過去に起きた攻撃および脆弱性を弊社が先に確認した実績例

Nov.2015

パロアルトネットワーク株式会社

paloalto NETWORKS®
the enterprise security company™

Adobe関連

- 脆弱性
  - ADOBE SHOCKWAVE PLAYERに存在する重大な脆弱性を発見（2015.09.09）

    Windows版Adobe Shockwave Playerのバージョン12.1.9.160以前に影響を及ぼす重大な脆弱性を発見

    https://www.paloaltonetworks.jp/company/in-the-news/2015/palo-alto-networks-researchers-discover-critical-vulnerabilities-in-internet-explorer-and-adobe-shockwave-player.html

    （Adobe情報）

    https://helpx.adobe.com/security/products/shockwave/apsb15-22.html

IE関連

- 脆弱性
  - INTERNET EXPLORERに存在する重大な脆弱性を発見重大な脆弱性を発見（2015.09.09）

    Microsoft Internet Explorer 6、7、 8、9、10、11に影響を及ぼす脆弱性を新たに3件発見

    https://www.paloaltonetworks.jp/company/in-the-news/2015/palo-alto-networks-researchers-discover-critical-vulnerabilities-in-internet-explorer-and-adobe-shockwave-player.html

    （MS情報）

    https://technet.microsoft.com/ja-jp/library/security/ms15-sep.aspx

- 過去1年半で発見したIEの脆弱性について（2015.09.09）

  過去1年半で発見したIEの脆弱性は、69件

  2015年　14件

  今年7月の2件、6月の3件、5月の3件、3月の1件、2月の5件

  2014年　55件

  2014年11月の3件、2014年10月の1件、2014年9月の15件、2014年8月の3件、2014年7月の10件、2014年6月の22件

パロアルトネットワークスは、脆弱性の積極的な発見、顧客向けプロテクションの開発、パッチ適用の為のMicrosoftへの情報共有などを通じて、企業ネットワークの情報漏えいを狙った攻撃の脅威を取り除くことに尽力しています。

IOS関連

- マルウェア
  - プライベートAPIを悪用して非ジュエルブレイクIOS端末を攻撃する初のIOSマルウェア（2015.10.04）

    新しいApple iOSマルウェアを発見「YiSpecter（イースペクター）」

    YiSpecterは、iOSシステム内でプライベートAPIを不正使用し、ジェイルブレイクされたiOS端末だけでなくジェイルブレイクされていない端末も攻撃する、インターネット上で初めて確認されたマルウェアです。

    https://www.paloaltonetworks.jp/company/in-the-news/2015/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis.html
  - 22万5000件超のAPPLEアカウントを盗用するIOS マルウェア（2015.09.01）

    中国の調査グループ「WeipTech」は ユーザーによって報告された不審なiOS 脱獄アプリの分析を行い、サーバー上に保存された22万5000件の有効なAppleのアカウントとパスワードを発見。

    パロアルトネットワークスはWeipTechと協力し、インターネット上で新しいiOSマルウェア群のサンプルを92個識別しました。それら制作者の最終的な目的を究明すべくサンプルを分析し、このマルウェアを「KeyRaider」と命名しました。パロアルトネットワークスでは、本件がマルウェアを原因とした過去最大規模のAppleアカウント盗難事例と考えています。

    https://www.paloaltonetworks.jp/company/in-the-news/2015/KeyRaider-iOS-Malware-Steals-Over-225000-Apple-Accounts-to-Create-Free-App-Utopia1.html

Android関連

- マルウェア
  - 人気の広告ライブラリを用いてアンチウイルス検知を回避する新種のANDROIDマルウェア群を発見（2015.07.07）

    「VirusTotal」※1が提供するすべてのアンチウイルス製品を回避できる新種のAndroidマルウェア群を発見

    このマルウェア群はその悪質な主機能名から「Gunpoder」と名付けられ、Unit 42は3種類の亜種マルウェアを49件のサンプルから検出しました。

    今回の注目点は、アンチウイルス製品では従来防御されてこなかった「アドウェア」と、被害をもたらす「マルウェア」の間には微妙な差しかないということが明らかになりました。

    https://www.paloaltonetworks.jp/company/in-the-news/2015/07-14-new-android-malware-family-evades-antivirus-detection-by-using-popular-ad-libraries.html

