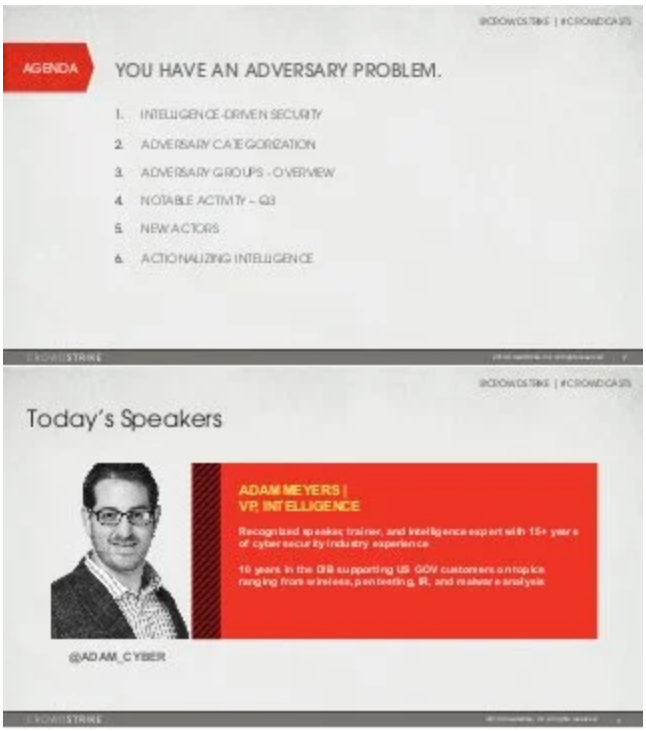
# CrowdCasts Monthly: You Have an Adversary Problem

slideshare.net/CrowdStrike/crowd-casts-monthly-you-have-an-adversary-problem

CrowdStrike


6

Share




Next SlideShares

Upcoming SlideShare


Bear Hunting: History and Attribution of Russian Intelligence Operations

Loading in …3

×

1 of 35

1 of 35

6

Share

Download to read offline

Technology Business

You Have an Adversary Problem. Who's Targeting You and Why?

Nation-States, Hacktivists, Industrial Spies, and Organized Criminal Groups are attacking your enterprise on a daily basis. Their goals range from espionage for technology advancement and disruption of critical infrastructure to for-profit theft of trade secrets and supporting a political agenda. You no longer have a malware problem, you have an adversary problem, and you must incorporate an intelligence-driven approach to your security strategy.

During this CrowdCast, you will learn how to:

Incorporate Actionable Intelligence into your existing enterprise security infrastructure
Quickly understand the capabilities and artifacts of targeted attacked tradecraft
Gain insight into the motivations and intentions of targeted attackers
Make informed decisions based off of specific threat intelligence

CrowdStrike
Follow

You Have an Adversary Problem. Who's Targeting You and Why?

Nation-States, Hacktivists, Industrial Spies, and Organized Criminal Groups are attacking your enterprise on a daily basis. Their goals range from espionage for technology advancement and disruption of critical infrastructure to for-profit theft of trade secrets and supporting a political agenda. You no longer have a malware problem, you have an adversary problem, and you must incorporate an intelligence-driven approach to your security strategy.

During this CrowdCast, you will learn how to:

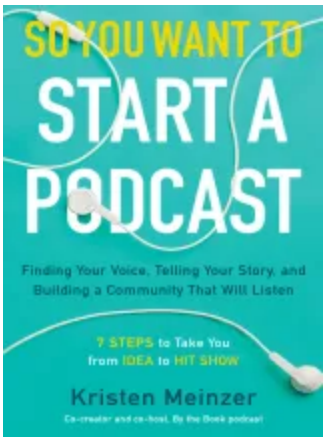
Incorporate Actionable Intelligence into your existing enterprise security infrastructure
Quickly understand the capabilities and artifacts of targeted attacked tradecraft
Gain insight into the motivations and intentions of targeted attackers
Make informed decisions based off of specific threat intelligence
Technology Business

