2015 年 12 月 16 日

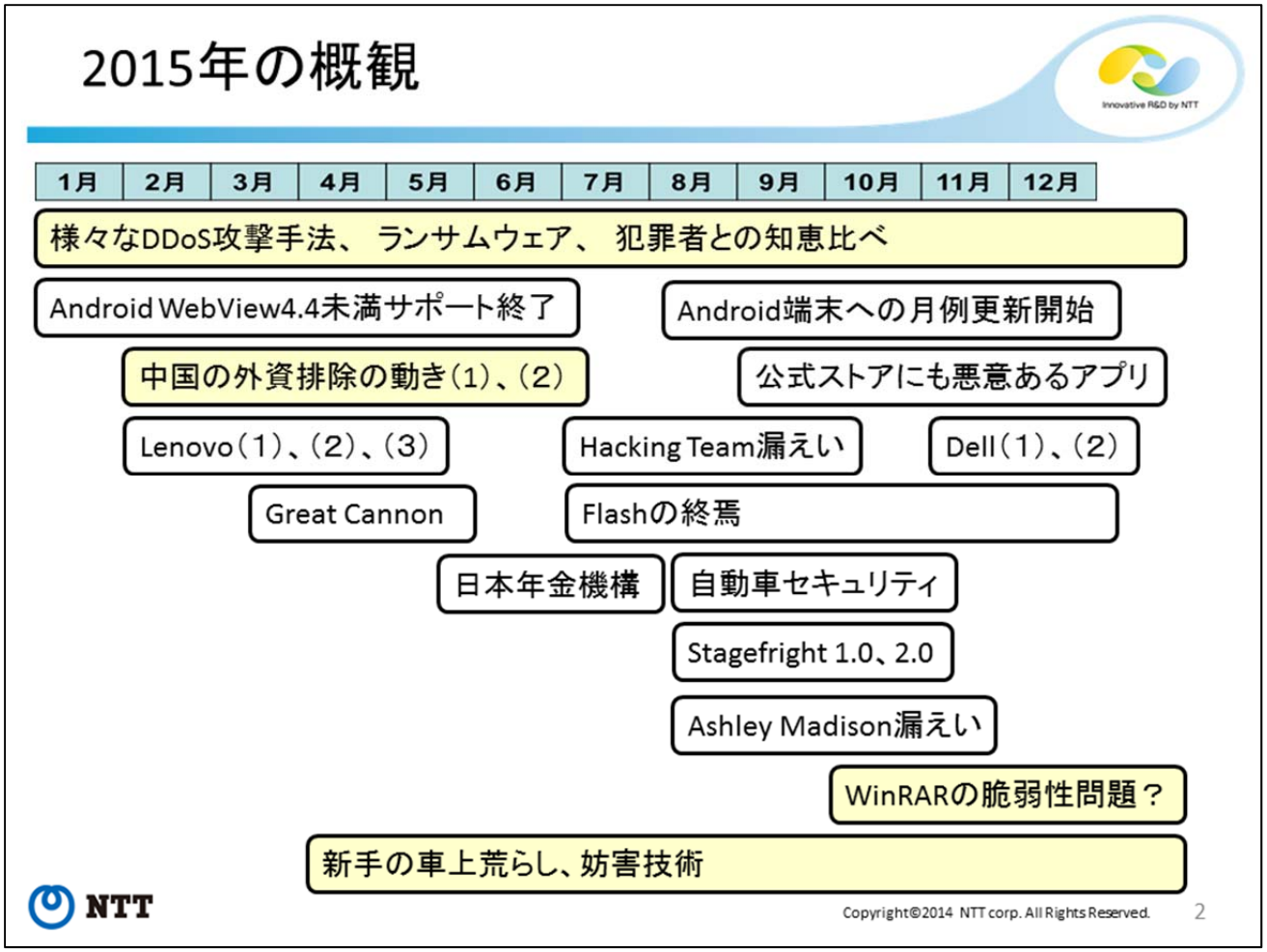
「2015 年 一年のセキュリティを振り返る」（配布用資料）

NTT セキュアプラットフォーム研究所

遠藤 斉、CISSP、CISM

●はじめに

本資料は講演スライドそのものではありません。講演スライドで参照した記事のリファレンスとなります。講演で気になった話題について詳細を知りたい、原文で確認したい場合などにご活用ください。



