Inside Cybercrime Groups Harvesting Active Directory for Fun and Prof…

slideshare.net/proidea_conferences/inside-cybercrime-groups-harvesting-active-directory-for-fun-and-profit-vitali-kremez

PROIDEA

CONFIDENCE 2019

Inside Cybercrime Groups Harvesting Active Directory for Fun & Profit

Vitali Kremez

@VK_Intel

Successfully reported this slideshow.

Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez

4

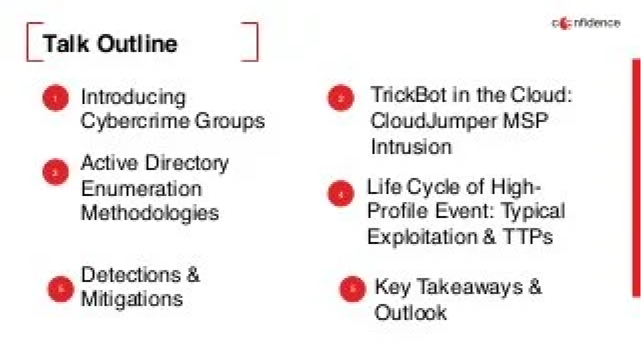
Share

CONFIDENCE 2019

Inside Cybercrime Groups Harvesting Active Directory for Fun & Profit

Vitali Kremez

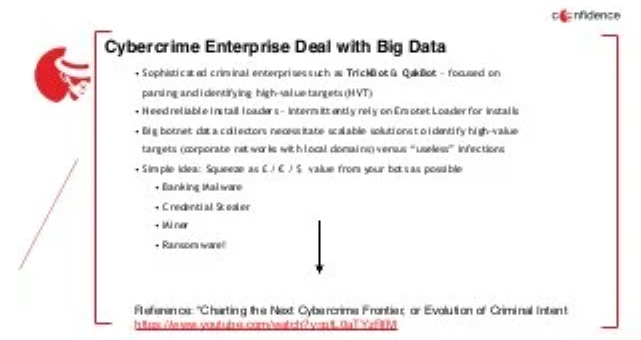
@VK_Intel



confidence

Talk Outline

1. Introducing Cybercrime Groups
2. Active Directory Enumeration Methodologies
3. TrickBot in the Cloud: CloudJumper MSP Intrusion
4. Life Cycle of High-Profile Event: Typical Exploitation & TTPs
5. Detections & Mitigations
6. Key Takeaways & Outlook



confidence

Cybercrime Enterprise Deal with Big Data

- Sophisticated criminal enterprises such as **TrickBot & QakBot** – focused on parsing and identifying high-value targets (HVT)
- Need reliable install loaders – intermittently rely on Emotet Loader for installs
- Big botnet data collectors necessitate scalable solutions to identify high-value targets (corporate networks with local domains) versus "useless" infections
- Simple idea: Squeeze as £ / € / $ value from your bots as possible
  - Banking Malware
  - Credential Stealer
  - Miner
  - Ransomware!

Reference: "Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent
https://www.youtube.com/watch?v=[illegible]

Next SlideShares

Upcoming SlideShare

클라우드 환경에서의 SIEMLESS 통합 보안 서비스, Alert Logic

Openbase

클라우드 환경에서의 SIEMLESS 통합 보안 서비스, Alert Logic - 채현주 보안기술본부장, Openbase :: AWS Sum...

Loading in …3

×

1 of 28

1 of 28

Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez

4

Share

Download to read offline

Technology

Vitali presents malware techniques and tricks on how to reverse engineer and analyze malware families exploiting active directory. The talk dives deeper into pseudo-source code level analysis and malware developer implementation of Lightweight Directory Access Protocol (LDAP) harvesting techniques for lateral movement and persistence across corporate environment. The talks explores three prolific malware families such as TrickBot, QakBot, and IcedID (BokBot) and their coding routine and patterns that are focused on collecting LDAP. For example, TrickBot specifically grabs credential and group policy information stored in “SYSVOL” das well as searching for corporate machines for possible sensitive machines associated with possible point-of-sale terminals on domain controller. Vitali also presents detection and mitigation methods on how to detect active directory exploitation and discusses defense mechanisms surrounding most popular active methods used in the wild by the sophisticated groups.

