Digital ESSAY

「ラズパイの脅威」

坂口 裕靖

NASA の JPL（ジェット推進研究所）のネットワークにちょろっと繋がった Raspberry Pi を踏み台として、約 500MB のデータが失われたというニュースが流れました。実際の報告書は 2019 年 6 月 19 日に公開されれていて、URL は https://oig.nasa.gov/docs/IG-19-022.pdf とのことです。今回はこの報告書を読んで、詳細を確認してみましょう。JPL のネットワークは 3 つの部分、すなわち管理用ネットワーク、ミッションの運用 / 開発用ネットワーク、DSN（Deep Space Network）用のネットワークに別れていて、合計で 26,714 台のコンピュータと 3,511 台のサーバが接続されているとのこと。でかいよね。

当然色々なところから狙われており、例えば 2009 年には国際武器取引規則・輸出管理規則により保護されるべき約 22GB のプログラムデータが、中国に位置する IP アドレス（これ、中国からの攻撃とは名言してないのがミソ）へと違法に転送される事件があった。この原因は機微情報に対するアクセスが広く許されていた点にあったため、ホストベースのファイアーウォールを設置し、セグメント化することで対処したという。

2011 年には中国に位置する IP アドレス（名言してない以下略）からの侵入者が、DSN・地球観測衛星「テラ」に搭載されている光学センサの運用等を担ってる 18 のサーバに対し侵入し、全権限を奪われるという事件が発生。侵入者はやりたい放題で、検知するまでの二週間に約 87GB のデータが持っていかれ、機密ファイルが変更されたり、アカウントがグシャグシャにされたり、隠蔽のためにログが修正されたり。この対策としては悪意ある行動をするとすぐに連絡が自動で飛ぶようなシステムを実装したとのこと。

2014 年には、ミッション運用中のサーバに対し誰でもアップロードできる状態になっていることが発見され、さらなるセグメント化と IPS（Intrusion Prevention System：不正侵入防止システム）の追加を実施。

2016 年には web サーバの設定ミスで誰でも開発ツールが使える状態になってることが判明。SSL で暗号化されてたため気づかなかったとのこと。

2017 年には JPL のサーバで地上管制用に使っていたソースコードの欠陥を利用した攻撃を受け、外部から認証なしにプログラムが実行できる状態になっていた。対策として、ソフトを使う前に事前承認が必要となるようにしたとのこと。

2018 年、外部ユーザーがネットワー

One Point BUZZ WORD　e 鎖国

アメリカはイランに対して制裁を加えていますが、その中の一つにゲームサーバへのアクセス禁止というのが含まれていてちょっとびっくりしました。具体的には dotesports の記事 https://dotesports.com/league-of-legends/news/us-government-blocks-league-in-syria-and-iran で、要するにイランとシリアのユーザーが閉め出されているとのこと。ゲーム封鎖ということですな。

経済封鎖って、要するに市民の鬱憤をたまらせて事態の打開を図るわけだから、ストレスが溜まるような施策は大変効果的でしょう。その意味でゲームを封鎖するというのは、まぁ、わからんでもないですが。こんなとこに政治が絡んでくるのか、という意味で、正直だいぶ驚きました。つーか、もっとやりようあるじゃん。

この延長線には色々なものが考えられて、「どこそこからアクセスしてくるユーザーに対してはガチャのレアキャラ払い出し確率を 1/10 にする」とか「キャラのイラスト解像度が 1/8 に落ちる」とか「アイテムの攻撃力が 1/4 になる」などなど、鬱憤をたまらせつつユーザー課金を増やすような施策はいくらでも考えつくのではないでしょうか。あるいは動画サービスで 1/24 の確率でカクるとか、1/8 の確率でステレオがモノラルになるとか、字幕で特定の文字が表示されないとか、登場人物の顔のモザイクがかかるとか。陸・海・空・宇宙に連なる、あらたなバトルフィールドが出現したことは明らかです。

ここいらへんは、サービスがネットワーク上に実装され、サーバの制御権が一点に集中しているがために実現可能ということもできるでしょう。少なくとも、ローカルのパッケージであるなら、封鎖を行うことなどできなかったはずです。とは言え、ここまで来ると google 封鎖、Office365 停止までもう一歩じゃないでしょうか。くわばらくわばら IEEE...

