[CB19] Cyber Threat Landscape in Japan – Revealing Threat in the Shad…

slideshare.net/codeblue_jp/cb19-cyber-threat-landscape-in-japan-revealing-threat-in-the-shadow-by-chi-en-shen-ashley-oleg-bondarenko

CODE BLUE

FIREEYE™

Cyber Threat Landscape in Japan

Revealing Threats in the Shadow

Oleg Bondarenko
Director of Research Team

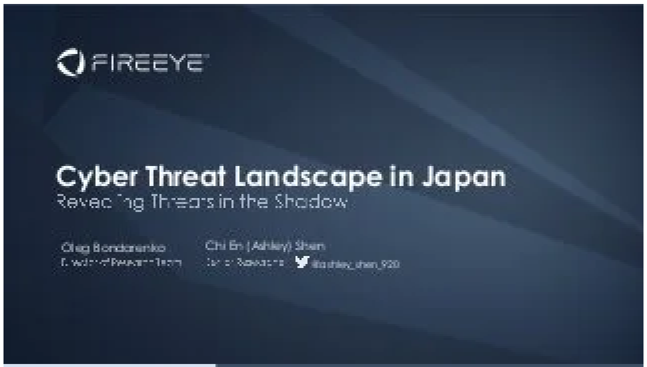
Chi En (Ashley) Shen
Senior Researcher @ashley_shen_920

Successfully reported this slideshow.

[CB19] Cyber Threat Landscape in Japan – Revealing Threat in the Shadow by Chi En Shen (Ashley) Oleg Bondarenko

8

Share

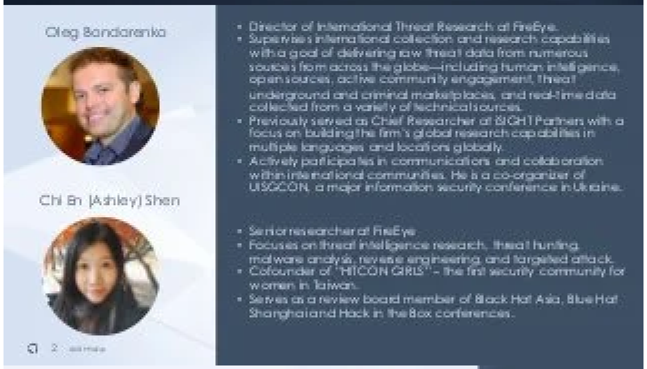


Cyber Threat Landscape in Japan

Revealing Threats in the Shadow

Oleg Bondarenko
Director of Research Team

Chi En (Ashley) Shen
Senior Researcher @ashley_shen_920

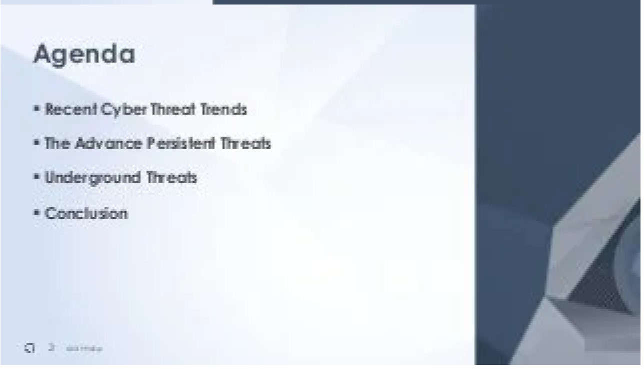


Oleg Bondarenko

- Director of International Threat Research at FireEye.
- Supervises international collection and research capabilities with a goal of delivering raw threat data from numerous sources from across the globe—including human intelligence, open sources, active community engagement, threat underground and criminal marketplaces, and real-time data collected from a variety of technical sources.
- Previously served as Chief Researcher at iSIGHT Partners with a focus on building the firm's global research capabilities in multiple languages and locations globally.
- Actively participates in communications and collaboration within international communities. He is a co-organizer of UISGCON, a major information security conference in Ukraine.

Chi En (Ashley) Shen

- Senior researcher at FireEye
- Focuses on threat intelligence research, threat hunting, malware analysis, reverse engineering, and targeted attack.
- Cofounder of "HITCON GIRLS" – the first security community for women in Taiwan.
- Serves as a review board member of Black Hat Asia, Blue Hat Shanghai and Hack in the Box conferences.



Agenda

- Recent Cyber Threat Trends
- The Advance Persistent Threats
- Underground Threats
- Conclusion

[Next SlideShares]

Upcoming SlideShare

Into the Fog –
The Return
of ICEFOG APT

[“Into the Fog The Return of ICEFOG APT” - Chi en (Ashley) Shen]

Loading in …3

×

1 of 72

1 of 72

[CB19] Cyber Threat Landscape in Japan – Revealing Threat in the Shadow by Chi En Shen (Ashley) Oleg Bondarenko

8

Share

Presentations & Public Speaking

For the past few years, Asia Pacific and Japan have continued to be a regular target of cyber threat actors. From 2018 to 2019, we have observed several threats targeting Japan involving cyber espionage and underground activities. Some of the adversaries and campaigns are revealed in OSINT, however, some are still lurking in shadow.

In this talk, we will reveal the TTP's (tactics, techniques and procedures) of espionage threat actors interested in Japanese electronics, chemical and 5G equipment manufacturing companies. One campaign leverages a malware attributed to APT41, a prolific Chinese cyber threat group that carries out state-sponsored espionage activity in parallel with financially motivated operations. Beside the Chinese actors, we have also observed a group which historically focused on the EMEA region shift to showing interest in Japan. In addition, we will also disclose details of underground activity involving a target in the Japanese financial industry.

CODE BLUE

Follow

For the past few years, Asia Pacific and Japan have continued to be a regular target of cyber threat actors. From 2018 to 2019, we have observed several threats targeting Japan involving cyber espionage and underground activities. Some of the adversaries and campaigns are revealed in OSINT, however, some are still lurking in shadow.

In this talk, we will reveal the TTP's (tactics, techniques and procedures) of espionage threat actors interested in Japanese electronics, chemical and 5G equipment manufacturing companies. One campaign leverages a malware attributed to APT41, a prolific Chinese cyber threat group that carries out state-sponsored espionage activity in parallel with financially motivated operations. Beside the Chinese actors, we have also observed a group which historically focused on the EMEA region shift to showing interest in Japan. In addition, we will also disclose details of underground activity involving a target in the Japanese financial industry.

