BlueHat v17 || 10 Years of Targeted Credential Phishing

slideshare.net/MSbluehat/10-years-of-targeted-credential-phishing-billy-leonard

BlueHat Security Conference

BlueHat v17 || 10 Years of Targeted Credential Phishing | Billy Leonard

1

Share

Next SlideShares

Upcoming SlideShare

BlueHat Seattle 2019 || The cake is a lie! Uncovering the secret world of mal...

Loading in …3

×

1 of 54

1 of 54

BlueHat v17 || 10 Years of Targeted Credential Phishing | Billy Leonard

1

Share

Download to read offline

Technology

While it's not kernel 0days or EMET bypasses, credential phishing has been a go-to in attackers toolboxes for many years, rising to prominence during the run up to the 2016 US Presidential Elections. Being able to access a target's email or files stored in the cloud without burning your prized 0day has proven to be too much for even the most advanced attackers to pass up. In this talk, we will look at how attackers have evolved and adapted their credential phishing operations over the past 10 years, from changes in delivery mechanisms to changes in persistence and exfiltration and how defenses have evolved during that same time.

BlueHat Security Conference
Follow

While it's not kernel 0days or EMET bypasses, credential phishing has been a go-to in attackers toolboxes for many years, rising to prominence during the run up to the 2016 US Presidential Elections. Being able to access a target's email or files stored in the cloud without burning your prized 0day has proven to be too much for even the most advanced attackers to pass up. In this talk, we will look at how attackers have evolved and adapted their credential phishing operations over the past 10 years, from changes in delivery mechanisms to changes in persistence and exfiltration and how defenses have evolved during that same time.

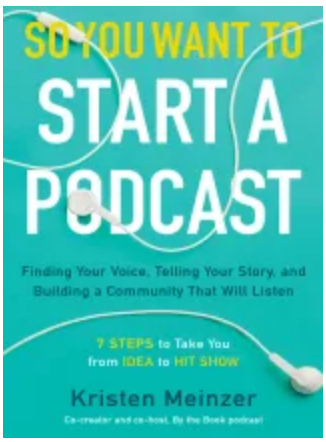
Technology

More Related Content

Related Books

Free with a 14 day trial from Scribd

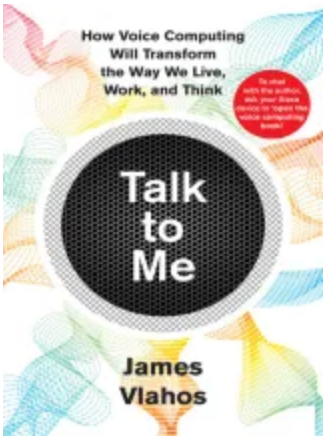
See all



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

(3.5/5)

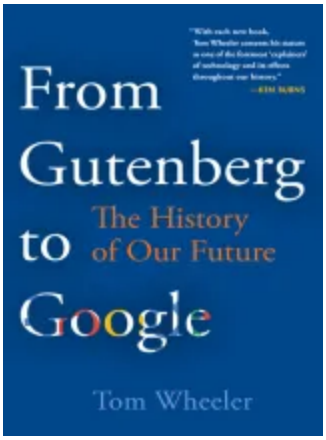
Free



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

(4/5)

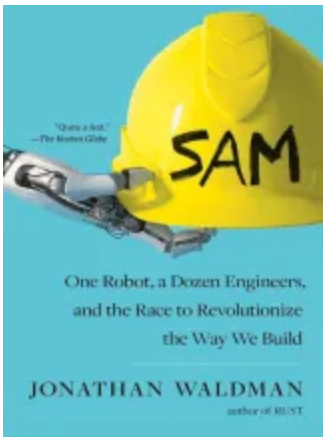
Free



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

(3.5/5)

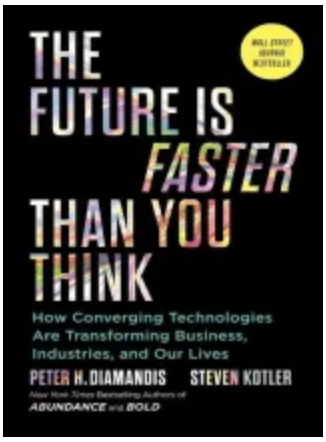
Free



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

(5/5)

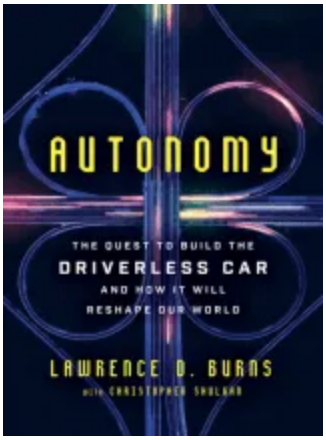
Free



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

(4.5/5)