## More Related Content

### Related Books

Free with a 14 day trial from Scribd

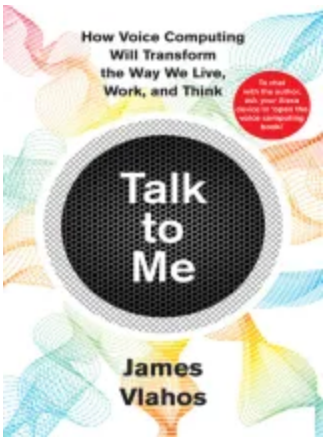
See all




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

(3.5/5)

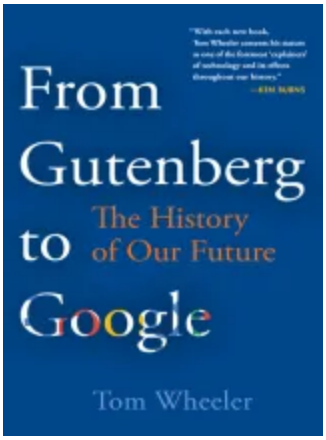
Free




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

(4/5)

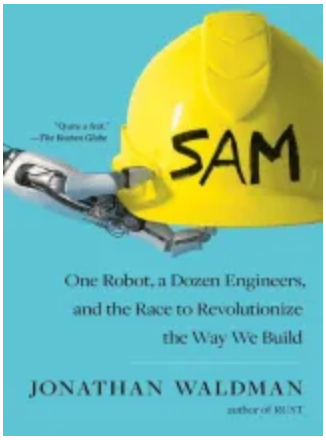
Free




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

(3.5/5)

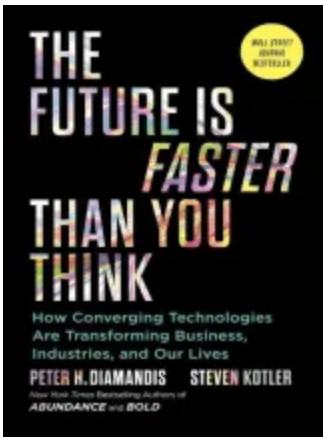
Free




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

(5/5)

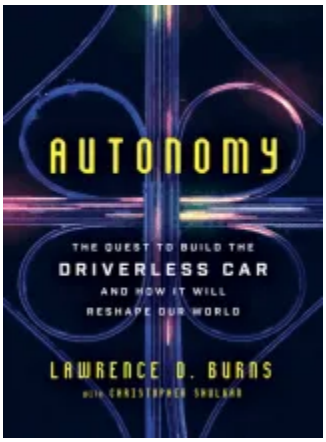
Free




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

(4.5/5)

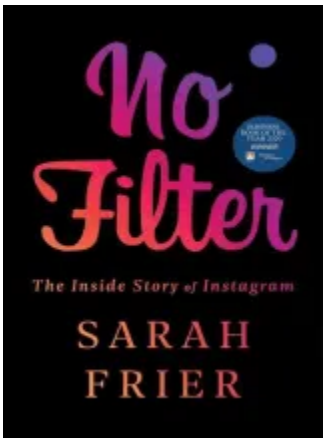
Free




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

(5/5)

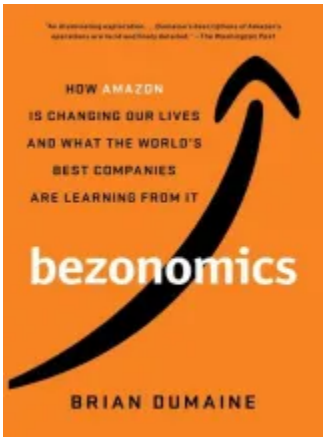
Free




No Filter: The Inside Story of Instagram Sarah Frier

(4.5/5)

