ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●IoTマルウェアが激増…Telnetのパスワードや脆弱性を悪用

http://www.itmedia.co.jp/news/articles/1809/21/news072.html

このニュースをザックリ言うと・・・

- 9月18日（現地時間）、セキュリティベンダーのKaspersky社より、2018年上半期におけるIoTマルウェアの検出数が2017年の年間検出数の3.7倍に上ったとする報告が発表されました。

- 発表によれば、2016年と2017年の年間検出数がそれぞれ3,219件と32,614件なのに対し、2018年は上半期だけで121,588件を検出したとのことです。

- マルウェアがIoTデバイスに感染するための手口としては、Telnetのパスワードクラッキングによるものが75.40%と最も多かった一方、それに対する対策を受けて、ファームウェアの脆弱性を突く攻撃にシフトする傾向も見られている模様です。

AUS便りからの所感等

- IoTという概念が「セキュリティ攻撃のターゲットとしても」注目されるようになり、特に2016年9月頃から「Mirai」やその亜種の活動が始まったことが検出数の爆発的増加に現れていると考えられます。

- Telnetという古いプロトコルが依然としてIoT機器の管理目的で使用されていたことや、そういったサービスポートに外部からアクセス可能で、かつパスワードをデフォルトから変更しない状態の機器あるいはネットワークが多く存在したことが皮肉にもマルウェアによって洗い出される形になったと言えます。

- 次の代表的なものをはじめとする各種対策をどれか一つだけではなく複数行い、PCよりも管理の目が向きにくいことを意識して確実な管理体制をとることが重要です。

◆適切なパスワードを設定する
◆ファームウェアを適宜アップデートする（できないものは場合によっては交換も検討する）
◆（UTM等も活用しつつ）不特定多数からサービスポートにアクセスされないようにする

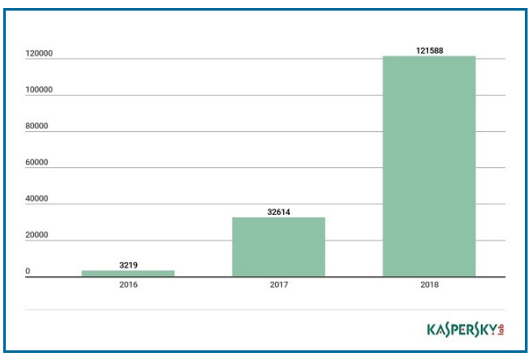
ITmedia NEWS

IoTマルウェアが激増　Telnetのパスワードや脆弱性を悪用

2018年09月21日 10時30分 公開　[鈴木聖子，ITmedia]

印刷　通知　40　12　B!　2

IoTデバイスを狙う攻撃が世界中で増大している。ロシアのセキュリティ企業Kaspersky Labは9月18日に発表した2018年上半期の報告の中で、この半年間に検出されたIoTマルウェアの数は、2017年の年間を通じて検出された数の3倍に上ったと伝えた。

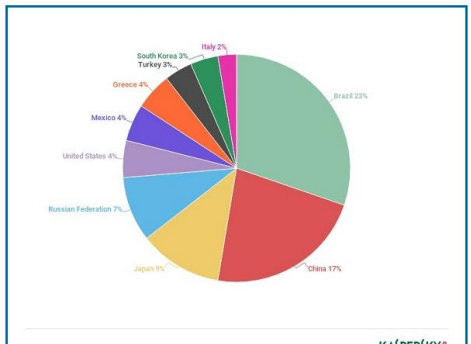


Kaspersky Labの調査によると、2018年の上半期に検出されたIoTマルウェアの数は、2017年の1年間で検出された数の3倍に上った（出典：Kaspersky Lab）

IoTマルウェアは、パスワードをデフォルトのまま変更していない機器や、脆弱性が放置されている機器を狙う傾向がある。Kaspersky によると、同社のおとり用のハニーポットに対する攻撃では、Telnetのパスワードクラッキングを通じてマルウェアに感染させる手口が最多の75.40%を占めた。次いでSSHのパスワードクラッキングが11.59%となっている。

Telnetパスワードクラッキング攻撃の発信源を国別にみると、1位がブラジルの23%、2位の中国は17%、日本は9%で3位だった。

ただ、ユーザーがTelnetのデフォルトのパスワードを変更するようになり、Telnetをサポートしない機器も増える中、ルータなどのソフトウェアの既知の脆弱性を狙うマルウェアが台頭しつつあるという。



Telnetパスワードクラッキング攻撃の発信源を国別にみると、1位がブラジルの23%、2位の中国は17%、日本は9%で3位だった（出典：Kaspersky Lab）