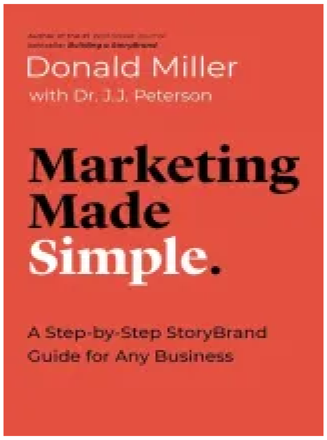
Presentations & Public Speaking

More Related Content

Related Books

Free with a 14 day trial from Scribd

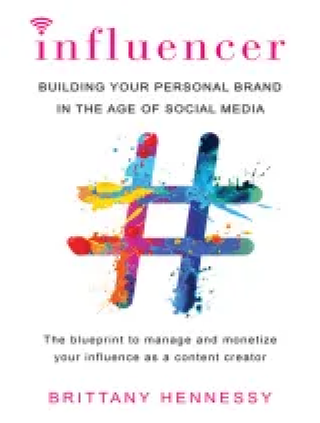
See all



Marketing Made Simple: A Step-by-Step StoryBrand Guide for Any Business Donald Miller

(5/5)

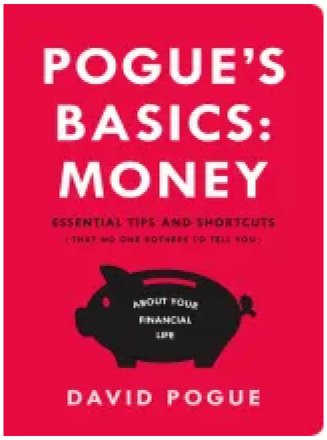
Free


influencer
BUILDING YOUR PERSONAL BRAND IN THE AGE OF SOCIAL MEDIA
The blueprint to manage and monetize your influence as a content creator
BRITTANY HENNESSY

Influencer: Building Your Personal Brand in the Age of Social Media Brittany Hennessy

(3.5/5)

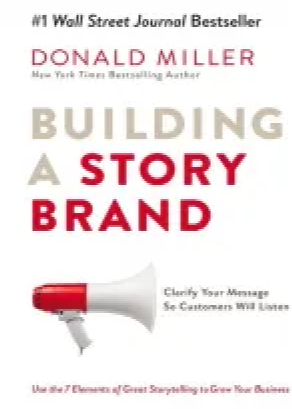
Free


POGUE'S BASICS: MONEY
ESSENTIAL TIPS AND SHORTCUTS
(THAT NO ONE BOTHERS TO TELL YOU)
ABOUT YOUR FINANCIAL LIFE
DAVID POGUE

Pogue's Basics: Money: Essential Tips and Shortcuts (That No One Bothers to Tell You) About Beating the System David Pogue

(4/5)

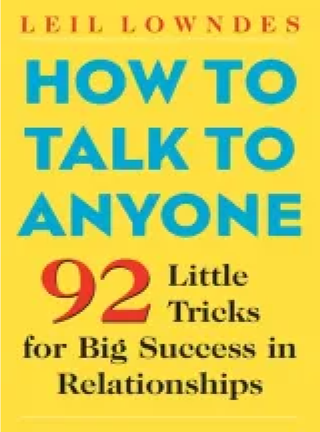
Free


#1 Wall Street Journal Bestseller
DONALD MILLER
New York Times Bestselling Author
BUILDING A STORY BRAND
Clarify Your Message So Customers Will Listen
Use the 7 Elements of Great Storytelling to Grow Your Business

Building a StoryBrand: Clarify Your Message So Customers Will Listen Donald Miller

(4.5/5)

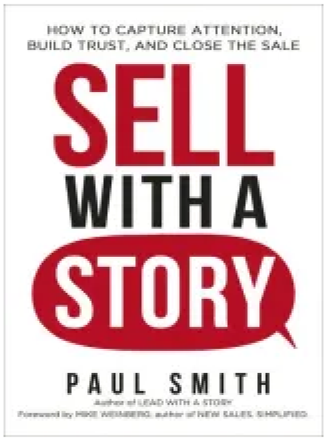
Free



How to Talk to Anyone: 92 Little Tricks for Big Success in Relationships Leil Lowndes

(4/5)

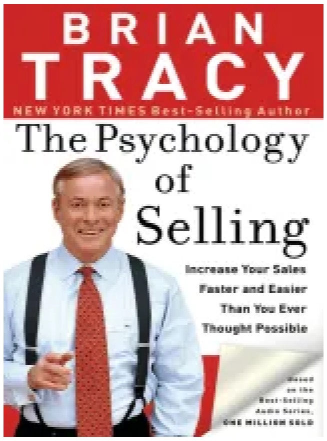
Free


HOW TO CAPTURE ATTENTION, BUILD TRUST, AND CLOSE THE SALE
SELL
WITH A
STORY
PAUL SMITH
Author of LEAD WITH A STORY
Foreword by MIKE WEINBERG, author of NEW SALES. SIMPLIFIED.

Sell with a Story: How to Capture Attention, Build Trust, and Close the Sale Paul Smith

(1/5)

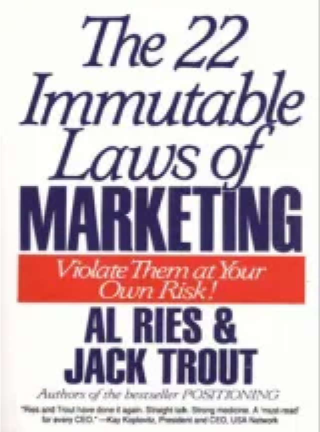
Free


BRIAN
TRACY
NEW YORK TIMES Best-Selling Author
The Psychology of Selling
Increase Your Sales Faster and Easier Than You Ever Thought Possible
Based on the Best-Selling Audio Series, ONE MILLION SOLD

The Psychology of Selling: Increase Your Sales Faster and Easier Than You Ever Thought Possible Brian Tracy

(4.5/5)

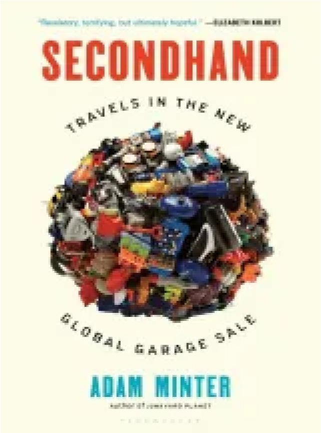
Free


The 22 Immutable Laws of MARKETING
Violate Them at Your Own Risk!
AL RIES &
JACK TROUT
Authors of the bestseller POSITIONING

The 22 Immutable Laws of Marketing: Exposed and Explained by the World's Two Al Ries

(4.5/5)

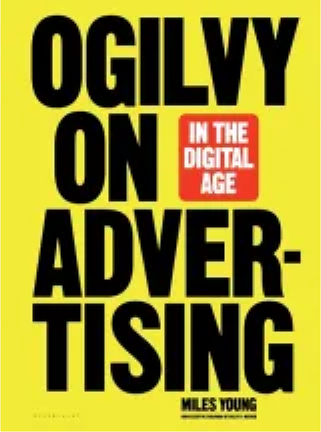
Free



Secondhand: Travels in the New Global Garage Sale Adam Minter

(4/5)

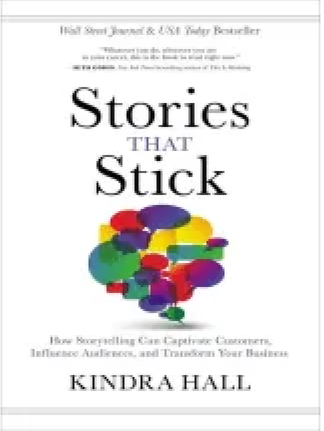
Free



Ogilvy on Advertising in the Digital Age Miles Young

(5/5)