ク内を自由自在に動き回っていることが発覚したが、1年以上気づかなかったし、現在も詳細を調査中とのこと。発見されるまでの10ヶ月間、攻撃者は各ネットワークの弱点を丹念に探し出しては侵入することを繰り返し、23個のファイルから約500MBのデータを持ち出した。うち2つは火星探査ミッションに関係する、国際武器取引規則により規制される方法を含むファイルとのこと。これがニュースに出ていた500MBの中身。で、攻撃者はJPLの3つのネットワーク（管理系、運用系、DSN）のうち2つ（管理系、運用系）にアクセスしていることがわかったため、一時的にDSNを切り離したとのこと。肝心のRaspberry Piの話はPDFのp.19、ノンブルの12ページに出てて、この2018年の攻撃はチェックも承認もされずにネットワークに接続されていた、Raspberry Piを標的とした攻撃が発端とのこと。

この事態が判明した結果、友人飛行の管制等を行っているJSC（Johonson Space Center：ジョンソン宇宙センター）は攻撃者が侵入して来ることを危惧してJPLとのゲートウェイを遮断、さらにDSNのデータが故意に破損されたり、変更されたりした場合を危惧して利用を停止。ゲートウェイとの接続は2018年11月に復活、DSNのデータも2019年3月に一部利用を再開したが、すべてのデータを使うには至っていないという。うーん、巨大組織で一度信用が失われると、回復するのはなかなか難しいよね。特に「正しいデータ」がわからない状態だから、チェックする方法がないわけで、信用する以外ないのだし。

この後、報告書はどういう原因で穴が放置された状況が作り出されたかをざっくり調べて報告しているわけですが、まあ結局は「根気よくちゃんとやっていきましょう」という話。例えば2007年から放置されているチケットがあって、しかもその中身はすでに利用をやめたパッチインストーラをインストールする、というものだったとか、そういう感じ。こういうことをなくしていきましょう、という方向になってます。一方、Appendix Cとして、マネジメントからのコメントが載っており、10個挙げられた対策について、いつまでに何をどうやるかを返答してます。そこには公開に至る経緯も書いてあり、元のレポートは2019年5月1日付けで、マネジメントコメントが2019年6月13日付け。2019年5月17日に関係各所が集まって会議を行い、内容が承認されて公開されたのがこのレポートとのこと。さすがちゃんとしてらっしゃる。

10個出てきた勧告のうち、No.8の「正式な、文書化された脅威検出（threat hunting）手順を確立すること：役割と責任範囲、検出の標準的手順、追跡を成功させるために必要な指標等を含む」について、「NASAは同意しかねる。そりゃNISTの役割だ。NISTが決めたら検討する」と返してたのは面白い。まあそうだよね、NASAが決めるべきものではないし、ましてや契約先のCaltechが作るべきもんでもない。実施予定の日付については早めにできるものは2019年9月30日まで、時間がかかるものは2020年1月15日までに終えるとのこと。3万台近くを半年程度で対処するのか…とてもとても大変そうだけど、予算がちゃんと出るならどうにかなるのでしょう。最後にAppendix Dとして、レポートの配布先がずらずら並んでおります。

具体的にどうやって侵入したかは不明ですが、怖いのはRaspberry Piがあまりに小さく、USBのコネクタさえあればどこにでも設置できる上に、これ自体が一個の独立したコンピュータですから、コンピュータにできることなら一通りできてしまうことです。例えばVPNサーバを仕込んで、しれっとネットワークの片隅に接続しておくと、外部からRaspberry Piに接続することができてしまいます。Raspberry Piに接続できるということは、そこを足がかりにしてネットワークにアクセスできるということを意味します。あとは放置されてる脆弱性を探していって、次の足場にして…ということを繰り返していたのでしょう、きっと。まあいくらなんでもVPNサーバを仕込んだRaspberry Piを、誰にも報告せずに、ネットワークにそっと接続する時点で悪意100%な気もしますが、そもそも何かの実験用だったかもしれませんし、wifiを閉じ忘れただけかもしれませんので、なんとも言えません。ただ、本気出してごまかそうとされるとどうにもならないのが正直なところです。例えば、ぱっと見外付けハードディスクみたいなケースに入ってて、ホコリだらけになってるマシンの裏側に転がしてあったら、見つけることは困難でしょう。それでも通信には有線もしくは無線のMAC ADDRESSが必要なはずですから、頑張ってスキャンすれば存在を見つけることはできるかもしれません。ただ、そいつが物理的にどこにあるかがわからないと、止める手立てがありません。有線の場合は線をたどれば必ず見つかりますが、無線の場合は絶望的です。それを調査するような予算もない場合、逆にできることは無線にMAC ADDRESS制限をかけることぐらいでしょう。結局地道な作業が一番効果的ってわけ。

Hiroyasu Sakaguchi
株式会社 IMAGICA Lab.