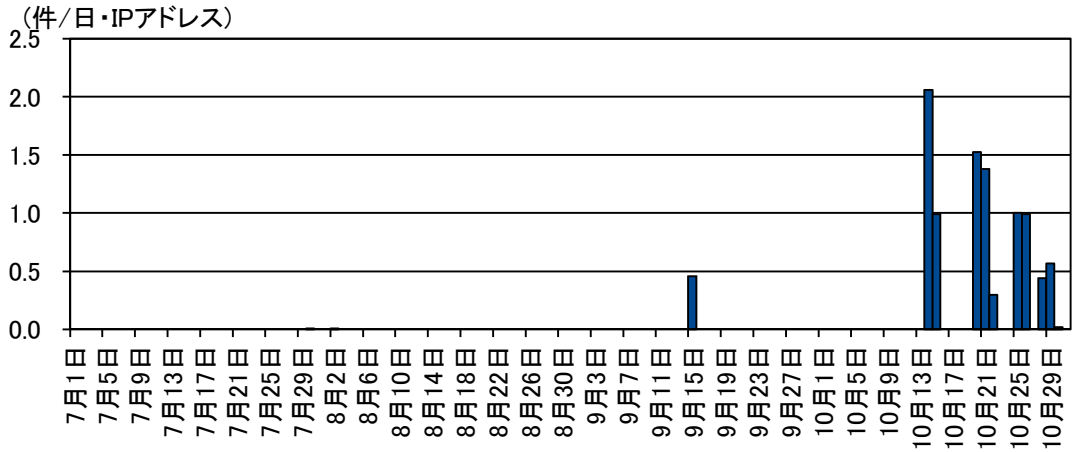

図1 宛先ポート 389/UDP に対するアクセス件数の推移（H28.7.1～10.31）
（発信元 IP アドレスが調査活動を実施している組織以外）

観測したアクセスは、ディレクトリ・サービス[ii]の検索要求である「SearchRequest」メッセージがほとんどであったことから、このメッセージに応答する機器の探索行為が行なわれていると考えられます。

[i] LDAP（Lightweight Directory Access Protocol）
ディレクトリ・サービスに接続するために使用されるプロトコルであり、コネクションレスのものは 389/UDP ポートで使用されています。

[ii] ネットワークを利用するユーザ名やマシン名などの様々な情報を管理するためのサービスのことで、ユーザ名などのキーとなる値から様々な情報を検索します。

LDAP は、US-CERT において、リフレクター攻撃に悪用することができるプロトコルとして注意喚起[i]がなされており、インターネットに公開された LDAP サーバが外部からの「SearchRequest」メッセージに応答すると、リフレクター攻撃（図2）の踏み台として悪用される危険性があります。

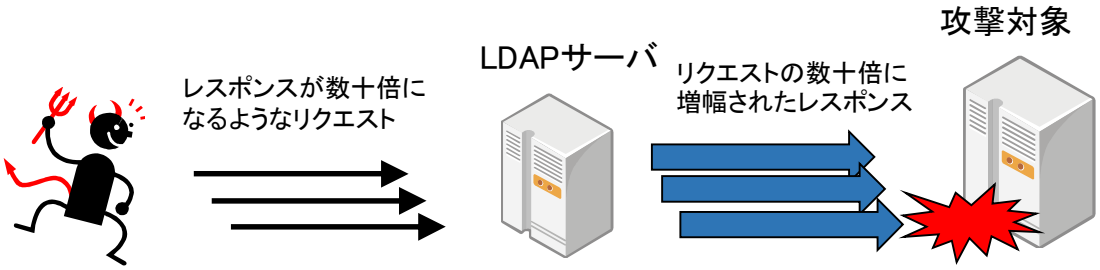

図2　LDAP サーバを悪用したリフレクター攻撃のイメージ

10 月下旬には、海外のセキュリティ企業が、LDAP を悪用したリフレクター攻撃を確認したと公表[ii]しています。

管理する機器がリフレクター攻撃の踏み台として悪用されないためにも、管理者は機器の状況を確認し、インターネットからの通信を遮断したり、適切なアクセス制限を実施したりするなどの対策が必要です。

[i] 「Alert (TA14-017A) UDP-Based Amplification Attacks」
https://www.us-cert.gov/ncas/alerts/TA14-017A

[ii] 「Corero Warns of Powerful New DDoS Attack Vector with Potential for Terabit-Scale DDoS Events」
https://www.corero.com/company/newsroom/press-releases/corero-warns-of-powerful-new-ddos-attack-vector-with-potential-for-terabit-scale-ddos-events/

2 宛先ポート 4786/TCP に対するアクセスの観測

10 月下旬に、宛先ポート 4786/TCP に対するアクセスを観測しました（図3）。4786/TCP は、Cisco Systems 社製スイッチやルータ等の Smart Install 機能[i]で使用されているポートです。

図3 宛先ポート 4786/TCP に対するアクセス件数の推移

平成 28 年9月 28 日に、Cisco Systems 社から、同社製のネットワーク機器用ソフトウェアである Cisco IOS 及び Cisco IOS XE の Smart Install に対する脆弱性[ii]が存在することが公表されました。同脆弱性が悪用された場合、リモートでメモリリークを発生させ、サービス不能に至る可能性があるとされています。また、海外のセキュリティ機関の SANS ISC（Internet Storm Center）から、同該脆弱性に関する情報が公表[iii]されています。公表された情報には、同脆弱性に関連するとされるエラーログが掲載されており、エラーログの日時は、日本標準時で 10 月 22 日 11 時 12 分であったことから、同時間帯に同脆弱性に対する攻撃活動が行われていた可能性があります。インターネット定点観測システムにおいても、同時間帯に宛先ポート 4786/TCP へのアクセスを観測しています（図4）。