PROIDEA
Follow

Vitali presents malware techniques and tricks on how to reverse engineer and analyze malware families exploiting active directory. The talk dives deeper into pseudo-source code level analysis and malware developer implementation of Lightweight Directory Access Protocol (LDAP) harvesting techniques for lateral movement and persistence across corporate environment. The talks explores three prolific malware families such as TrickBot, QakBot, and IcedID (BokBot) and their coding routine and patterns that are focused on collecting LDAP. For example, TrickBot specifically grabs credential and group policy information stored in “SYSVOL” das well as searching for corporate machines for possible sensitive machines associated with possible point-of-sale terminals on domain controller. Vitali also presents detection and mitigation methods on how to detect active directory exploitation and discusses defense mechanisms surrounding most popular active methods used in the wild by the sophisticated groups.

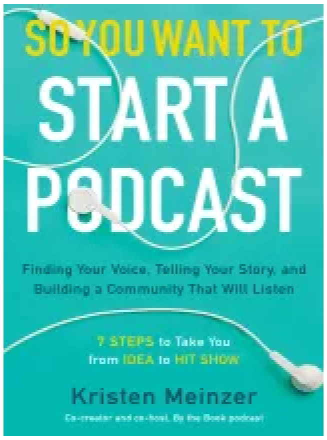
Technology

More Related Content

Related Books

Free with a 14 day trial from Scribd

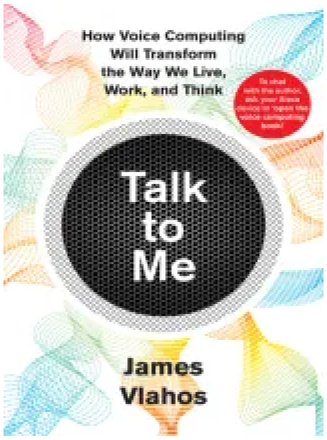
See all


SO YOU WANT TO
START A PODCAST
Finding Your Voice, Telling Your Story, and Building a Community That Will Listen
7 STEPS to Take You from IDEA to HIT SHOW
Kristen Meinzer
Co-creator and co-host, By the Book podcast

So You Want to Start a Podcast: Finding Your Voice, Telling Your Story, and Building a Community That Will Listen Kristen Meinzer

(3.5/5)

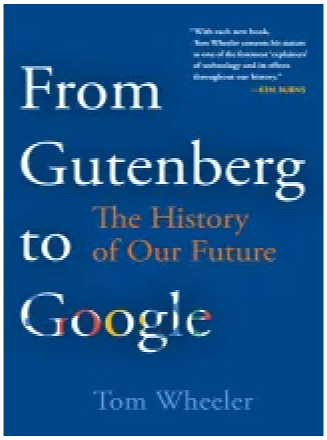
Free


How Voice Computing Will Transform the Way We Live, Work, and Think
Talk to Me
James Vlahos

Talk to Me: How Voice Computing Will Transform the Way We Live, Work, and Think James Vlahos

(4/5)

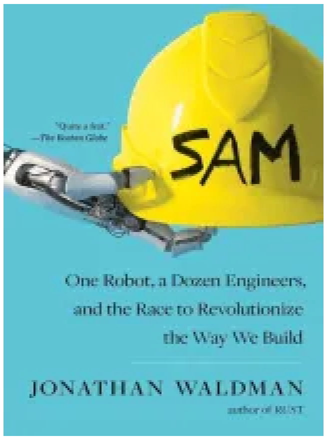
Free



From Gutenberg to Google: The History of Our Future Tom Wheeler

(3.5/5)

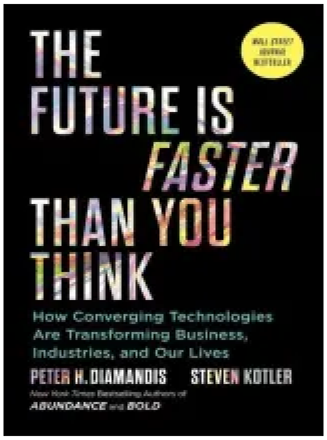
Free



SAM: One Robot, a Dozen Engineers, and the Race to Revolutionize the Way We Build Jonathan Waldman

(5/5)

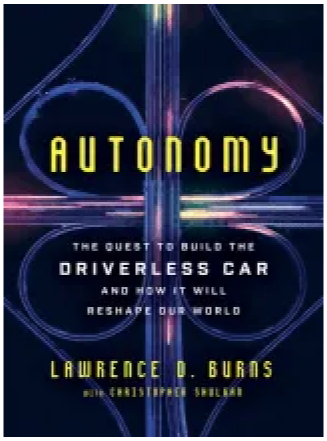
Free



The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives Peter H. Diamandis

(4.5/5)

