レポート

平成 29 年 7月 31 日

海外製デジタルビデオレコーダの脆弱性を標的としたアクセスの観測等について

- 海外製デジタルビデオレコーダの脆弱性を標的としたアクセスの観測
- Samba の脆弱性（CVE-2017-7494）を標的としたアクセスを観測
- Intel AMT の脆弱性を標的としたアクセスの観測

1 海外製デジタルビデオレコーダの脆弱性を標的としたアクセスの観測

警察庁のインターネット定点観測システムにおいては、平成 29 年5月 29 日頃から宛先ポート 9000/TCP に対する海外製デジタルビデオレコーダへのリクエストコマンドを含むアクセスの急増を観測しました（図1、2）。

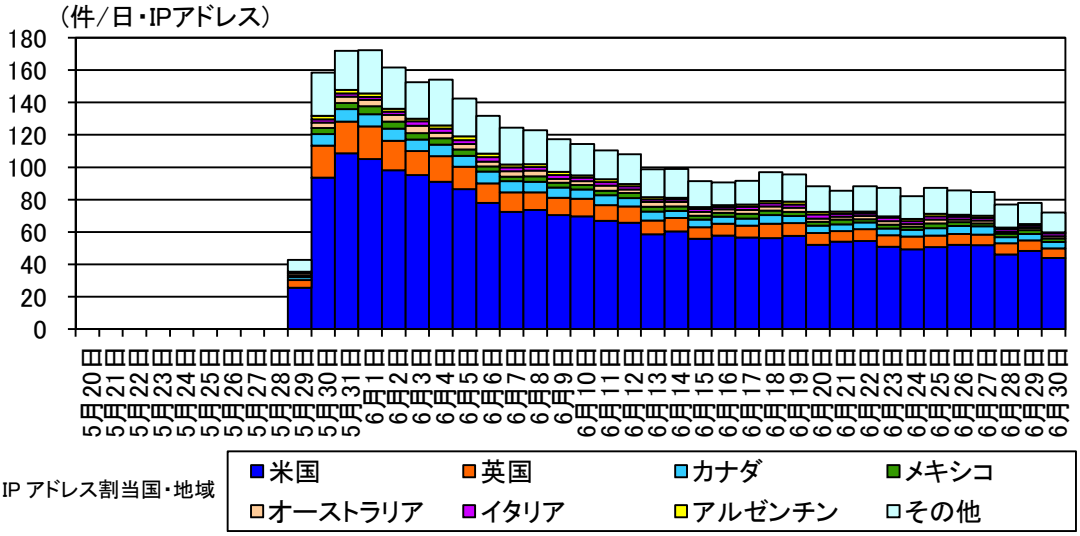

図1 宛先ポート 9000/TCP に対する海外製デジタルビデオレコーダへのリクエストコマンドを含むアクセス件数の発信元国・地域別推移（H29.5.20～6.30）

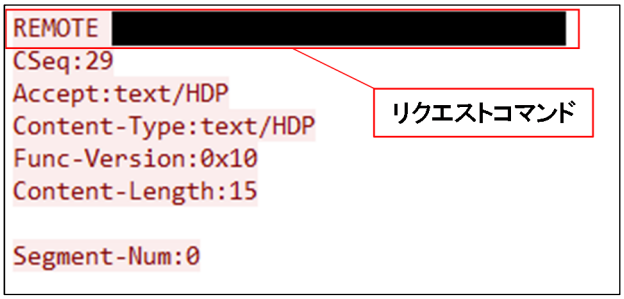

図2 観測したアクセスに含まれるリクエストコマンドの例（一部マスキングを実施）

この海外製デジタルビデオレコーダについては、平成 27 年3月に複数の脆弱性が公表[i]されています。これらの脆弱性には、9000/TCP ポートにおいてリモートでコマンドが実行されるものが含まれるとのことです。また、当該脆弱性を標的とした PoC[ii] が公開されています。今期観測したリクエストコマンドは、同 PoC に含まれるリクエストコマンドと類似するものであったことから、当該脆弱性に対する探索等を企図したアクセスが活発化している可能性があります。

当該アクセスの発信元に対して調査したところ、デジタルビデオレコーダのログイン画面が表示される発信元が多数存在しました。(図3)。

図3 デジタルビデオレコーダのログイン画面の例(一部マスキングを実施)

このことから、何らかのマルウエアに感染したデジタルビデオレコーダ等の IoT 機器が、感染拡大のためのスキャン活動や攻撃の踏み台として悪用されている可能性が考えられます。

デジタルビデオレコーダ等の IoT 機器の利用者は以下の対策を参考に、総合的にセキュリティ対策を行うことを推奨します。

- 該当機器をインターネットに接続する場合には、直接インターネットに接続するのではなく、ルータ等を使用してください。また、ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。
- 製造元のウェブサイト等で脆弱性情報を確認し、脆弱性がある場合はファームウェアのアップデート等の適切な対策を実施してください。
- ユーザ名及びパスワードは、初期設定のままでは使用せず、必ず変更してください。また、変更する際は、ユーザ名及びパスワードを推測されにくいものにしてください。

