重要生活機器の脅威事例集

2017年度の脅威事例

2017年2月3日

一般社団法人重要生活機器連携
セキュリティ協議会（CCDS）事務局

台湾製のホームルーターにおける脆弱性

分　類	実例	分野	ネットワーク	時期	2014/02	地域	米国他

情報源

FEDERAL TRADE COMMISION
「ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk」
https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

脅威

ホールルータの脆弱性による機密情報(個人情報)の漏えい、インターネットからのストレージへの不正アクセス

概要

■概要
・米FEDERAL TRADE COMMISIN（FTC）は、台湾のコンピュータ・ハードウェアメーカASUS Tek Computer, inc.のホームルータに脆弱性があり、2014年2月には、脆弱性を悪用した不正アクセスにより12,900件の個人データが流出したと報告を行った。

■インシデント詳細
・ASUSのルータは全ての機器のユーザ名とパスワードが「admin/admin」に設定されているほか、多くの設計上の脆弱性を指摘されている。
・同社のAiCloud、AiDiskと呼ばれるサービスは、ユーザがUSBメディアをルータに接続して、クラウドストレージを構築する仕組みとしていたため、ハッカーはAiCloudの脆弱性を利用してログイン画面を迂回し、Webブラウザからユーザのクラウドストレージへのアクセス権を取得することができた。
・同様に、AiDiskサービスでは、格納されたデータが暗号化されていないため、インターネットからストレージ内への不正アクセスが可能となっていた。
・2014年2月には、ハッカーは容易に入手可能なツールを使用して、ASUSのルータを検出し、12,900件を超えるユーザのストレージデバイスへの不正アクセスを行っていたとされる。

■FTCの対応
・この問題は米FTCとASUSの間で訴訟に発展し、ASUSは今後20年間、独立監査の対象となる他、ソフトウェアのアップデートやユーザへの注意喚起など、包括的なセキュリティプログラムを確立し、維持していく必要がある。

「Mirai」ボットネットによるDDoS攻撃

分　類	実例	分野	ネットワーク	時期	2016/09	地域	米国他

情報源	The ZERO/ONE「100万台以上のIoT機器がマルウェアに感染しDDoS攻撃。IoTは今後も狙われる」 https://the01.jp/p0004125/
脅威	マルウェア感染したIoTデバイス（防犯カメラやルータなど）を踏み台とした、非常に大規模なDDoS攻撃

概要

■概要
・米国の著名なセキュリティブログ「Krebs on Security」が、「Mirai」というボットネットに感染したIoTデバイス（防犯カメラやルータなど）を踏み台に、非常に大規模なDDoS攻撃を受けた。

■インシデント詳細
・ 2016年9月10日、「Krebs on Security」は大規模なDoS攻撃を受けている事を自身のサイトで報告。大規模なDoS攻撃は620Gbpsに達したと言われ、同サイトのサービスプロバイダ「Akamai」でも対処ができず、一時期サイトの公開中止となった。
・「Mirai」と呼ばれるマルウェアは、「工場出荷時のデフォルトのままの、あるいはハードコードされたユーザー名とパスワードによって保護されているIoTのシステム」をインターネット上でスキャンし、脆弱なデバイスを探し出して拡散する。
・Miraiは数十万台の機器に感染してボットネットを構築したというが、それを上回る100万台以上の機器からなるボットネットを作り上げたと言われるBashlightマルウェアも確認されている。

・同様のボットネットによる大規模なDDoS攻撃は、 「Krebs on Security」に次いで、フランスのISPであるOVH社が攻撃を受け、同社はこれが1Tbpsの規模だったとしている。さらに10月には、DNSサービスを運営するアメリカのDyn社が攻撃に見舞われた。

米航空宇宙局（NASA）へのハッキング事例

分　類	実例	分野	ネットワーク ・航空宇宙	時期	2011-12	地域	米国
情報源	産経ニュース「人工衛星をハックして墜落させる？　空想ではない宇宙サイバーテロの危険」 http://www.sankei.com/smp/wired/news/130628/wir1306280002-s.html BBC「Hackers had 'full functional control' of Nasa computers」 http://www.bbc.com/news/technology-17231695						
脅威	米ジェット推進研究所(JPL)のコンピュータにおける物理的な脆弱性及び、ネットワーク上の脆弱性						
概要							

■概要
・2012年、米航空宇宙局（NASA）、ジェット推進研究所(JPL)のコンピュータがハッキングを受けた。

■インシデント詳細
・調査委員会の報告によれば、ハッキング時、コンピュータは完全にハッカーの制御下に置かれ、重要なファイルの改変（コピー、削除）や、ユーザー認証情報を盗むためのウイルスを仕込む事で、NASAのほかのシステムに損害を与えることが可能であった。

・また2011年には、国際宇宙ステーション(ISS)の制御コードが記録されたコンピュータの盗難も発生しており、攻撃に悪用されればステーション内の宇宙飛行士たちを、生命の危険に晒す可能性もあった。