●島田市、1,800人分の個人情報流出か…フリーメールに不正アクセス

http://www.at-s.com/news/article/social/shizuoka/546714.html

このニュースをザックリ言うと・・・

- 9月28日（日本時間）、静岡県島田市より、同市が管理していた個人情報のうち約1,800人分が流出した可能性があると発表されました。

- 発表によれば、同市農林課の複数の職員が業務で「フリーメール」を使用しており、そのアカウントが不正アクセスを受けたことが流出の原因としています。

AUS便りからの所感等


@S 静岡新聞 SBS

フリーメール業務使用　島田市、１８００人分の情報流出か

（2018/9/29 07:11）

島田市は２８日、農林課の複数の職員がフリーメールを業務使用して不正アクセスを受け、２４４６件、約１８００人分の個人情報が流出した可能性があると発表した。対象者への通知を始めているが、２８日時点で漏えいに伴う被害は確認されていない。

市によると、原則フリーメールを業務で使わないとする内規があるが、他の３課でもフリーメールを使用していた。他の３課については「不正アクセスされた形跡がないことを確認した」として明らかにしていない。

市によると、農林課は２０１５年１０月からフリーメールを使用。複数の職員がスキャナーなどで取り込んだ文書やデータをフリーメールで個々の執務用パソコンに送付していた。漏えいした可能性があるのは、住所や氏名、電話番号などが書かれた補助金申請書や関係団体の名簿、免許証など。金融機関の口座情報１２件については、自宅訪問するなどして説明している。

１８日に職員が不正アクセスの警告メールに気づき、使用停止した。確認できるだけで米国、中国、台湾などから１５回の不正アクセスがあった。萬屋正副市長は記者会見で「市民の安全安心を脅かしかねない。再発防止策を徹底する」とした。

謝罪会見する萬屋正副市長（左）＝２８日午後、島田市役所

- 同課では業務上でのフリーメールの利用を内規で禁止していましたが、複数の職員がスキャナー等で取り込んだ文書やデータを執務用PCに送付するために使用しており、その文書の一部に含まれていた個人情報にアクセスされたとみられています。

- 「セキュリティ対策は最も弱いところから突破される」とよく言われますが、今回のようなケースで問われるべきは、単に「禁止されている」ことではなく、例えば、適切なパスワードや二段階認証等を設定していないような「安全に管理されていない」ものを使用したことでしょう。

- 業種によるものではありますが、単に情報管理手段を制限する場合であっても、クラウドサービスの利用やBYOD（個人が所有する機器の業務利用）を認める場合であっても、UTM等の導入によるデータの出入りや、資産管理ソリューション等の導入による機器・サービスの利用を適切に把握・管理しているかが結局はセキュリティ面で重要なこととなります。

●Adobe AcrobatとReaderの定例外セキュリティアップデート…約2週間後にも再度アップデート予定

http://www.itmedia.co.jp/news/articles/1809/28/news079.html

このニュースをザックリ言うと・・・

- 9月19日（現地時間）、Adobe社より、「Acrobat/Acrobat DC」「Acrobat Reader/Reader DC」の定例外セキュリティアップデートがリリースされました。

- 同日にリリースされたバージョンは2018.011.20063（連続トラック）、2017.011.30102（Classic 2017）、2015.006.30452（Classic 2015）となっており、不正なPDFファイルを開くことでPCを乗っ取られる可能性のある脆弱性が修正されています。

- その後同27日には、前述の最新バージョンまでに含まれている未修正の脆弱性について、10月2日に新たな定例外アップデートのリリースが予告されています。

AUS便りからの所感等


ITmedia NEWS

Adobe Acrobat/Readerに脆弱性、Adobeがセキュリティアップデート公開を予告

2018年09月28日 11時00分 公開　[鈴木聖子, ITmedia]

印刷　通知　25　1　B! 1

Adobe Systemsは、WindowsとmacOS向けに、Adobe Acrobat（以下、Acrobat）とAdobe Acrobat Reader（以下、Reader）のセキュリティアップデートを米国時間の2018年10月2日に公開すると予告した。

Adobe Systemsのセキュリティ情報によると、10月2日のアップデートでは、複数の脆弱（ぜいじゃく）性の修正を予定している。脆弱性が存在するのは、Acrobat DC/Reader DCの連続トラックの2018.011.20063までのバージョンと、Acrobat 2017/Reader DC 2017のクラシック2017トラックの2017.011.30102までのバージョン、およびAcrobat DC/Reader DCのクラシック2015トラックの2015.006.30452までのバージョン。優先度は「2」に分類されている。

- AcrobatおよびReaderのセキュリティアップデートは、近年は3ヶ月に一度のペースでリリースされてましたが、7月以降毎月リリースと頻度が高くなっています。

- 今では、Chrome・Firefox・Edgeといった各種ブラウザにPDFリーダー機能が搭載されており、全ての場面でAdobe ReaderでPDFファイルを開く必要はなくなってきています。

- 前述のブラウザ等、Adobe以外のPDFリーダーを利用することはセキュリティリスクを考慮する意味でも有効ですが、これらのソフトウェアについてもまたアップデートが必要であることに注意し、アンチウイルス・UTMによる防御との両面を怠りなく実施するよう心がけてください。