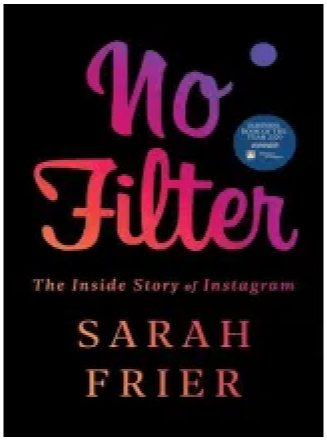
Free



Autonomy: The Quest to Build the Driverless Car—And How It Will Reshape Our World Lawrence D. Burns

(5/5)

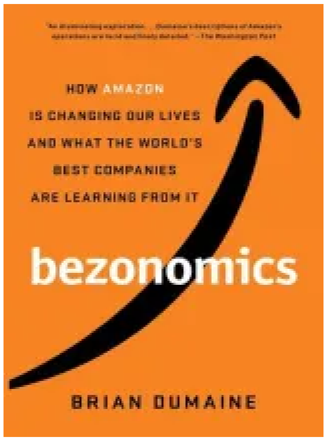
Free



No Filter: The Inside Story of Instagram Sarah Frier

(4.5/5)

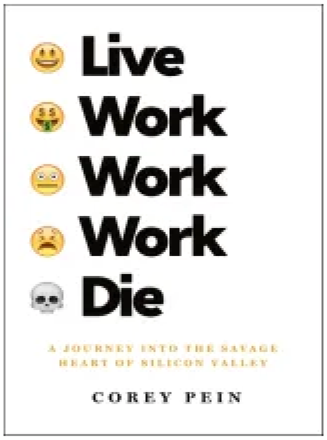
Free



Bezonomics: How Amazon Is Changing Our Lives and What the World's Best Companies Are Learning from It Brian Dumaine

(4/5)

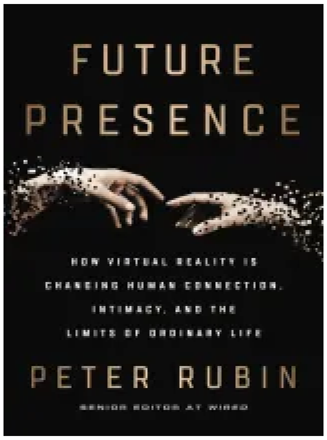
Free



Live Work Work Work Die: A Journey into the Savage Heart of Silicon Valley Corey Pein

(4.5/5)

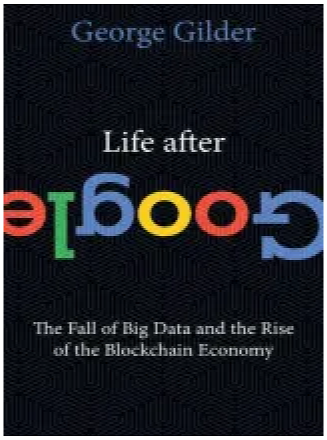
Free


FUTURE PRESENCE
HOW VIRTUAL REALITY IS CHANGING HUMAN CONNECTION, INTIMACY, AND THE LIMITS OF ORDINARY LIFE
PETER RUBIN
SENIOR EDITOR AT WIRED

Future Presence: How Virtual Reality Is Changing Human Connection, Intimacy, and the Limits of Ordinary Life Peter Rubin

(4/5)

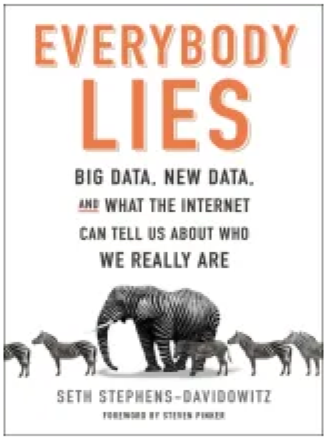
Free



Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy George Gilder

(4/5)

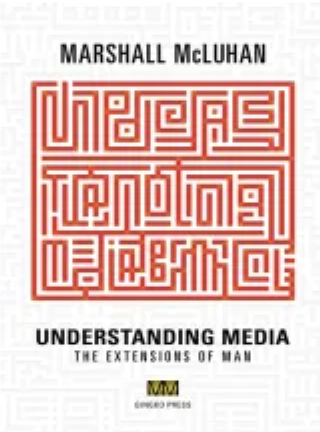
Free


EVERYBODY LIES
BIG DATA, NEW DATA, AND WHAT THE INTERNET CAN TELL US ABOUT WHO WE REALLY ARE
SETH STEPHENS-DAVIDOWITZ
FOREWORD BY STEVEN PINKER

Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are Seth Stephens-Davidowitz

(4.5/5)

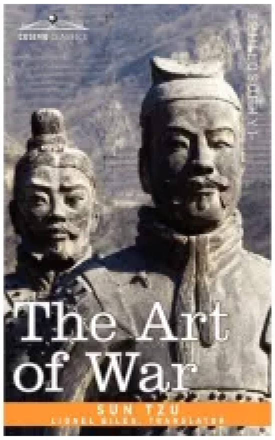
Free



Understanding Media: The Extensions of Man Marshall McLuhan

(4/5)

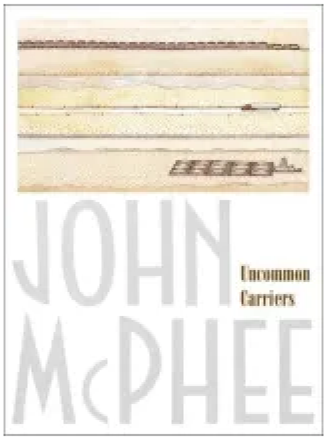
Free



The Art of War Sun Tsu

(3/5)

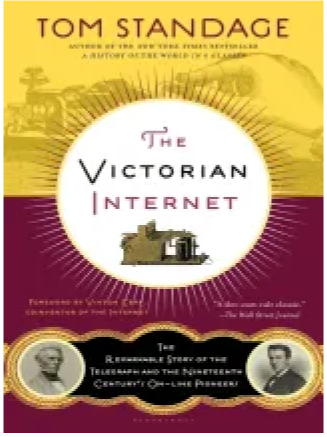
Free



Uncommon Carriers John McPhee

(3.5/5)

Free


TOM STANDAGE
The Victorian Internet
The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers

The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers Tom Standage

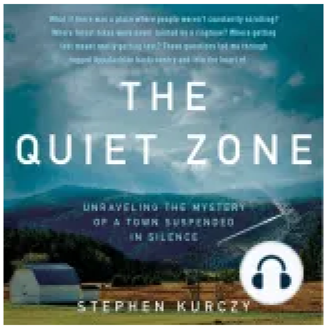
(3.5/5)

Free

Related Audiobooks

Free with a 14 day trial from Scribd

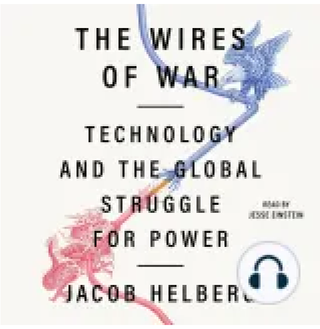
See all



The Quiet Zone: Unraveling the Mystery of a Town Suspended in Silence Stephen Kurczy

(4.5/5)

Free



The Wires of War: Technology and the Global Struggle for Power Jacob Helberg

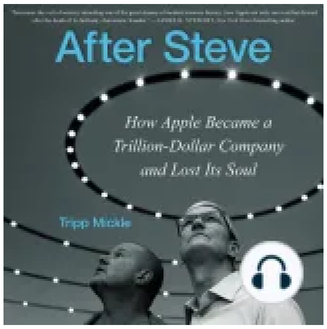
(4/5)

Free

System Error: Where Big Tech Went Wrong and How We Can Reboot Rob Reich

(4.5/5)

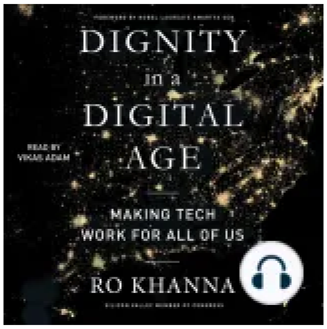
Free



After Steve: How Apple Became a Trillion-Dollar Company and Lost its Soul Tripp Mickle

(4.5/5)

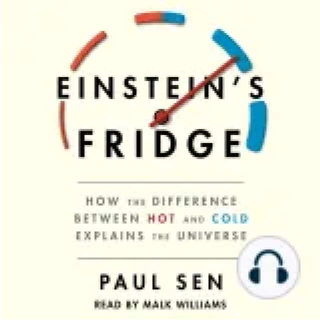
Free



Dignity in a Digital Age: Making Tech Work for All of Us Ro Khanna

(4/5)