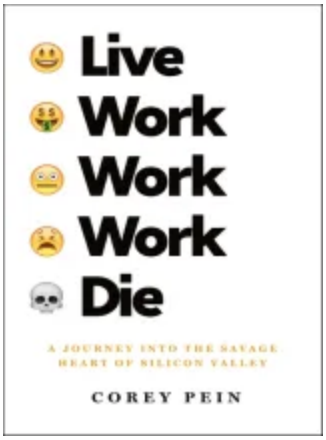
Free




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

(4/5)

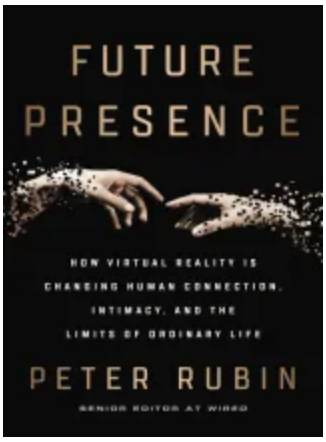
Free




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

(4.5/5)

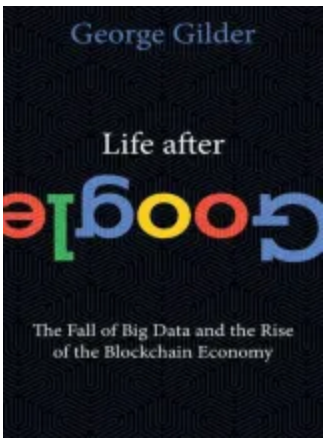
Free




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

(4/5)

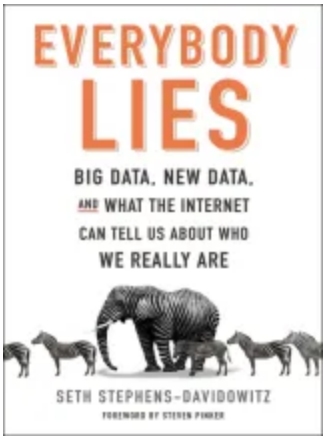
Free



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

(4/5)

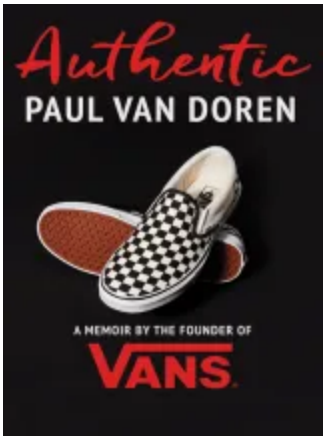
Free




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

(4.5/5)

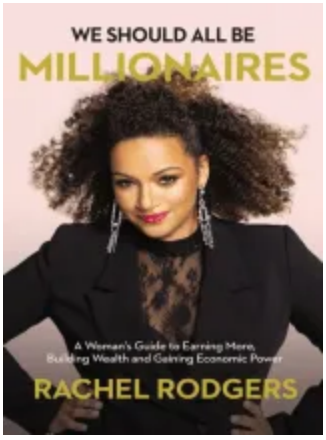
Free




Authentic: A Memoir by the Founder of Vans Louise Maclellan

(4.5/5)

Free




We Should All Be Millionaires: A Woman's Guide to Earning More, Building Wealth, and Gaining Economic Power Rachel Rodgers

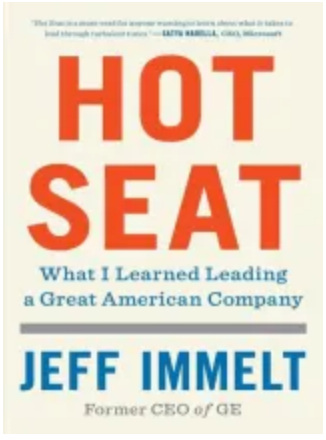
(4.5/5)

Free


Believe IT: How to Go from Underestimated to Unstoppable Jamie Kern Lima

(4.5/5)

Free




Hot Seat: What I Learned Leading a Great American Company Jeff Immelt

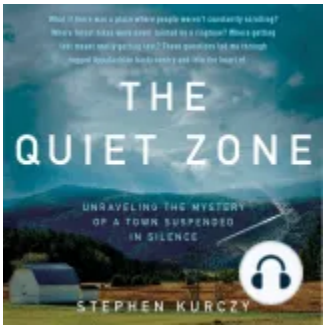
(4.5/5)