■様々な DDoS の攻撃手法

・Portmapper

UDP-based Portmap latest target for DDoS attackers looking to amplify attacks

http://www.net-security.org/secworld.php?id=18789

・BitTorrent

Exploiting BitTorrent flaws to run Distributed Reflective DDoS

http://securityaffairs.co/wordpress/39382/hacking/bittorrent-ddos.html

BitTorrent Fixes Reflective DDoS Attack Security Flaw

http://thehackernews.com/2015/08/bittorrent-dos-attack_28.html

・NetBIOS name server、Sentinel licensing servers

New DDoS attacks misuse NetBIOS name server, RPC portmap, and Sentinel licensing servers
http://www.net-security.org/secworld.php?id=19039
アカマイ、3 種類の新たなリフレクション DDoS 攻撃ベクトルについて警告
http://internet.watch.impress.co.jp/docs/release/20151030_728118.html
・監視カメラ
Hacking CCTV Cameras to Launch DDoS Attacks
http://thehackernews.com/2015/10/cctv-camera-hacking.html
・Great Cannon
China's Anti-Censorship Service Hit by First DDoS Attack
http://www.hotforsecurity.com/blog/chinas-anti-censorship-service-hit-by-first-ddos-attack-11589.html
China's Great Cannon
https://citizenlab.org/2015/04/chinas-great-cannon/

■ランサムウェアの動向
・暴露型
Chimera Ransomware Threatens to Publish Personal Files
http://news.softpedia.com/news/chimera-ransomware-threatens-to-publish-personal-files-495617.shtml
・孤立系
Offline Ransomware Encrypts Your Data without C&C Communication
http://blog.checkpoint.com/2015/11/04/offline-ransomware-encrypts-your-data-without-cc-communication/
・Ransomware-as-a-service
FAKBEN Ransomware-as-a-service emerges from the underground
http://securityaffairs.co/wordpress/41950/cyber-crime/fakben-ransomware-as-a-service.html

■犯罪者との知恵比べ
USBKill used to wipe clean criminal's PCs
http://securityaffairs.co/wordpress/36554/cyber-crime/usbkill-wipe-clean-criminals-pcs.html
How Carders Can Use eBay as a Virtual ATM
http://krebsonsecurity.com/2015/11/how-carders-can-use-ebay-as-a-virtual-atm/
Russian ATM Hackers Steal $4 Million in Cash with 'Reverse ATM Hack' Technique
http://thehackernews.com/2015/11/atm-hacker.html
http://www.forbes.com/sites/thomasbrewster/2015/11/23/visa-mastercard-atm-fraud-hackers-steal-millions-dollars/

■新手の車上荒らし、妨害技術

Keeping Your Car Safe From Electronic Thieves

http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html

Could thieves use jamming technology to steal your car?

http://www.theguardian.com/technology/2015/may/26/high-tech-thieves-jamming-technology-steal-car

RollJam - $30 Device That Unlocks Almost Any Car And Garage Door

http://thehackernews.com/2015/08/rolljam-unlock-car-garage.html

WiFi jamming attacks more simple and cheaper than ever

http://www.net-security.org/secworld.php?id=18971

Seeing stars, again: Naval Academy reinstates celestial navigation

http://www.capitalgazette.com/news/naval_academy/ph-ac-cn-celestial-navigation-1014-20151009-story.html

■WinRAR の脆弱性問題？

WinRAR に脆弱性報告、遠隔操作される恐れ

http://www.itmedia.co.jp/enterprise/articles/1510/01/news097.html

WinRAR SFX v5.21 - Remote Code Execution Vulnerability

http://seclists.org/fulldisclosure/2015/Sep/106

WinRAR RARLab

http://www.rarlab.com/vuln_sfx_html2.htm

REDACTION: WinRAR Vulnerability

https://blog.malwarebytes.org/news/2015/10/redaction-winrar-vulnerability/

■中国の外資排除の動き

(1)