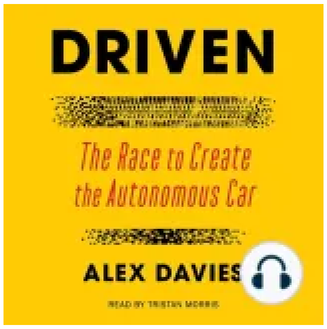
Free



Einstein's Fridge: How the Difference Between Hot and Cold Explains the Universe Paul Sen

(4.5/5)

Free



Driven: The Race to Create the Autonomous Car Alex Davies

(4.5/5)

Free

Test Gods: Virgin Galactic and the Making of a Modern Astronaut Nicholas Schmidle

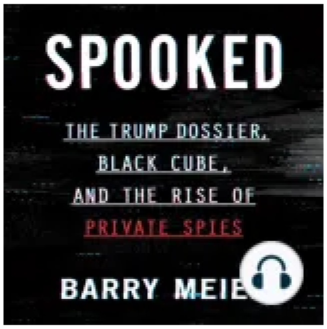
(5/5)

Free

Second Nature: Scenes from a World Remade Nathaniel Rich

(5/5)

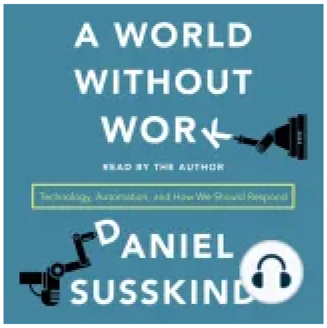
Free


SPOOKED
THE TRUMP DOSSIER, BLACK CUBE, AND THE RISE OF PRIVATE SPIES
BARRY MEIE

Spooked: The Trump Dossier, Black Cube, and the Rise of Private Spies Barry Meier

(4/5)

Free



A World Without Work: Technology, Automation, and How We Should Respond Daniel Susskind

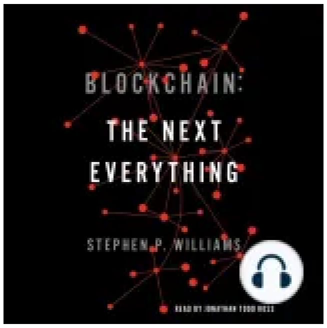
(4.5/5)

Free

Lean Out: The Truth About Women, Power, and the Workplace Marissa Orr

(4.5/5)

Free



Blockchain: The Next Everything Stephen P. Williams

(4/5)

Free

Inside Cybercrime Groups Harvesting Active Directory for Fun and Profit - Vitali Kremez

1. 1. Inside Cybercrime Groups Harvesting Active Directory for Fun & Profit CONFIDENCE 2019 @VK_Intel Vitali Kremez

2. 2. Introducing Cybercrime Groups Talk Outline 1 3 TrickBot in the Cloud: CloudJumper MSP Intrusion Active Directory Enumeration Methodologies 2 4 Life Cycle of High-Profile Event: Typical Exploitation & TTPs 5 Detections & Mitigations 5 Key Takeaways & Outlook
3. 3. Cybercrime Enterprise Deal with Big Data • Sophisticated criminal enterprises such as TrickBot & QakBot - focused on parsing and identifying high-value targets (HVT) • Need reliable install loaders - intermittently rely on Emotet Loader for installs • Big botnet data collectors necessitate scalable solutions to identify high-value targets (corporate networks with local domains) versus "useless" infections • Simple idea: Squeeze as £ / € / $ value from your bots as possible • Banking Malware • Credential Stealer • Miner • Ransomware! Reference: "Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM
4. 4. Cybercrime Enterprise Deal with Big Data Reference: "Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM
5. 5. Emotet (Loader for Installs) -> TrickBot -> Ryuk Ransomware (via PowerShell Empire/Cobalt Strike) Reference: "Charting the Next Cybercrime Frontier, or Evolution of Criminal Intent https://www.youtube.com/watch?v=ptL0aTYzRfM Credit: Ryuk image (https://nogiartshop.com/products/ryuk) …Network & Active Directory Parsing!…. Automated Malware + Interactive Human Exploitation Operator
6. 6. Scope of TrickBot Installs: How Big is the Problem?
7. 7. Newer Cybercrime Frontier: TrickBot Makes Headlines with Ryuk Install via Active Directory
8. 8. TrickBot in the Cloud: CloudJumper MSP Intrusion: $5 Billion Extortion Amount in Total (!) Reference: https://twitter.com/barton_paul/status/1127088679132987394
9. 9. TrickBot Makes Headlines with Ryuk Install via Active Directory: CloudJumper MSP Breached MSP Victim —> Gateway to Other Organization Cloud Infrastructure
10. 10. LDAP Exploitation Methodologies Credit: Rahmat Nurfauzi (https://github.com/infosecn1nja/AD-Attack-Defense/blob/master/README.md)
11. 11. Active Directory Enumeration & Exploitations
12. 12. • "domainDll32," compiled via 'GCC: (Rev1, Built by MSYS2 project) 7.2.0,' allows TrickBot operators to collect domain controller information once they are already on the compromised machine. • This module is internally called "DomainGrabber" and accepts command "getdata" in order to start harvest domain information. • domainDll appears to be aimed at exploiting networks with unsecured domain controllers. domainDll (32|64) Reference: https://www.vkremez.com/2017/12/lets-learn-introducing-new-trickbot.html Active Directory Enumeration Methodologies
13. 13. domainDll (32|64) (decoded) (1e2791877da0249998dea79515a89ca) Active Directory Enumeration Methodologies
14. 14. domainDll (32|64) Active Directory Enumeration Methodologies