Free

## Related Audiobooks

Free with a 14 day trial from Scribd

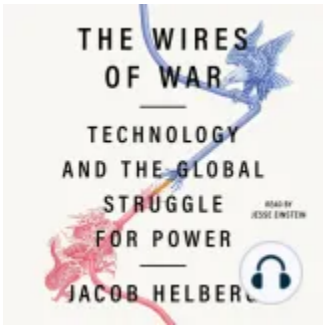
See all




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

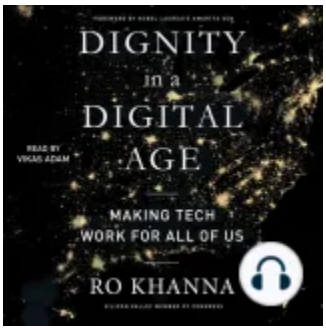
(4.5/5)

Free


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

(4.5/5)

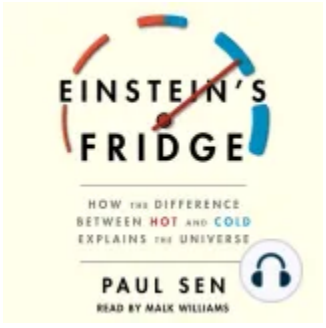
Free




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

(4/5)

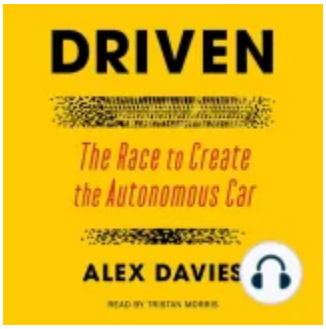
Free




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 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


Uncanny Valley: A Memoir Anna Wiener

(4/5)

Free


User Friendly: How the Hidden Rules of Design Are Changing the Way We Live, Work, and Play Cliff Kuang

(4.5/5)

Free


Bitcoin Billionaires: A True Story of Genius, Betrayal, and Redemption Ben Mezrich

(4.5/5)

Free

1. 1. You Have an ADVERSARY PROBLEM. Who's Targeting You and Why?
2. 2. @CROWDSTRIKE | #CROWDCASTS AGENDA YOU HAVE AN ADVERSARY PROBLEM. 1. INTELLIGENCE-DRIVEN SECURITY 2. ADVERSARY CATEGORIZATION 3. ADVERSARY GROUPS - OVERVIEW 4. NOTABLE ACTIVITY – Q3 5. NEW ACTORS 6. ACTIONALIZING INTELLIGENCE 2013 CrowdStrike, Inc. All rights reserved. 2