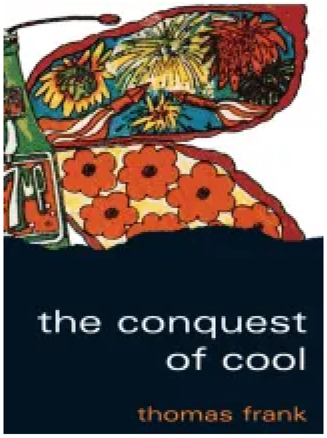
Free


Wall Street Journal & USA Today Bestseller
Stories
THAT
Stick
How Storytelling Can Captivate Customers,
Influence Audiences, and Transform Your Business
KINDRA HALL

Stories That Stick: How Storytelling Can Captivate Customers, Influence Audiences, and Transform Your Business Kindra Hall

(5/5)

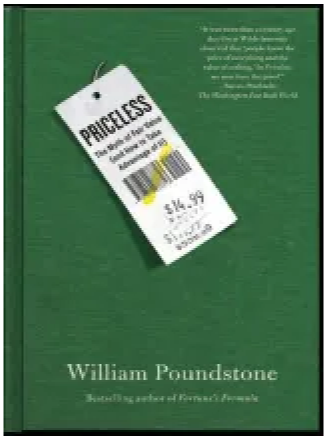
Free



The Conquest of Cool: Business Culture, Counterculture, and the Rise of Hip Consumerism Thomas Frank

(4.5/5)

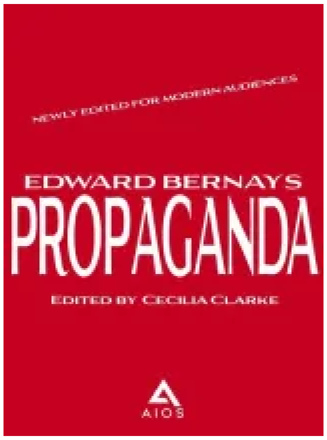
Free



Priceless: The Myth of Fair Value (and How to Take Advantage of It) William Poundstone

(4.5/5)

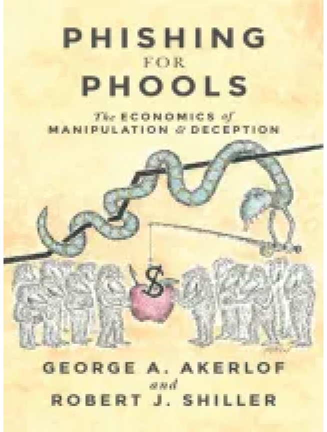
Free



Propaganda Edward Bernays

(5/5)

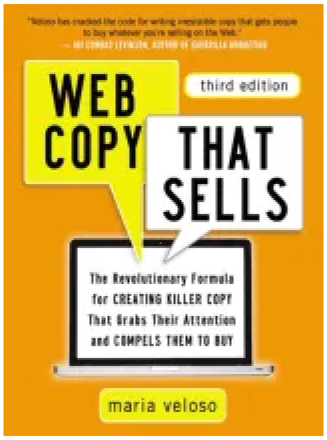
Free



Phishing for Phools: The Economics of Manipulation and Deception George A. Akerlof

(3.5/5)

Free



Web Copy That Sells: The Revolutionary Formula for Creating Killer Copy That Grabs Their Attention and Compels Them to Buy Maria Veloso

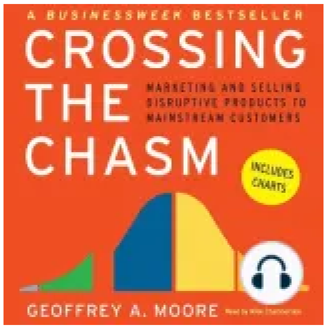
(5/5)

Free

Related Audiobooks

Free with a 14 day trial from Scribd

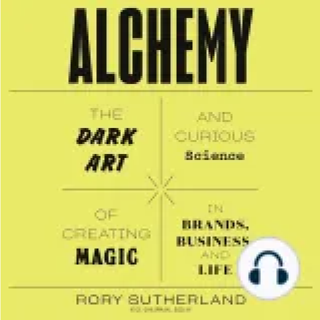
See all



Crossing the Chasm: Marketing and Selling Technology Projects to Mainstream Customers Geoffrey A. Moore

(4.5/5)

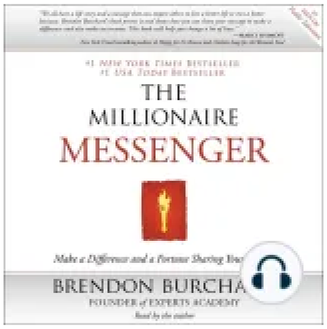
Free



Alchemy: The Dark Art and Curious Science of Creating Magic in Brands, Business, and Life Findaway

(4.5/5)

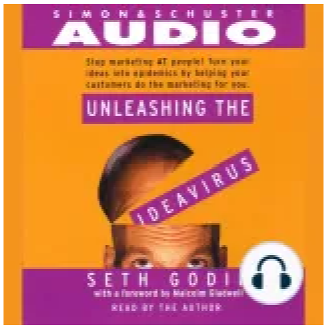
Free



The Millionaire Messenger: Make a Difference and a Fortune Sharing Your Advice Findaway

(4.5/5)

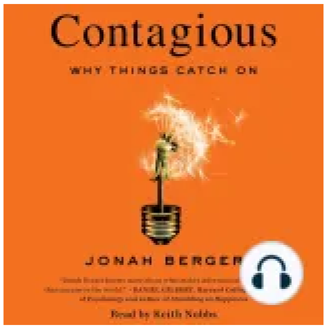
Free



Unleashing the Idea Virus Seth Godin

(4.5/5)

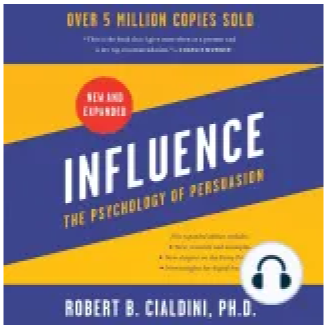
Free



Contagious: Why Things Catch On Jonah Berger

(4.5/5)

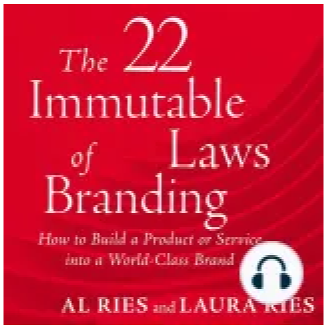
Free



Influence, New and Expanded: The Psychology of Persuasion Robert B. Cialdini

(4.5/5)

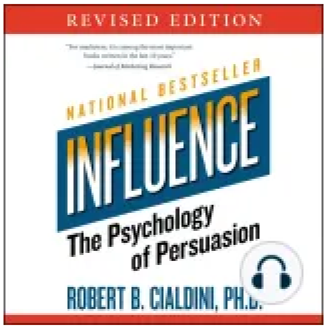
Free



22 Immutable Laws of Branding Findaway

(4.5/5)

Free



REVISED EDITION

NATIONAL BESTSELLER

INFLUENCE

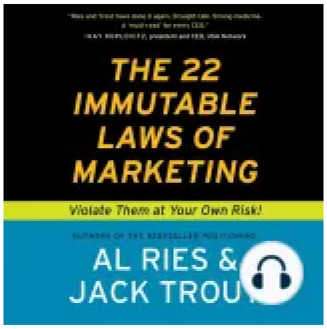
The Psychology of Persuasion

ROBERT B. CIALDINI, PH.D.