15. 15. Active Directory Enumeration Methodologies • “networkDll” module is a single harvester of all possible network victim information from running commands such as "ipconfig /all" and "nltest /domain_trusts /all_trusts" to WMI Query Language (WQL) queries such as "SELECT * FROM Win32_OperatingSystem" to lightweight directory access protocol (LDAP) queries. • Notably, the group leverages "nltest" commands to establish trust relationship between between a compromised workstation and its possible domain before querying LDAP. networkDll (32|64) Reference: https://www.vkremez.com/2018/04/lets-learn-trickbot-implements-network.html
16. 16. networkDll (32|64) (decoded) (aeb08b0651bc8a13dcf5e5f6c0d482f8) Active Directory Enumeration Methodologies
17. 17. networkDll (32|64) Active Directory Enumeration Methodologies
18. 18. • “psfin32” is a point-of-sale finder reconnaissance module hunts for point of sale related services, software, and machines in Lightweight Directory Access Protocol (LDAP) • The module itself does not steal any point-of-sale data but rather used to profile corporate machines of interest with possible point-of-sale devices. • This module arrived just in time for the holiday shopping season highlighting the group interest in exploring possible point-of-sale breaches. psfinDll (32|64) Reference: https://www.vkremez.com/2018/11/lets-learn-introducing-latest-trickbot.html Active Directory Enumeration Methodologies
19. 19. psfinDll (32|64): Typical Point-of-Sale Network Layout Credit: https://www.smart-acc.com/?page=size-options/multiple-outlets/retail Active Directory Enumeration Methodologies
20. 20. psfinDll (32|64) (4fce2da754c9a1ac06ad11a46d215d23) Active Directory Enumeration Methodologies
21. 21. psfinDll (32|64) Active Directory Enumeration Methodologies
22. 22. Life Cycle of High-Profile Event: Typical Exploitation Chain & Tactics, Techniques & Procedures Credit: Brad Duncan (https://www.malware-traffic-analysis.net/2018/10/08/index.html)
23. 23. Life Cycle of High-Profile Event: Victim Domain Parser
24. 24. Life Cycle of High-Profile Event: “No system is safe”
25. 25. Detections & Mitigations • Identify who has AD admin rights (domain/forest) • Identify who can logon to Domain Controllers (& admin rights to virtual environment hosting virtual DCs) • XML Permissions • Place a new xml file in SYSVOL & set Everyone:Deny • Audit Access Denied errors. • Scan Active Directory Domains, OUs, AdminSDHolder, & GPOs for inappropriate custom permissions Credit: Rahmat Nurfauzi (https://github.com/infosecn1nja/AD-Attack-Defense/blob/master/README.md#defense-evasion) Sean Metcalf (https://adsecurity.org/?p=2288)

26. 26. Key Takeaways & Outlook • Automated Malware + Interactive Human Exploitation Operator -> New Cybercrime Frontier • Active Directory & Network Enumeration are the key to identify high-value corporate and multi-tenancy targets for additional monetization (e.g., Ryuk ransomware) • Cloud MSP are the desired targets as they are gateways to their customer environments (e.g., CloudJumper) Credit: CloudJumper image (https://www.drawingtutorials101.com/how-to-draw-cloudjumper-from-how-to-train- your-dragon-2)
27. 27. Special Credit • Joshua Platt • Jason Reaves
28. 28. La Fin Thank you for attending! Please feel free to reach out. @VK_Intel