人工衛星に対するハッキングレポート

分　類	実例	分野	ネットワーク ・航空宇宙	時期	2015	地域	米国
情報源	[3] BLACK HAT USA 2015 「SPREAD SPECTRUM SATCOM HACKING　ATTACKING THE GLOBALSTAR SIMPLEX DATA SERVICE」						
脅威	人衛星のトランスミッタの脆弱性（通信傍受、偽装、改ざん、インテリジェント妨害など）						
概要							

■概要
・Black hat USA 2015において、人工衛星のハッキングに対するレポート報告が行われた。

■インシデント詳細
・人工衛星は、そもそもハッキングを前提とした設計になっておらず、衛星の制御はできなくても、誤った情報を送信することは可能であると発表された。これにより、航空機に不正な航空情報を送信して混乱させたり、貨物船なのどの位置情報を特定出来ないように出来るため、密入国や禁製品の輸送など、犯罪に使われる危険が大きくなる。

・具体的には、人口衛星Globalstarに使用されるトランスミッタには、通信傍受、偽装、改ざん、インテリジェント妨害に関する設計・実装上の欠陥があり、12万円程度の費用で、ハッキングが可能であるという。

ノートPCほどの大きさの装置で人工衛星をハッキングできる（Blachat2015）

米人工衛星２基に対するハッキング事例

分　類	実例	分野	ネットワーク ・航空宇宙	時期	2007-8	地域	米国

情報源

[1]Reuters　「米人工衛星2基にハッキング、中国軍が関与の疑い＝調査委員」
http://jp.mobile.reuters.com/article/worldNews/idJPJAPAN-23894420111029
[2]Newsweek「中国、世界初のハッキング不能な量子通信衛星を打ち上げ」
http://www.newsweekjapan.jp/stories/world/2016/08/post-5662.php

脅威

衛星通信における危険度の高い脆弱性（傍受や制御コマンドの不正操作、遮断の被害など）

概要

■概要
・2007年と2008年に、米航空宇宙局（NASA）と米地質調査所（USGS）の人工衛星２基（Landsat-7とTerra）が、ハッカーにより攻撃を受けた。(中国による攻撃と推定)

■インシデント詳細
・4回にわたり、数分間2基の制御を完全に奪取された。1基は2007年と08年に計12分以上の妨害を受け、もう1基は2008年6月に2分以上、同年10月に9分以上の妨害を受けた。
・ハッキングは、ノルウェーの地上施設を経由して行われていたが、施設を所有する企業によると、システム上に異常は見られなかった。

■参考情報：対策事例
・一方で中国では、人工衛星のセキュリティや安全性を高めるため、通信の傍受、解読が不可能な量子科学実験衛星（QUESS）の打ち上げを行った。[2]

商業衛星通信を経由したマルウェア攻撃

分　類	実例	分野	ネットワーク・航空宇宙	時期	2015/09	地域	各国

情報源

[1]サイバーセキュリティ.com　「ロシアの集団、衛星をサイバー攻撃で非難砲火を浴びる」
https://cybersecurity-jp.com/security-measures/5477
[2]DNA　「ドイツのハッカー、検閲を避けるため独自の通信衛星の打ち上げを計画中」
http://dailynewsagency.com/2012/01/07/hackers-satellite/

脅威

商業衛星通信におけるプロトコル上の脆弱性

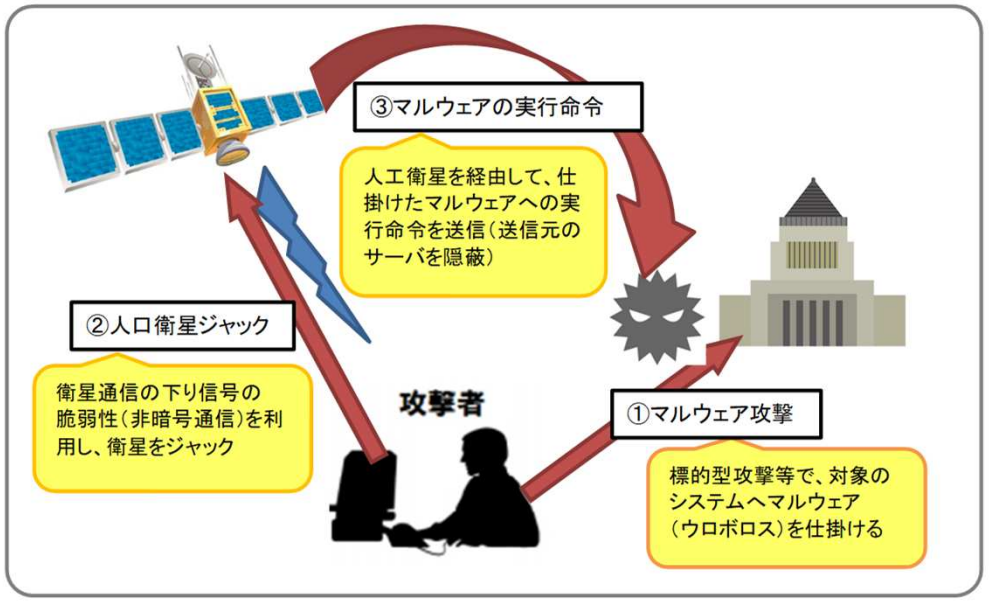
概要

■概要
・カスペルスキーのセキュリティリサーチャーは、ハッカー集団「Turla」が、商業衛星通信を経由し、マルウェアによるハッキングを行っていたことを報告した。

■インシデント詳細
・標的に「ウロボロス」というマルウェアを感染させて、内部の情報を抜き取るが、衛星通信を経由することでマルウェアに指示を出す指揮統制サーバーの居場所を隠蔽している。