Influence: The Psychology of Persuasion Robert B. Cialdini, PhD

(4.5/5)

Free



THE 22 IMMUTABLE LAWS OF MARKETING

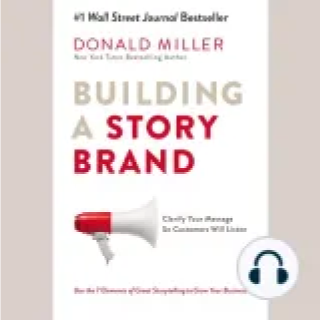
Violate Them at Your Own Risk!

AL RIES & JACK TROU

The 22 Immutable Laws of Marketing Findaway

(4.5/5)

Free



#1 Wall Street Journal Bestseller

DONALD MILLER

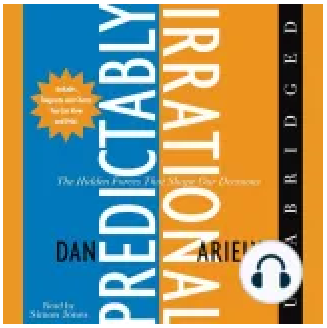
BUILDING A STORY BRAND

Clarify Your Message So Customers Will Listen

Building a StoryBrand: Clarify Your Message So Customers Will Listen Donald Miller

(5/5)

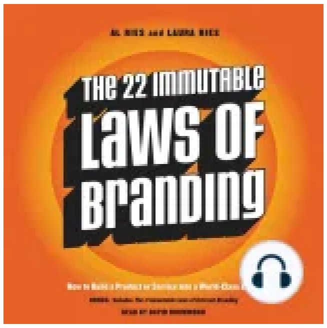
Free



Predictably Irrational: The Hidden Forces That Shape Our Decisions Edgar Allan Poe

(4.5/5)

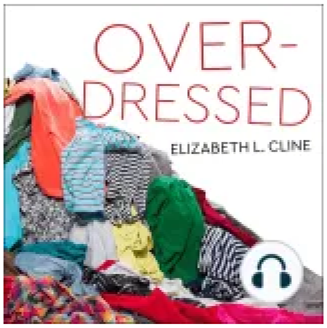
Free



The 22 Immutable Laws of Branding Al Ries

(4/5)

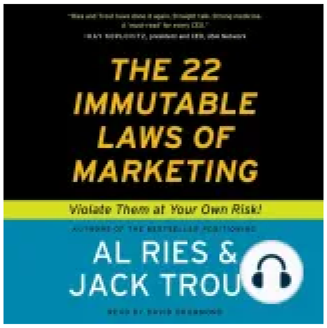
Free



Overdressed: The Shockingly High Cost of Cheap Fashion Elizabeth L. Cline

(4.5/5)

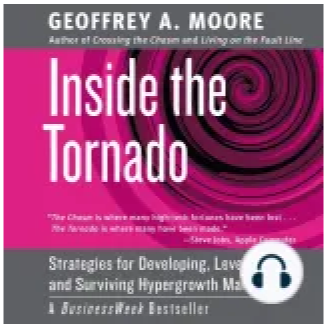
Free



The 22 Immutable Laws of Marketing Al Ries

(4.5/5)

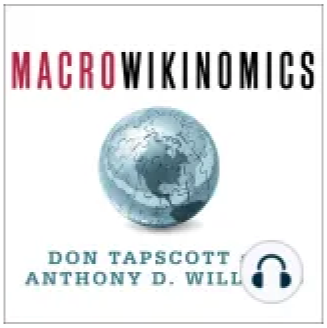
Free


GEOFFREY A. MOORE
Inside the Tornado
Strategies for Developing, Leve
and Surviving Hypergrowth Ma
A BusinessWeek Bestseller

Inside the Tornado Geoffrey A. Moore

(4/5)

Free



Macrowikinomics: Rebooting Business and the World Don Tapscott

(4/5)

Free

[CB19] Cyber Threat Landscape in Japan – Revealing Threat in the Shadow by Chi En Shen (Ashley) Oleg Bondarenko

1. 1. Oleg Bondarenko Cyber Threat Landscape in Japan Chi En (Ashley) Shen @ashley_shen_920

2. 2. ©2019 FireEye©2019 FireEye Oleg Bondarenko • Director of International Threat Research at FireEye. • Supervises international collection and research capabilities with a goal of delivering raw threat data from numerous sources from across the globe —including human intelligence, open sources, active community engagement, threat underground and criminal marketplaces, and real-time data collected from a variety of technical sources. • Previously served as Chief Researcher at iSIGHT Partners with a focus on building the firm's global research capabilities in multiple languages and locations globally. • Actively participates in communications and collaboration within international communities. He is a co-organizer of UISGCON, a major information security conference in Ukraine. 2 Chi En (Ashley) Shen • Senior researcher at FireEye • Focuses on threat intelligence research, threat hunting, malware analysis, reverse engineering, and targeted attack. • Cofounder of "HITCON GIRLS" – the first security community for women in Taiwan. • Serves as a review board member of Black Hat Asia, Blue Hat Shanghai and Hack in the Box conferences.
3. 3. ©2019 FireEye©2019 FireEye § Recent Cyber Threat Trends § The Advance Persistent Threats § Underground Threats § Conclusion Agenda 3
4. 4. ©2019 FireEye©2019 FireEye § Recent Cyber Threat Trends § The Advance Persistent Threats § Underground Threats § Conclusion Agenda 4
5. 5. ©2019 FireEye | Private & Confidential Top 10 Malware Families Affecting National Governments (Q3 2019) 5
6. 6. ©2019 FireEye | Private & Confidential Top 10 Malware Families. 2018-2019 Comparison. 6 Europe 2018 World 2018 World 2019 1 Pony Lokibot Emotet Emotet is modular credential theft Trojan 2 Emotet Emotet Lokibot Lokibot is a credential stealer 3 Lokibot Pony Nanocore NanoCore is a publicly available RAT available for purchase 4 Formbook Chanitor Formbook FormBook is a data stealer/form grabber - keylogger 5 Chanitor Formbook Pony Pony is a credential stealer. Chanitor is a downloader malware that has been observed loading Pony, Send-Safe spambot, Vawtrak, or Nymaim malware 6 NanoCore Ursnif Remcos Remcos is a configurable RAT program written in the C++ language that has a large number of implemented features, including: file management, screen capture, access to clipboard data, command shell, arbitrary file access, mouse control, and more 7 Zeus Nanocore Azorult AZORULT is a credential stealer. 8 Adwind Remcos Netwire NetWire is a RAT capable of stealing a large number of account details, keylogged data, system information, screen captures, remote shell, downloads, reverse proxy and more 9 Ursnif Zeus Ursnif Ursnif (aka Gozi and, now, Gozi-ISFB) is a modified modular banking malware with backdoor capabilities 10 Remcos Hawkeye Adwind Adwind is a Java-based, cross-platform RAT