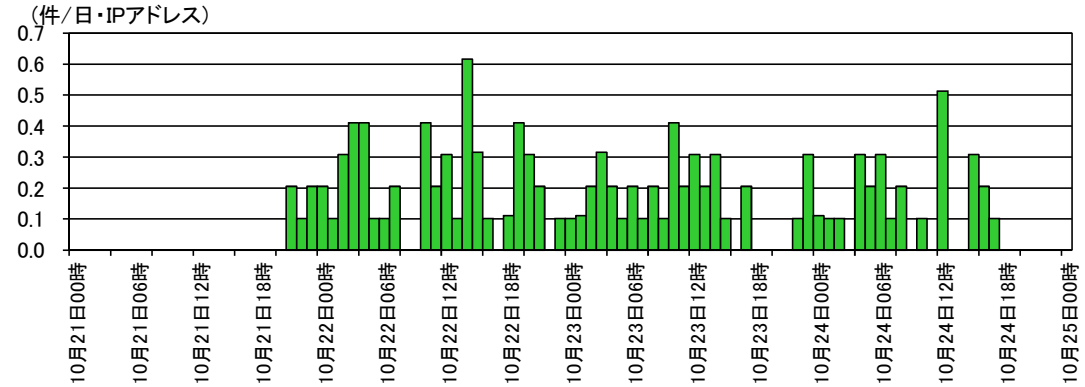

図4 宛先ポート 4786/TCP に対するアクセス件数の推移（H28.10.21～10.24）

[i] ネットワークにスイッチが接続されると、自動的に上位のスイッチやルータからコンフィグをダウンロードし、スイッチの OS である Cisco IOS を適切にアップグレードしてユーザに使えるようにする機能。

[ii] 「Cisco IOS and IOS XE Software Smart Install Memory Leak Vulnerability」
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160928-smi

[iii] 「Request for Packets TCP 4786 - CVE-2016-6385」
https://isc.sans.edu/diary/21625

観測した宛先ポート 4786/TCP に対するアクセスと同脆弱性との具体的な関連性は不明ですが、攻撃者が脆弱性を有する機器を探索し、攻撃の準備行為を行っている可能性も十分考えられます。このため、同脆弱性の影響を受ける機器を利用している場合は、Cisco IOS や Cisco IOS XE を脆弱性が修正された最新のバージョンにアップデートするなどの対策を実施することを推奨します。

3 D-Link[i]社製ルータの脆弱性を標的としたアクセスを観測

D-Link 社製の特定のルータについては、平成 28 年9月下旬に海外のセキュリティ企業から複数の脆弱性が報告[ii]されています。同脆弱性を悪用されると第三者から管理者権限でリモートログインされるおそれがあります。同脆弱性は、特定ポートに対して特定の文字列を送信することにより、ユーザ認証を回避して管理者権限でのアクセスを可能とするもの（以下「バックドア」という。）です。

インターネット定点観測システムでは、D-Link 社製の特定のルータのバックドアを標的としたアクセスを、10 月上旬に観測しました（図5）。

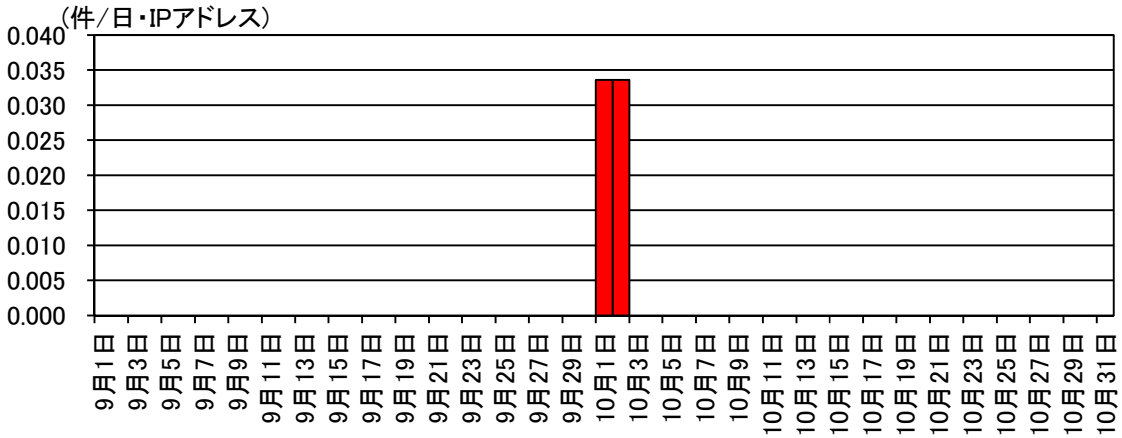

図5 D-Link 社製の特定のルータのバックドアを標的としたアクセス件数の推移（H28.9.1～10.31）

D-Link 社製の特定のルータを利用している場合は、ルータの使用状況を確認し意図しない通信が行われていないか点検するとともに、ルータを外部ネットワークからアクセスさせる必要がある場合は、適切なアクセス制限を実施することを推奨します。

[i] 1986 年に設立されたネットワーク機器メーカで、台湾台北市に本社を置く企業。
http://www.dlink.com/

[ii] 「Backdoored D-Link Router Should be Trashed, Researcher Says」
https://threatpost.com/backdoored-d-link-router-should-be-trashed-researcher-says/120979/