3. 3. @CROWDSTRIKE | #CROWDCASTS Today's Speakers ADAM MEYERS | VP, INTELLIGENCE Recognized speaker, trainer, and intelligence expert with 15+ years of cyber security industry experience 10 years in the DIB supporting US GOV customers on topics ranging from wireless, pen testing, IR, and malware analysis @ADAM_CYBER 2013 Crowdstrike, Inc. All rights reserved. 3
4. 4. @CROWDSTRIKE | #CROWDCASTS Today's Speakers MATT DAHL | SENIOR ANALYST/ LEGAL COUNSEL Cyber threat analyst focused on targeted intrusion activity Focused on investigating indicators of compromise to identify specific adversary activity Legal liaison to the CrowdStrike Intelligence Team @CROWDSTRIKE 2013 Crowdstrike, Inc. All rights reserved. 4
5. 5. @CROWDSTRIKE | #CROWDCASTS Adversaries are humans Targeted Attackers: WHO ARE THE ADVERSARIES? Motivation can range from disruption, theft, to even destruction They need to get in They will likely need to move laterally Spray and Pray (Prey): They don't care who they target (sometimes what) The more they compromise the more they win Motivation can range from disruption, theft, to even destruction 2013 Crowdstrike, Inc. All rights reserved. 5
6. 6. INTELLIGENCE-DRIVEN SECURITY 2013 CrowdStrike, Inc. All rights reserved. 6
7. 7. @CROWDSTRIKE | #CROWDCASTS Adversary Categorization CATEGORIZATION| Adversary Groups 1 Tactics, Techniques, and Practices 2 Never assume relationships exist Between indicators 3 Recognize adversaries are constantly changing 4 But RECOGNIZE they are HUMAN CATEGORIZATION 2013 Crowdstrike, Inc. All rights reserved. 7
8. 8. Intelligence: Adversary Groups @CROWDSTRIKE | #CROWDCASTS CHINA Anchor Panda Comment Panda Impersonating Panda Temper Panda Keyhole Panda Aurora Panda Stone Panda Vixen Panda Union Panda Poisonous Panda Pirate Panda Dagger Panda Violin Panda Putter Panda Test Panda Gibberish Panda Electric Panda Wet Panda Karma Panda Dynamite Panda Radio Panda Samurai Panda Toxic Panda Numbered Panda Pitty Panda Foxy Panda Deep Panda 2013 CrowdStrike, Inc. All rights reserved. 8
9. 9. Intelligence @CROWDSTRIKE | #CROWDCASTS Adversary Groups IRAN Clever Kitten: Energy Companies Cutting Kitten: For Hire NORTH KOREA Silent Chollima: Energy Companies RUSSIA Energetic Bear: Oil and Gas Companies INDIA Viceroy Tiger Government, Legal, Financial, Media, Telecom 2013 CrowdStrike, Inc. All rights reserved. 9
10. 10. Intelligence @CROWDSTRIKE | #CROWDCASTS Adversary Groups HACKTIVIST/ACTIVIST/ TERRORIST CRIMINAL Deadeye Jackal Commercial, Singing Spider Commercial, Financial Financial, Media, Social Networking Union Spider Manufacturing Ghost Jackal Commercial, Energy, Andromeda Spider Numerous Financial Corsair Jackal Commercial, Technology, Financial, Energy Extreme Jackal Military, Government 2013 CrowdStrike, Inc. All rights reserved. 10