7. 7. ©2019 FireEye | Private & Confidential 7 Top 10 Malware Families. Emotet. ▶ Emotet is a modular credential theft Trojan that primarily collects usernames and passwords for accounts at financial institutions. The malware downloads and executes various modules from hard-coded C&C servers. The modules are not written to disk but loaded directly from memory and include web browser and email client credential harvesters, an email scraper for Microsoft Outlook, and a spam engine. FireEye iSIGHT Intelligence researchers have recently identified newer variants of the Emotet malware that contain a self-propagation module and other notable host- and network-based indicator changes.
8. 8. ©2019 FireEye | Private & Confidential 8 Top 10 Malware Families. Emotet. ▶ collects usernames and passwords for accounts at financial institutions; ▶ downloads and executes various modules from hard-coded C2s; ▶ loaded directly from memory; ▶ include Web browser and email client credential harvesters, an email scraper for Microsoft Outlook, and a spam engine; ▶ Secondary Payloads in 2018 - Trickbot, IcedID, and ZeusPanda;
9. 9. ©2019 FireEye | Private & Confidential 9 Top 10 Malware Families. Emotet.
10. 10. ©2019 FireEye | Private & Confidential 10 Top 10 Malware Families. Lokibot. ▶ LokiBot is a .NET launcher that executes an embedded credential stealer. It can download and then drop, load, or execute other binaries to the system. It is also designed to steal private data from infected machines, and then submit that information to a C&C host via HTTP POST. The compromised data includes stored passwords, login credential information from web browsers, FTP/SSH, email, poker clients, and a variety of cryptocurrency wallets. It is designed to work on Windows XP, Vista, 7, 8, and has a Linux option.
11. 11. ©2019 FireEye | Private & Confidential 11 Top 10 Malware Families. LokiBot.
12. 12. ©2019 FireEye | Private & Confidential 12 Top 10 Malware Families. LokiBot.
13. 13. ©2019 FireEye | Private & Confidential 13 Top 10 Malware Families. FormBook. ▶ FormBook is a data stealer/form grabber that has been advertised on HackForums by its developer "Ng. Coder" since early 2016. The malware injects itself into various processes and installs function hooks to log keystrokes, steal clipboard contents, and extract data from HTTP sessions. The malware can also execute commands from a C&C server. The commands include instructing the malware to download and execute files, start processes, shut down and reboot the system, and steal cookies and local passwords. It also features a persistence method that randomly changes the path, filename, file extension, and the registry key used for persistence.
14. 14. ©2019 FireEye | Private & Confidential 14 Top 10 Malware Families. FormBook. ▶ Coded in C and Assembly; ▶ Lagos Island method; ▶ Persistence; ▶ Exe as a service; ▶ Ng.Coder
15. 15. ©2019 FireEye | Private & Confidential 15 Top 10 Malware Families. FormBook.
16. 16. ©2019 FireEye | Private & Confidential 16 Top 10 Malware Families. FormBook.
17. 17. ©2019 FireEye | Private & Confidential Better Detection, More Evasion 17

18. 18. ©2019 FireEye | Private & Confidential Multi-stage Sample Delivery & Hit and Run 18 § Increasing number of multi-stage delivery. – Payload removed after compromised (sometimes in 2 days) – Increase the difficulty to do attribution. – Increase the difficulty to track. – Increase the difficulty of detection on the final payload. PayloadExploit DocumentsSpear-phishing Emails Script Downloader PE Downloader
19. 19. ©2019 FireEye | Private & Confidential Old is the New Fashion – Macro +Script 19 Exploit Count Macro / Macro + Script 43 CVE 2017-11882 27 Fake document EXE 21 CVE 2018-20250 4 CVE 2015-2545 3 HWP exploit 3 CVE-2017-8291 2 LNK 2 CVE 2017-0199 1 CVE 2017-0261 1 CVE-2017-12824 1 CVE-2017-15399 1 Exploit Count Macro / Macro + Script 50 CVE 2017-11882 44 Fake document EXE 19 CVE 2017-0199 9 HWP exploit 8 LNK + Script 5 CVE 2017-8570 5 CVE 2017-8291 4 Powershell 3 CVE 2012-0158 2 CVE 2015-1641 2 CVE 2018-0802 2 2018 Jan – Oct (10 months) 2018 Nov – 2019 May ◆More MACRO documents than exploit ▶ Needless to embed the payload into document. (avoid detection) ▶ Encryption bypass static detection. ▶ Low sophisticated but still effective. ◆Frequently employ with Powershell script ▶ Because it is "POWER" shell ▶ Execute directly in memory, leaving fewer trace for analysis (most org don't enable logging) ▶ Mainly as downloader to download 2nd stage payload
20. 20. ©2019 FireEye | Private & Confidential Automobile 1% Cryptocurrency 6% Defense 3% Dissident/defect or 2% Education 3% Energy 9% Finance 6% Gov 50% Healthcare 1% Media 1%NGO 1% Professional Service 1% Research Institute 2% Telecommunicati on 3% Information Technology 10% TOTAL Increasing Targeted Attack on IT, Cryptocurrency and Energy 20 Aerospace 1% Crytocurrency 1% Defense 1% Dissidents 1% Education 4% Energy 2% Financial 8% Gov 60% Healthcare 1% Human Right 1% Media 3% NGO 1% Professional Service 1% Social Enterprise 1% Technology 6% Telecom 6% Think Tank 2% Automobile 1% 2018 Jan – 2018 Oct 2018 Nov – 2019 May
21. 21. ©2019 FireEye©2019 FireEye § Recent Cyber Threat Trends § The Advance Persistent Threats § Underground Threats § Conclusion / Takeaway Agenda 21
22. 22. Temp.Overboard's Campaign Target Japan, Taiwan and South Korea
23. 23. ©2019 FireEye | Private & Confidential Temp.Overboard (aka BlackTech) Group 23 ◆ Temp.Overboard's target active since at least 2016, main focus was Taiwan and Hong Kong before 2017. ◆ Starting from 2017 the group was observed expanding target scale to include Japan and Europe. ◆ We also observed samples suspected target Chinese financial institute. ◆ Targeted industry: ▶ Education/Academia/Research Institutions ▶ Media/Entertainment/Publishing ▶ Aerospace & Defense ▶ Governments ▶ Media ▶ Think tank ▶ Government ▶ Telecommunication ▶ Conglomerate (Transportation)