US tech firms ask China to postpone 'intrusive' rules

http://www.bbc.co.uk/news/technology-31039227

U.S. consistently raised concerns with China on IT rules: trade office

http://www.reuters.com/article/2015/01/29/us-china-tech-security-ustr-idUSKBN0L22JZ20150129

Tech Firms Required to Add Backdoors in Hardware, Software for Selling in China

http://www.techworm.net/2015/02/tech-firms-required-add-backdoors-hardware-software-selling-china.html

Exclusive: Obama sharply criticizes China's plans for new technology rules

http://www.reuters.com/article/2015/03/02/us-usa-obama-china-idUSKBN0LY2H520150302

Washington says waiting for China response on tech rule concerns

http://www.reuters.com/article/2015/03/02/us-china-tech-regulations-usa-idUSKBN0LY2F920150302

Global push aims to change China's mind on bank rules: U.S. official

http://www.reuters.com/article/2015/03/18/us-china-security-usa-idUSKBN0ME1WV20150318
U.S. questions China at WTO on banking technology restrictions
http://www.reuters.com/article/2015/03/26/us-china-tech-usa-idUSKBN0MM26320150326
China suspends bank tech restrictions: U.S. Treasury official
http://www.reuters.com/article/2015/03/30/us-usa-china-jacklew-idUSKBN0MQ20S20150330

(2)
Foreign business lobbies ask China to revise cyber insurance draft rules
http://www.reuters.com/article/2015/11/05/us-china-cybersecurity-insurance-idUSKCN0SU17O20151105

■公式ストアもあぶない
・XcodeGhost
Apple cleaning up iOS App Store after first major attack
http://www.reuters.com/article/2015/09/21/us-apple-china-malware-idUSKCN0RK0ZB20150921
・Youmi SDK
Apple to Remove 256 iOS Apps Using Private APIs, Collecting Personal Data
https://threatpost.com/apple-to-remove-256-ios-apps-using-private-apis-collecting-personal-data/115098/
http://thehackernews.com/2015/10/apple-ios-malware-apps.html
Apple が個人情報にアクセスしていた数百のアプリを App Store から削除
http://jp.techcrunch.com/2015/10/20/20151019hundreds-of-apps-banned-from-app-store-for-accessing-users-personal-information/
・Baidu SDK
Backdoor in Baidu Android SDK Puts 100 Million Devices at Risk
http://thehackernews.com/2015/11/android-malware-backdoor.html
http://blog.trendmicro.com/trendlabs-security-intelligence/setting-the-record-straight-on-moplus-sdk-and-the-wormhole-vulnerability/

■情報漏えいしても、政府機関向けスパイビジネスは健在
・Gamma International 社（FinFisher）
You Only Click Twice: FinFisher's Global Proliferation
https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/
Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation
https://citizenlab.org/2015/10/mapping-finfishers-continuing-proliferation/
・Hacking Team 社
Hacking Team Offering Encryption Cracking Tools to Law Enforcement Agencies
http://thehackernews.com/2015/10/hacking-team-tools.html

http://motherboard.vice.com/en_uk/read/hacking-team-is-back-with-a-bold-pitch-to-police

■その他

US baseball team accused of hacking rival club

http://www.bbc.co.uk/news/world-us-canada-33159086

http://www.nytimes.com/2015/06/17/sports/baseball/st-louis-cardinals-hack-astros-fbi.html

http://www.cnet.com/news/st-louis-cardinals-investigated-by-fbi-for-hacking-houston-astros-report-says/

http://www.cnet.com/news/hackers-in-the-outfield-cardinals-probed-for-allegedly-hacking-astros/

The Trojan Games: Odlanor malware cheats at poker

http://www.welivesecurity.com/2015/09/17/the-trojan-games-odlanor-malware-cheats-at-poker/

U.S. Air Force confirms electromagnetic pulse weapon

http://edition.cnn.com/videos/us/2015/05/25/orig-boeing-electromagnetic-pulse-weapon.cnn

以上