---

[i] 「Kguard Digital Video Recorder Multiple Security Vulnerabilities」
http://www.securityfocus.com/bid/73032/info

[ii] Proof of Concept の略。脆弱性を利用した攻撃が可能であることを示すための検証用プログラム。

- 製造終了から年月が経過した製品は、製造元が脆弱性への対応を実施しない場合があります。脆弱性が存在するにもかかわらず、製造元が対応しない製品は、使用を中止してください。

2 Samba の脆弱性（CVE-2017-7494）を標的としたアクセスを観測

Samba は Linux 等の Windows 以外の OS を搭載した機器で動作し、Linux 等と Windows において、ファイル、フォルダ、プリンタ等を共有するために使用されるソフトウェアです。Samba は通信ポートとして 445/TCP ポートを使用します。平成 29 年5月 24 日に開発元である The Team Samba から、Samba に存在する脆弱性（CVE-2017-7494）が公表[i]されました。開発元によると、バージョン 3.5.0 以降の Samba においてリモートでコードを実行される脆弱性があるとしています。また、当該脆弱性を標的とした PoC が少なくとも2種類既に公開されていることを確認しています。

警察庁のインターネット定点観測システムにおいては、6月上旬頃から宛先ポート445/TCPに対する上記 PoC の特徴と一致するセッションリクエストパケット及びネゴシエーションパケットの増加を観測しました（図4）。当該パケットは脆弱性の公表後から増加していることから、上記 PoC を使用した当該脆弱性を標的とするアクセスの可能性があります。

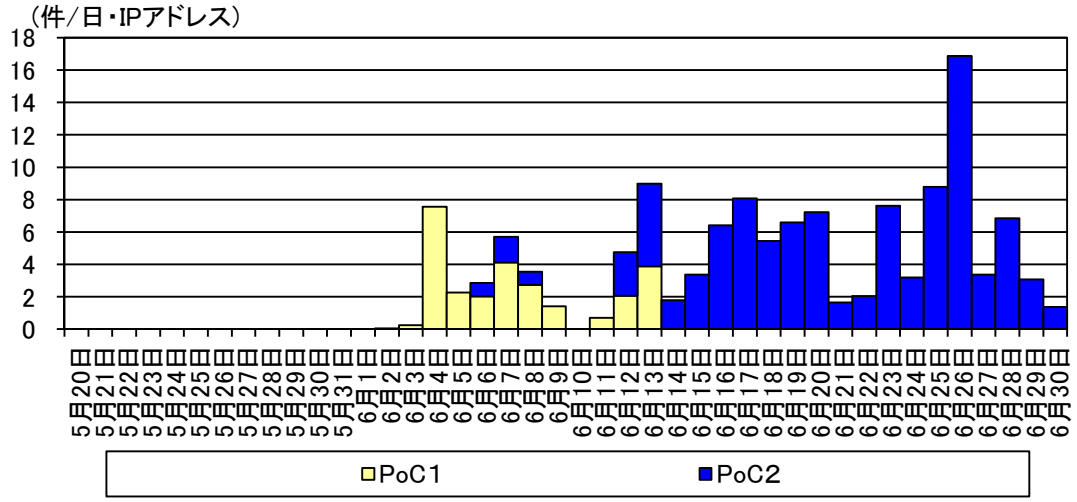

図4 宛先ポート 445/TCP に対する PoC の特徴と一致するアクセス件数の PoC 別推移
（H29.5.20～6.30）

当該脆弱性を悪用したリモートコードを実行するためには、Samba が稼動するサーバや PC において書き込み可能な共有フォルダが存在し、同フォルダに共有ライブラリファイルがアップロードされることが必要であり、リモートでコードを実行させるための条件となっています。しかしながら、アクセスを継続して観測しており、また PoC が容易に実行可能であることから注意が必

[i] http://www.samba.org/samba/security/CVE-2017-7494.html

要です。

以上のことから、Samba が稼動するサーバや PC 等を利用している場合には、次の対策を実施することを推奨します。

- 外部からの 445/TCP ポートへのアクセスを許可している場合には、可能な限り当該ポートを遮断してください。外部からのアクセスを許可する必要がある場合には、ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。
- 開発元が公開する情報を確認し、該当するバージョンの Samba を使用している場合は、修正パッチの適用又は最新バージョンへのアップデートを行い、利用している Samba を最新の状態にしてください。
- 推測されにくいユーザ名及びパスワードが設定されていること、及び、不必要な共有フォルダが設定されていないことを確認してください。
- Samba を使用する機器は、サーバや PC に限らず NAS 等の製品も含まれることから、NAS 等の製造元が公開する修正パッチやアップデート等の情報を確認してください。