24. 24. ©2019 FireEye | Private & Confidential Malware Observed in Temp.Overboard’s Recent Campaigns 24 FIREEYE Naming JPCERT Naming Malware Type Description FRONTSHELL TSCOOKIE loader Launcher FRONTSHELL is a loader decrypts and loads the payload and inject into memory. TSCOOKIE TSCOOKIE Downloader TSCOOKIE is an MFC-based downloader with persistence capability. WORKMATE TSCOOKIERAT (overlap code) Backdoor WORKMATE is a backdoor which provides many commands including remote shell, command execution, file transfer, file searching, process enumeration and termination, window enumeration and closing, screen capture, and time stamp manipulation DRAWDOWN PLEAD (downloader) Downloader DRAWDOWN is a downloader that makes an HTTP request and decrypts and decompresses the response. The results is expected to be a PE file that is manually loaded and executed. GOODTIMES PLEAD module Backdoor GOODTIMES will attempt to send a variety of information about the infected host back to the C&C . It has the ability to upload, download, execute and delete files, execute commands, and gather system information CAVEMAN N/A Downloader CAVEMAN is a downloader that has the ability to download and execute malware from a hardcoded C&C server. TINYSHELL (public) Backdoor TINYSHELL is an open source unix backdoor. we observed a Tinyshell linux sample activity connecting to TEMP.Overboard infrastructure. ◆ Temp.Overboard’s most frequently used backdoor and downloader tools in recent years.
25. 25. ©2019 FireEye | Private & Confidential FRONTSHELL v.s. TSCOOKIE ? 25 Launcher Payload Injector FRONTSHELL. standalone Downloader Backdoor FRONTSHELL.fused Shellcode + DLL RC4 Encrypted File Loads FRONTSHELL. Injector (MyNewInjector_Atla ntis_[Mark].dll) TSCOOKIE (FrontShell_[Mark].dl l) (FrontShell_Avria.dll) WORKMATE Loads Downloads DLL DLLShellcode +
26. 26. ©2019 FireEye | Private & Confidential Case:1 26 ◆REDACTED
27. 27. ©2019 FireEye | Private & Confidential 27 ◆REDACTED Case:1
28. 28. ©2019 FireEye | Private & Confidential Case 2: Thread Hijacking Email Target Japanese Conglomerate (April 2019) 28 Targeted Company A Affiliate Company B ◆In April 2019, FireEye detected a spear-phishing email sent to Japanese conglomerate oversea office. ◆Based on the email content and targeted department, the actor is potentially interested in railway system. Actor XLSM Malicious macro encrypted with default password “VelvetSweatshop” TSCOOKIE
29. 29. ©2019 FireEye | Private & Confidential 29 Embedded PE Extracted as OneDrive.exe Stolen certificate ◆Binary signed with stolen certificate. (previous stolen certificate used by this group included D-link and Changin) ◆C&C: ▶ http://185.227.153.186/t3445851474.aspx ▶ http://www.microsoftonline.com.organiccrap.com/t167918 7984.aspx

30. 30. ©2019 FireEye | Private & Confidential Case 3: Sample Compiled in March 2019 linked to Old Campaign (2017) 30 FRONTSHELL asiainfo.hpcloudnews.com 122.115.49.247 c2452dea557e3d6fc8ac61b8126f8ea2 ntt.capital-db.com acer.microsoftmse.com adc.microsoftmse.com chtd.microsoftmse.com dlink.microsoftmse.com htctrans.microsoftmse.com hk.microsoftmse.com kr.microsoftmse.com sonet.microsoftmse.com Potential Target Country NTT Japan Acer Taiwan Acer eDC Taiwan Chunghwa Telecom Co Taiwan D-link Taiwan HTC Taiwan Hong Kong South Korea Sony Network Communications Inc. Japan, Taiwan
31. 31. SWEETCANDLE Campaign From Chinese Actor Targets Japan
32. 32. ©2019 FireEye | Private & Confidential SWEETCANDLE Downloader 32 ◆Also called ABK downloader because of the pdb string. ◆The downloader search for Trend Micro AV (PccNT.exe) and terminate it before running. ◆The downloader sends beacons includes CPU model information to C&C server. ▶ Examples: – http://<server>//shop//img//marks_escrow//index.php?uid=<DWORD_1 (ascii hex)> <DWORD_2 (ascii hex)> ◆If receive an ascii “y” from C&C, it download a file (usually a fake picture) from C&C to %TEMP% folder. ◆Files observed downloaded by SWEETCANDLE downloader: ▶ Reconnaissance tool ▶ Benign Notepad.exe with language zh-cn ▶ POISONPLUG
33. 33. ©2019 FireEye | Private & Confidential Case1: Spear-phishing Email targeted Manufacturing and Financial Industries in JP 33 Spear-phishing email Attachment 中国_投資概況.zip Password protected archive Contains PPSX 中国投資概況.ppsx CVE 2017-8759 Compromised C&C Connects Download Malicious script forged as PNG Drops SWEETCANDLE Downloader Compromised C&C Connect Download Reconnaissance Tool
34. 34. ©2019 FireEye | Private & Confidential Reconnaissance Tool Downloaded by SWEETCANDLE 34 Also checks for the Trend Micro OfficeScan antivirus process “PCCNTMon.exe” and terminates “PccNT.exe”. Using dir commands to collect directory information Send result.txt to C&C with HTTP Compromised server MD5:680f481a477a709b2ef4ddf66c25cdc0 PDB: c:usersxfdocumentsvisual studio 2010Projects123Release123.pdb
35. 35. ©2019 FireEye | Private & Confidential 35 PPSX 中国投資概況.ppsx CVE 2017-8759 Compromised C&C Connects Download Malicious script forged as PNG Drops IRONHALO Downloader Variant Another Sample Download a New Variant of IRONHALO Downloader Sample using same exploit, sharing same decoy File and file name with SWEETCANDLE sample 0987a57e2da9294d7bb9bd798999efd2 www.114pr.co.kr