11. 11. @CROWDSTRIKE | #CROWDCASTS Notable Activity – Q3 NEW ADVERSARIES STONE PANDA | NIGHTSHADE PANDA | GOBLIN PANDA | CORSAIR JACKAL NOTABLE ACTIVITY DEADEYE JACKAL | NUMBERED PANDA | SILENT CHOLLIMA 2013 Crowdstrike, Inc. All rights reserved. 11
12. 12. NEW ACTORS 2013 CrowdStrike, Inc. All rights reserved. 12
13. 13. Intelligence: STONE PANDA OPERATIONAL WINDOW May 2010 to Present @CROWDSTRIKE | #CROWDCASTS TARGETING Healthcare Defense Aerospace OBJECTIVES Recon Lateral movement Data exfiltration Government TOOLS Poison Ivy RAT IEChecker/EvilGrab 2013 CrowdStrike, Inc. All rights reserved. 13
14. 14. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Healthcare, Defense, Aerospace, Government Delivery: Likely spearphishing WHO IS STONE PANDA? Malware: Poison Ivy and EvilGrab/ IEChecker Known Poison Ivy passwords: menuPass, happyyongzi, Thankss, Xgstone, keaidestone, and admin C2 Indicators: fbi.sexxxy.biz; u1.FartIT.com; jj.mysecondarydns.com; 54.241.13.219; 184.169.176.71; 114.80.96.8 2013 Crowdstrike, Inc. All rights reserved. 14
15. 15. Intelligence: NIGHTSHADE PANDA OPERATIONAL WINDOW Feb 2008 to Present OBJECTIVES Recon Lateral movement Data exfiltration @CROWDSTRIKE | #CROWDCASTS TARGETING Media NGO/Int'l Relations Universities TOOLS Poison Ivy PlugX 2013 CrowdStrike, Inc. All rights reserved. 15
16. 16. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Media; NGO/Int'l Relations; Universities WHO IS NIGHTSHADE PANDA? Delivery: Likely spearphishing Malware: PlugX and Poison Ivy Known Poison Ivy passwords: synnia C2 Indicators: www.adv138mail.com; pu.flowershow.org; tech.network-sec.net; 184.105.178.83; 199.59.243.106; 112.137.162.151 2013 Crowdstrike, Inc. All rights reserved. 16
17. 17. Intelligence: GOBLIN PANDA OPERATIONAL WINDOW July 2012 to July 2013 OBJECTIVES Recon Lateral movement Data exfiltration @CROWDSTRIKE | #CROWDCASTS TARGETING Aerospace Defense Energy Government Shipping TOOLS Technology Spearphishing using office doc ZeGhost specific mutexes 2013 CrowdStrike, Inc. All rights reserved. 17
18. 18. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Aerospace; Defense; Energy; Government; Shipping; Technology; Telecommunications WHO IS GOBLIN PANDA? Delivery: Spearphishing Malware: HttpTunnel (AV detection = Zegost) Mutexes: HttpTunnel@@ or Http@@@ C2 Indicators: vnpt.conimes.com; mofa.conimes.com; pvep.scvhosts.com; 112.175.79.55; 223.26.55.122; 198.100.97.245 2013 Crowdstrike, Inc. All rights reserved. 18
19. 19. @CROWDSTRIKE | #CROWDCASTS Intelligence: CORSAIR JACKAL OPERATIONAL WINDOW February 2013 to May 2013 OBJECTIVES Information Disclosure TARGETING Energy Financial Government Shipping Telecom TOOLS Cross Site Scripting (XSS) 2013 CrowdStrike, Inc. All rights reserved. 19

20. 20. @CROWDSTRIKE | #CROWDCASTS Timeline: CORSAIR JACKAL 2012 XTnR3v0LT colludes with Anonymous group XL3gi0n January 25, 2013 New members added January 22, 2013 XTnR3v0LT announce formation of TCA March 1 2013 Announced compromise of US financial February 2013 Announced participation in #opblacksummer July 29 2013 Ben Khlifa announces new personal page May 7, 2013 XTnR3v0LT arrested by Tunisian Authorities September 2, 2013 Tweets XSS vulnerability on Sourceforge 2013 CrowdStrike, Inc. All rights reserved. 20
21. 21. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Energy; Financial; Government; Shipping; Telecommunications WHO IS CORSAIR JACKAL? Primarily One Individual: Fahmi Ben Khlifa (XTnR3v0LT) Professed nationalistic motivations for malicious activity, but also white hat activity. Cross-site scripting attacks used to compromise databases at target organizations. 2013 Crowdstrike, Inc. All rights reserved. 21
22. 22. NOTABLE ACTIVITY 2013 CrowdStrike, Inc. All rights reserved. 22
23. 23. @CROWDSTRIKE | #CROWDCASTS Intelligence: DEADEYE JACKAL OPERATIONAL WINDOW TARGETING May 2011 to Present Financial Institution Media/News Social Network Platforms OBJECTIVES Propaganda Disinformation Disruption TOOLS Spearphishing Web Exploitation Facebook Spamming 2013 CrowdStrike, Inc. All rights reserved. 23
24. 24. @CROWDSTRIKE | #CROWDCASTS Timeline: DEADEYE JACKAL August 26, 2011 May 5, 2011 SEA Mohammad Ahmad Fall 2011 – Spring 2013 Officially Formed Kabbani Killed Web Defacements Facebook Spamming September 2011 Harvard Defacement July 2013 3rd Party Provider Breaches February 2013 Twitter Account Takeovers August 2013 Domain Hijacking 2013 CrowdStrike, Inc. All rights reserved. 24
25. 25. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Financial Institutions; Media/News; Social Network Platforms WHO IS DEADEYE JACKAL? Delivery: Spearphishing Nationalistic, pro-Syrian regime motivations Defacement, account takeover, third-party provider attacks, credential collection 2013 Crowdstrike, Inc. All rights reserved. 25
26. 26. Intelligence: NUMBERED PANDA OPERATIONAL WINDOW 2009 - Present OBJECTIVES Recon Lateral movement Data exfiltration @CROWDSTRIKE | #CROWDCASTS TARGETING Government Financial Telecom Technology Media TOOLS Spearphishing Dynamic Calculation 2013 CrowdStrike, Inc. All rights reserved. 26
27. 27. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Government; Financial; Telecommunications; Media WHO IS NUMBERED PANDA? Delivery: Spearphishing Malware: Ixeshe, Mswab, Gh0st, ShowNews, 3001 C2 Indicators: getfresh.dnsrd.com; serial.ddns.ms; gfans.onmypc.us; 23.19.122.202; 192.154.108.10; 192.154.111.200 2013 Crowdstrike, Inc. All rights reserved. 27