3 Intel AMT の脆弱性を標的としたアクセスの観測

Intel AMT（Active Management Tecnology)とは、ビジネス向けのリモート管理機能で、リモートから電源のオン・オフ、ハードディスクの消去等の管理に加え、マウスやキーボード操作、画面の閲覧等のコンピュータの制御を行うことができます。同機能はブラウザを用いて、認証によって保護されたウェブコンソール経由で利用することができ、主に宛先ポートとして 16992/TCP 及び 16993/TCP が使用されています。

平成 29 年5月1日に開発元から、この Intel AMT を含む複数の機能に対して、深刻な脆弱性（CVE-2017-5689）が公表[i]されました。また、5月8日に JVN から同脆弱性に関する情報が国内向けに公表[ii]されています。同脆弱性が悪用された場合、認証を回避して Intel AMT のウェブコンソールにアクセスすることにより、第三者がコンピュータの制御を乗っ取ることが可能であるとされています。

警察庁のインターネット定点観測システムにおいては、同脆弱性が公表された翌日の5月2日から宛先ポート 16992/TCP 及び 16993/TCP に対するアクセスの急増を観測しました（図5）。観測したアクセスの中には、当該脆弱性が存在する機器の探索が目的と考えられる HTTP の GET リクエスト（図6）が含まれていました。

[i] 「Intel Active Management Technology, Intel Small Business Technology, and Intel Standard Manageability Escalation of Privilege」
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr

[ii] 「Intel Active Management Technology (AMT) にアクセス制限不備の脆弱性」
https://jvn.jp/vu/JVNVU92793783/

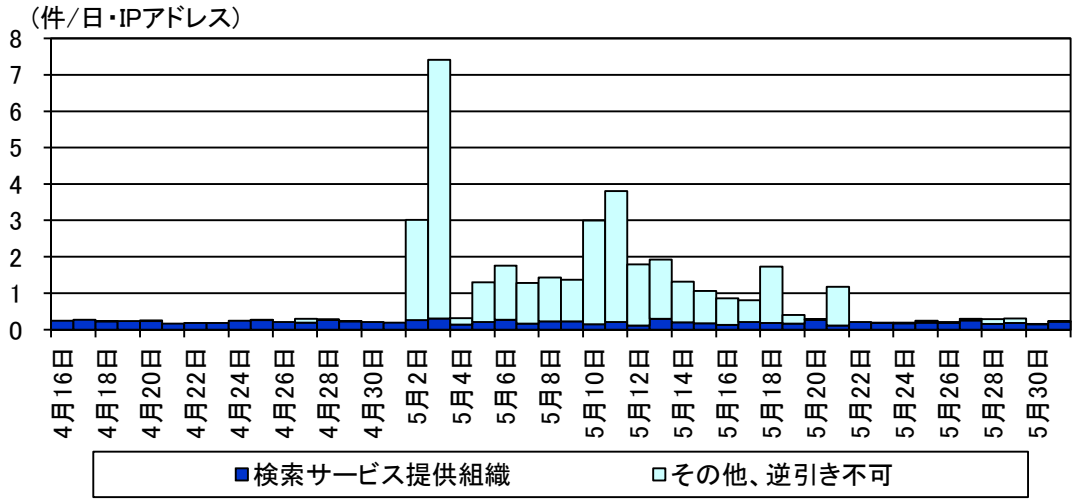

図5　宛先ポート 16992/TCP 及び 16993/TCP に対するアクセス件数の推移

```
GET /index.htm HTTP/1.1
Host: [redacted]:16992
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.13.0
```

図6　観測したアクセスのリクエスト内容（一部マスキングを実施）

これら宛先ポートに対するアクセスは、当該脆弱性が公表される以前から、検索サービス提供組織[i]を発信元 [ii] としたものを観測していましたが、5月2日以降は、当該脆弱性の悪用を意図したアクセスと考えられるものも観測しています。

これらのことから、Intel AMT の機能を有するコンピュータを使用している場合は以下の対策を早急に実施することを推奨します。

- 開発元の情報 [iii] を参考に、使用しているコンピュータが当該脆弱性の影響を受ける製品ではないか確認を実施してください。
- 使用しているコンピュータが当該脆弱性の影響を受ける機器であった場合は、各コンピュータの製造元から対策済みの最新のファームウェアへのアップデートを実施してください。
- 対策済みのファームウェアが利用できない場合、開発元の情報を参考に対策を実施してください。

[i] あらゆるサービスに対して探索を実施して結果を蓄積するとともに同結果の検索サービスを提供する組織です。同組織が運営するサイトでは、探索の結果を誰もが検索可能であるため、以前から攻撃に悪用される可能性も指摘されています。

[ii] 発信元組織は発信元 IP アドレスの DNS 逆引き結果に基づいています。

[iii] 「INTEL-sa-00075 検出と軽減ツール」
https://downloadcenter.intel.com/ja/download/26755/INTEL-sa-00075-?product=23549

- 外部からのアクセスを許可する必要がある場合には、ファイアウォール等によって不必要な外部からのアクセスを遮断する、特定の IP アドレスのみにアクセスを許可する等の適切なアクセス制限を実施してください。