36. 36. ©2019 FireEye | Private & Confidential 36 IRONHALO Downloader Variant IRONHALO in 2018: a8ccb2fc5fec1b89f778d93096f8dd65 IRONHALO Variant: 0987a57e2da9294d7bb9bd798999efd2 Sample string copy routine for different EXE file name IRONHALO Variant IRONHALO 2018 IRONHALO VariantIRONHALO 2018 Sample constant value for the size to read from C&C Same decode routine, different B64 table IRONHALO Variant IRONHALO 2018 Both check MZ header before run Different User Agent IRONHALO 2018 IRONHALO Variant
37. 37. ©2019 FireEye | Private & Confidential TTP Similar with TEMP.TICK Group 37 ◆Use compromised server as 1st stage C&C. ◆Enlarge malware binary to bypass detection. ◆Same targeted region (Japan). ◆Similar interests in economic, banks, manufacturing, foreign affairs specially between US and China. ▶ Example lure theme: – 中国投資概況 – 2019年昇給率参考資料 ◆Embedded 2nd stage malware in image files (JPG, IMG, PNG). ◆SWEETCANDLE potentially downloaded SPACEPANTS (aka Dapter)
38. 38. ©2019 FireEye | Private & Confidential Case 2: Spear-phishing Email Targets Japanese Conglomerate 38 ◆In February 2019, FireEye devices detected and blocked a malicious archive file sent via spear-phishing email to a Japanese conglomerate. ◆Sample leverage US-China Trade Friction-themed lure. ◆The SWEETCANDLE downloader was observed to download and execute a POISONPLUG variant SWEETCANDLE Downloader Spear-phishing email Fake document EXE Sender Email: shao.**@**-inc.co.jp POISONPLUG backdoor 114.118.21.146 Attacker's C&C Attachment Contain Drops Connects Compromised C&C Download www.86coding.com (compromised server)%TEMP%taskmor.exe %APPDATA%MicrosoftInternet ExplorerUserDatamscoree.dll
39. 39. ©2019 FireEye | Private & Confidential Decoy dropped by fake PDF 39
40. 40. ©2019 FireEye | Private & Confidential POISONPLUG Backdoor Variant 40 ◆POISONPLUG is a highly obfuscated modular backdoor with plug- in capabilities. The backdoor has been observed leveraged in APT41's campaign. ◆This variant of POISONPLUG has been recharacterized and many of the internal details have changed, likely rendering existing signatures ineffective. Suspected attribution: China Overview: APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control. ID Name Role 100 Root Loads / initializes plugins, executes Install plugin 101 Plugins Handles creation, removal, updating, and removal of plugins 102 Config Capable of reading, updating, and deleting config 103 Install Handles installation and removal of malware 104 Online Creates a C&C thread capable of sending a host survey and random number between 0 and 31 201 HTTP Performs C&C communication

41. 41. ©2019 FireEye | Private & Confidential C&C Server Certificate Linked to Potentially APT41 41 ◆114.118.21.146 used two self-signed SSL certificates serials. ◆The two SSL certificates combined were associated to 4 servers attributed to APT41, connected by malware POISONPLUG. ◆1 was reported by Avast as being related to SHADOWPAD. 146.118.21.146 MyServer MyCA 117.16.142.35 POISONPLUG Backdoor attributed to APT41 85.204.74.94 85.204.74.108 89.32.40.199
42. 42. ©2019 FireEye | Private & Confidential PDB Found in This Case 42 Fake PDF Dropper C:UsersFrankDesktopABKReleasePretender.pdb SWEETCANDLE Downloader C:UsersFrankDesktopABK-oldReleaseABK.pdb POISONPLUG Dropper C:UsersFrankDocumentsVisual Studio 2010ProjectsRunCasperReleaseRunCasper.pdb PDB Found in Other SWEETCANDLE Samples Dropper C:UsersFrankDesktopdoc_dllReleaseDocDll.pdb C:UsersFrankDesktopABKReleaseHidder.pdb SWEETCANDLE Downloader C:UsersXFDocumentsVisual Studio 2010ProjectsABKDLLReleaseABKDLL.pdb C:UsersXFDocumentsVisual Studio 2010ProjectsABKReleaseABK.pdb C:UsersFrankDesktopABK-oldReleaseABK.pdb C:UsersFrankDesktopABKReleaseABK.pdb C:UsersFrankDocumentsVisual Studio 2010ProjectsavengerReleaseavenger.pdb Reconnaissance tool download by SWEETCANDLE c:usersxfdocumentsvisual studio 2010Projects123Release123.pdb
43. 43. ©2019 FireEye | Private & Confidential Attribution? 43 ◆Connection to APT41: ▶ Same malware family ▶ Similar delivery method ▶ Overlapping infrastructure ◆Connection to Temp.TICK: ▶ Similar TTP ▶ Similar code ▶ Potential connection with SPACEPANTS (aka Dapter) ◆Theories: A. TEMP.TICK also applied POISONPLUG in their attack B. APT41 conducted all the SWEETCANDLE campaigns with similar TTP with Temp.TICK. C. SWEETCANDLE is a shared tool among Chinese APT group
44. 44. SOURCANDLE Campaign Target Japanese Chemical Industry and Conglomerate
45. 45. ©2019 FireEye | Private & Confidential SOURCANDLE Downloader 45 ◆This sample is is a downloader that executes the decoded payload via a call to CreateProcess(). Also try to terminate Trend Micro Office Scan Client http://<server>/phpcms/modules/block/block_modules.php?UID=<encoded value>&ws=<Base64 value> Hostname + MAC address XOR 0x01, 0x02, 0x03, 0x04, 0x05 Base64 encode Get system OS version Base64 encoded
46. 46. ©2019 FireEye | Private & Confidential SOURCANDLE Campaign Attack Vector 46 SOURCANDLE Downloader Spear-phishing email Attachment Connects Actor’s C&C Exploit CVE 2017-11882 Document Dropper SOURCANDLE Downloader Compromised C&C ConnectsDropDrop RTLO TRICK Binary SOURCANDLE Downloader <File name><202E>xcod.scr Delivery Exploitation Social Engineering
47. 47. ©2019 FireEye | Private & Confidential Leverage Chemical, 5G and Electronic as Lure 47 ◆Lure: ▶ カード管理体制TCL様.doc ▶ 亚洲化学工业现状研究.scr ▶ 各国の化学大手の5G材料分野における構築 ◆Target: ▶ Japanese Chemical company ▶ Japanese Conglomerate

48. 48. ©2019 FireEye | Private & Confidential SOURCANDLE Downloader 48 Block.css %TEMP%/Temp1.dat decode XOR 0x A9 decode %TEMP%/Temp2.dat offset Date type Data 0x00 int name_flag 0x04 int filesize 0x08 wchar[0x8 0] filename 0x88 var len data, PE file expected Temp2.dat data structure The dropped files Value Operation 0x00 Write PE to %TEMP%temp3.dat, and then copied to %TEMP%<attacker filename>. Other Write PE to %TEMP%<attacker filename> • All Dat deleted after file write to the final destination. • File run with CreateProcess()
49. 49. Leverage the Exploit CVE-2017-11882 Document Template Shared among Other Groups Shellcode decode routine Open Document Encoded (0xFC) Dropper (8.t) Drops into %temp% Shellcode decode & execute Malware Can be hunted by the RTF Object Dropper MD5: ac845ad6a5ac75842ead069f5daf29a1 MD5: ed6c250309b7d60d03023ecce69f546a (8.t) C:UsersabcDocumentsVisual Studio 2010Projects0103Release0103.pdb SOURCANDLE MD5: 5d105cd33be63400c9e36a9d74d1c564 Compromised C&C
50. 50. ©2019 FireEye | Private & Confidential The Shared Exploit Builder • Actually, shared among at least 3 different groups. (APT40, Conimes team aka Goblin Panda, ICEFOG Operators) Threat Group Hash Malware Create Date Author Targeted Region APT40 d5a7dd7441dc2b05464a 21dd0c0871ff BEACON 2017-12-07 08:17:00 Windows User USA Temp.CONIMES f223e4175649fa2e34271d b8c968db12 TEMPFUN 2018-01-15 14:47:00 Windows User LAO Temp.CONIMES 07544892999b91ae2c928 0d8ee3c663a TEMPFUN 2018-01-17 09:04:00 Windows User VNM Temp.CONIMES 45a94b3b13101c932a72d 89ff5eb715a TEMPFUN 2018-01-31 11:24:00 Windows User VNM ICEFOG Operator 46d91a91ecdf9c0abc7355 c4e7cf08fc ICEFOG 2018-02-22 20:07:00 T TUR ICEFOG Operator 80883df4e89d5632fa72a 85057773538 ICEFOG 2018-02-22 20:07:00 T KZ, RU SOURCANDLE Operator ac845ad6a5ac75842ead0 69f5daf29a1 SOURCANDL E 2019-01-24 13:24:00 Windows [U [JP
51. 51. APT33’s Phishing Target Conglomerate
52. 52. ©2019 FireEye | Private & Confidential Case: Spear-phishing Campaign Targeted Japanese Conglomerate Involved Energy Sector 52 Data Type Information Campaign timeframe June 2018 - November 2018 Associated Actor APT33 Targeted Sectors Energy Utilities Insurance Manufacturing Higher education Chemical Telecommunication Targeted Country/Region Middle East US Japan South Korea. Delivery Method Spear-phishing + malicious link Malware Discovered METERPRETER, POSHC2, PUPYRAT, PowerShell Empire Suspected attribution: Iran Overview: APT33 has targeted organizations, spanning multiple industries, headquartered in the U.S., Saudi Arabia and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.