28. 28. Intelligence: SILENT CHOLLIMA OPERATIONAL WINDOW 2007 to Present @CROWDSTRIKE | #CROWDCASTS TARGETING Multiple targets in ROK Global Targets of Opportunity OBJECTIVES Recon Criminal Monetization Lateral movement Data Destruction TOOLS Custom Malware 2013 CrowdStrike, Inc. All rights reserved. 28
29. 29. @CROWDSTRIKE | #CROWDCASTS Target Sectors: Media WHO IS SILENT CHOLLIMA? Delivery: Spearphishing Malware: HTTP/IRC-based; Tdrop; Concealment Troy; LSG C2 indicators: www.designface.net; www.sdmp.kr; www.socrates.tw; 202.172.28.111; 63.115.31.15; 209.137.232.3 2013 Crowdstrike, Inc. All rights reserved. 29
30. 30. @CROWDSTRIKE | #CROWDCASTS INTELLIGENCE-DRIVEN SECURITY INTELLIGENCE| Adversary-Centric 1 INTELLIGENCE Understand the adversaries targeting your Vertical | Company | Geo-Location | Customers 2 Build appropriate defenses to counter/detect these adversaries 3 Perform other security practices from an Adversary-centric perspective Pen Testing (Red Team) Security Operations Briefings Log Review 2013 Crowdstrike, Inc. All rights reserved. 30
31. 31. @CROWDSTRIKE | #CROWDCASTS INTELLIGENCE-DRIVEN SECURITY INTELLIGENCE| Making it Actionable 1 ACTIONALIZING INTELLIGENCE Intelligence is difficult to consume Lots of information to keep straight New data constantly flowing in (possibly unvetted) 2 Security Operations need to change shi□s & people 3 Actionable Intelligence Pass down can't possibly occur with all indicators 2013 Crowdstrike, Inc. All rights reserved. 31
32. 32. @CROWDSTRIKE | #CROWDCASTS Adversary Microsite COMING SOON TRACK: Track current Adversaries against other Industry nomenclature OVERVIEW: Gain insight Into adversary – new groups Added weekly 2013 Crowdstrike, Inc. All rights reserved. 32
33. 33. @CROWDSTRIKE | #CROWDCASTS RESOURCES Next up: Enterprise Activity Monitoring The Power to HUNT November 5th | 2PM ET/11AM PT Download a Sample Adversary Intelligence Report http://www.crowdstrike.com/ sites/default/ files/deeppanda.pdf For additional information, CONTACT SALES@CROWDSTRIKE.COM *NEW* Videos Every Thursday | 1PM ET http://www.crowdstrike.com/crowdcasts/index.html 2013 Crowdstrike, Inc. All rights reserved. 33
34. 34. Q&A Q&A @CROWDSTRIKE | #CROWDCASTS Please type all questions into the Q&A section of the GoToWebinar Control Panel If you have additional ?'s, contact us At crowdcasts@crowdstrike.com 2013 CrowdStrike, Inc. All rights reserved. 34