・通信網がまだ整備されていない地域で使われている衛星通信の下り回線は、データが暗号化されていないので、比較的簡単にジャックができる。また、中東とアフリカ諸国の衛星通信に接続するIPアドレスを悪用し、セキュリティ企業による検知を逃れている。

■参考)
・一方でドイツでは、ハッカー集団が検閲を避ける目的で、独自の衛星を打ち上げる計画を発表し、議論を生んでいる。[2]



図：衛星経由の攻撃プロセス（CCDS事務局）

新種のマルウェア「ウロボロス」の事例

分　類	実例	分野	ネットワーク	時期	2014/03	地域	各国
情報源	マイナビニュース　「G Data、新種マルウェア「ウロボロス」を発見 - ネット非接続のPCも感染」 http://news.mynavi.jp/news/2014/03/07/072/						
脅威	新種のマルウェア「ウロボロス」による機密情報の漏えい、遠隔操作による他機器への命令実行						
概要							

■概要
・ドイツのセキュリティソフト会社G DataSoftware AGは新種マルウェア「ウロボロス」についての報告レポートを公開した。

■インシデント詳細
・「ウロボロス」は、 直接インターネットにつながっていないコンピュータから機密情報を盗み出す高度な仕組みをもったルートキット。

・感染するとマシンを外部から操られ、気付かれることなくファイルを盗み出すことや、ネットワークのトラフィックを妨害することが確認されている。また、P2Pモードで動作するように設計されているので、相互に通信を行っているマシンが感染してしまうと、攻撃側は遠隔操作によってインターネットに接続していないマシンに対しても命令を実行できるようになる。

・ウロボロスの侵入経路は、USBメモリを使ったものが発見されているほか、スピアフィッシングやドライブバイダウンロード、またはソーシャルエンジニアリング攻撃など、多くの感染経路が考えられるが詳細は不明。

バングラディシュの中央銀行に対するハッキング

分　類	実例	分野	ネットワーク、金融端末	時期	2016/02	地域	バングラディシュ

情報源	The ZERO/ONE「バングラデシュ中央銀行がハッキングにより多額の不正送金被害」 https://the01.jp/p0003966/
脅威	金融端末へのハッキング、不正送金
概要	

■概要
・ニューヨーク連邦銀行にあるバングラデシュ銀行(バングラディシュの中央銀行)の外貨準備金口座に対し、バングラデシュ銀行の端末から30回以上の送金指示が送られ、合計8100万ドル（同約95億円）が失われた。

■インシデント詳細
・2016年2月4日から5日にかけて、ニューヨーク連邦銀行にあるバングラデシュ銀行(バングラディシュの中央銀行)の外貨準備金口座に対し、バングラデシュ銀行の端末から30回以上の送金指示が送られた。
・銀行間の取引に使われるSWIFT（Society for Worldwide Interbank Financial Telecommunication：国際銀行間通信協会）というシステムへのハッキングが懸念されたが、調査により、今回のケースではバングラデシュ銀行側の端末がハッキングされた事が原因であると判明した。
・ただ、銀行内部のSWIFTの認証情報を窃取した上で、SWIFTのメッセージなどを操作する機能を持つというマルウェアが見つかったと言われており、マルウェアの作者は銀行のシステムやSWIFTに関する十分な知識を持っていたと考えられる。そのマルウェアの侵入経路についてはまだよくわかっていないようだが、フィッシングメールによる可能性が高いと見られている。
・今回のケースの最大の原因はバングラデシュ銀行のセキュリティ体制がお粗末だったことにあるようだ。ファイアウォールによる防備が不十分だったことや、一般ネットワークとSWIFTシステムが接続されていたことなどが指摘されている。

ホテルの電子カードキーシステムの乗っ取り

分　類	実例	分野	ネットワーク、金融端末	時期	2017/01	地域	オーストリア
情報源	The ZERO/ONE「高級ホテルの電子カードキーシステムがランサムウェアに襲われる」 https://the01.jp/p0004410/						
脅威	ランサムウェア感染						
概要							

■概要
・オーストリアの4つ星高級ホテル「Romantik Seehotel Jägerwirt」の電子キーカードシステムがランサムウェアに感染し、約１８０名の宿泊者が部屋への入退出ができない状態となった。

■インシデント詳細
・サイバー犯罪者が内部のキーマネージメントシステムに侵入し、コンピューターシステム全体を乗っ取り、このホテルの予約システムやレジシステムを含むほぼ全ての機能を麻痺させた。
・ホテルの運営者側は、ランサムウェアに感染した電子キーカードシステムを回復させるために1500ユーロ(約18万円)をビットコインで支払わざるをを得なかった。