53. 53. ©2019 FireEye | Private & Confidential Case: Spear-phishing Campaign Targeted Japanese Conglomerate Involved Energy Sector 53 Spear-phishing email Subject: Job Opening Sender Email: careers@[REDACTED].ga jobs@[REDACTED].ga Malicious link HTA HTA Script http://[REDACTED]..ddns.net:880/SIPCHEMJobOpenning.hta Decoded PowerShell Download POSHC2 PUPYRAT PowerShell Empire Create task to download payloads at different time
54. 54. Other APT Groups
55. 55. ©2019 FireEye | Private & Confidential Other APT Activities 55 Group Recent Activity Timeframe Recent Activity APT28 Nov 2018 – Jan 2019 Leverage TRICKSHOW samples to target suspected Japan Military. FALLOUT (aka Darkhotel) Feb, 2018 Targeted Japanese media industry with SANNY sample APT32 April, 2019 Leverage METALJACK and ASEAN related decoy to target suspected Japan. APT10 N/A Since the indictment, monitoring of numerous attack surfaces, sensitive-source feeds, public repositories, and open-source reporting has not resulted in the detection of new APT10 activity. North Korea nexus July, 2019 Actor leveraged LEADLIFT (aka Dtrack) backdoor targeted Japanese manufacturing company. Unknown July, 2019 Leveraged “北朝鮮非核化の行方と制裁の課題” as lure with ZEROCHECKER downloader to target Japanese research institute.
56. 56. ©2019 FireEye©2019 FireEye § Recent Cyber Threat Trends § The Advance Persistent Threats § Underground Threats § Conclusion Agenda 56
57. 57. Access to Infrastructure/DB for sale
58. 58. ©2019 FireEye©2019 FireEye Threat tracking. Compromised databases. October 2018-March 2019 58 Advertised databases by country Advertised databases by industry
59. 59. ©2019 FireEye©2019 FireEye Threat tracking. Compromised databases. October 2018-March 2019 59 Price and size of databases by industry
60. 60. ©2019 FireEye©2019 FireEye 60 Access to your infrastructure. ▶ Fxmsp ▶ BigPetya ▶ Antony Moricone ▶ ETC.
61. 61. ©2019 FireEye©2019 FireEye 61 Access to your infrastructure. Fxmsp – POS Terminals in Europe, MENA, and South Asia; – Government Establishment in UAE; – UAE-based lighting company; – Access to 3 AV companies; Antony Moricone/BigPetya: – Back after some time; – Access to UAE-based mining company; – Hotel in Philippines; – Aircraft manufacturer;
62. 62. ©2019 FireEye©2019 FireEye Actor Number of Databases Advertised Between Oct. 2018 and March 2019 Forum/Language Reputation Gnosticplayers 37 Dream Market/English New Downloading 18 RAID/English New Lenfoire 14 Dream Market/English Established the.joker 10 Jabber/English "Trusted Seller" NetFlow 6 Exploit.in/Russian Established KelvinSecurity 6 RAID and Facebook/Spanish and English Established DB ads posted by the most prolific actors 62
63. 63. ©2019 FireEye©2019 FireEye 63 Recent addition to “Access for sale” Crew ▶ bc.monster, ▶ B.Wanted, ▶ Aaaakkkka, ▶ SHERIFF

64. 64. ©2019 FireEye©2019 FireEye 64 Access to your infrastructure. PII leak ▶ Japanese PII on Chinese Underground back in 2017-2018; ▶ Extremely low price point - ¥1,000 CNY;
65. 65. Mobile Malware
66. 66. ©2019 FireEye©2019 FireEye 66 Mobile Malware. Cerberus ▶ RAT, Android bot rental service that includes banking Trojan capabilities. ▶ Available for a larger audience since June 2019; ▶ Price: $2000-$12000; ▶ Targets: – jp.coxxxxxk.android.html jp.co.rxxxxx_bank.rxxxxxxbank.html
67. 67. ATM Jackpotting Operations
68. 68. ©2019 FireEye©2019 FireEye 68 ATM Jackpotting Operations ▶ ATM jackpotting kit in August 2019: – Based on Raspberry Pi; – RCE in Diebold Nixdorf ATMs; ▶ Actors are seeking for partnerships; ▶ Original software ATM NCR and Wincor with a wired lifetime key; ▶ Known targeting across India, Taiwan and Japan;
69. 69. ©2019 FireEye©2019 FireEye § Recent Cyber Threat Trends § The Advance Persistent Threats § Cyber Crime and Underground Threats § Conclusion Agenda 69
70. 70. ©2019 FireEye Conclusion 70 § Espionage actors from various countries still having a lot interests in targeting Japan. § With the improving dwell time, actor are devoting extra effort on bypassing detection products. § Organizations should consider thread hijacking as a possible attack vector in their red/blue/purple team scenarios. § We see actor shows increasing interests in chemical, 5G technology, manufacturing and energy sectors. § International events such as the 2019 Rugby World Cup and the 2020 Tokyo Olympics / Paralympics will continue to attract attack groups to Japan. § The threat hunting and monitoring should not overlook the underground forums aspect.
71. 71. Also Credit to our awesome collogues and friends! Thanks for your help Dominik Weber, Marcos Alvares Barbosa Junior, Cian Lynch, Nobuya Chida, Alex C. Lanstein, Jacob Christie Jakub Jozwiak,
72. 72. Oleg Bondarenko ありがとう! Any Questions? Chi En (Ashley) Shen