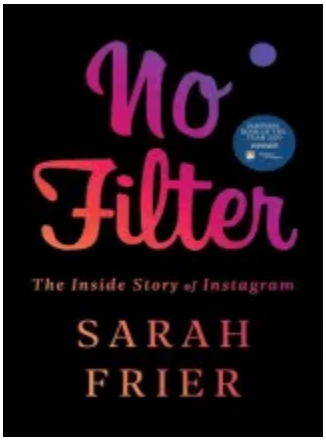
Free



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

(5/5)

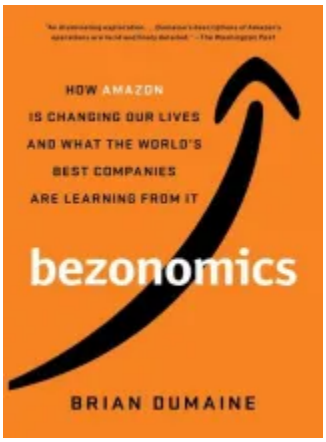
Free



No Filter: The Inside Story of Instagram Sarah Frier

(4.5/5)

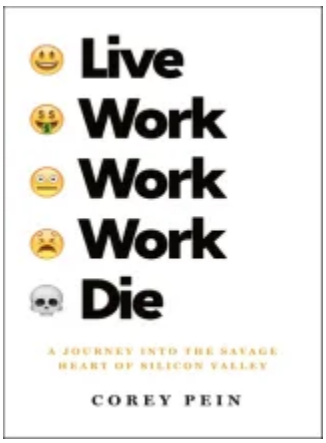
Free



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

(4/5)

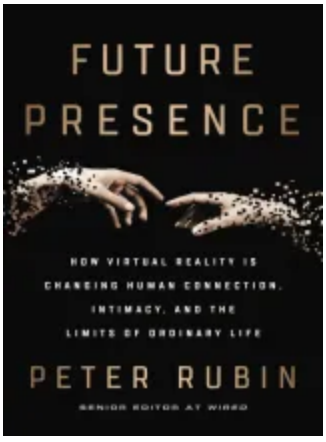
Free



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

(4.5/5)

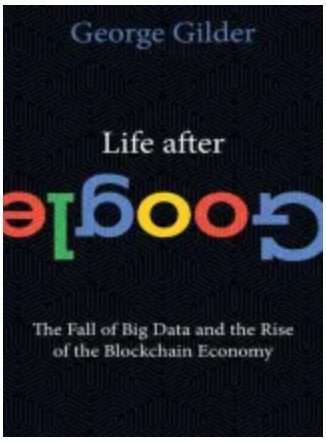
Free



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

(4/5)

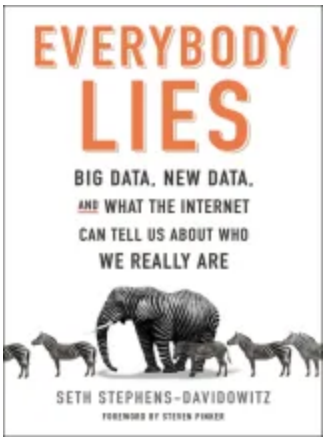
Free



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

Understanding Media: The Extensions of Man Marshall McLuhan

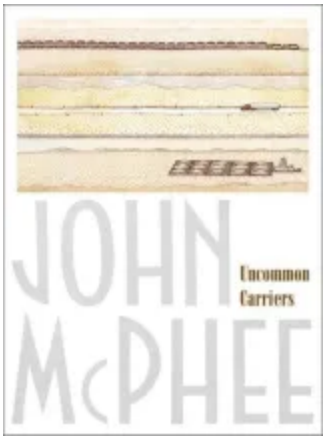
(4/5)

Free

The Art of War Sun Tsu

(3/5)

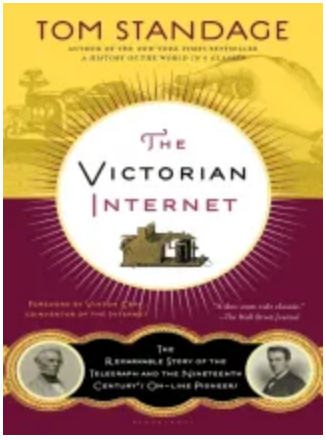
Free



Uncommon Carriers John McPhee

(3.5/5)

Free



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

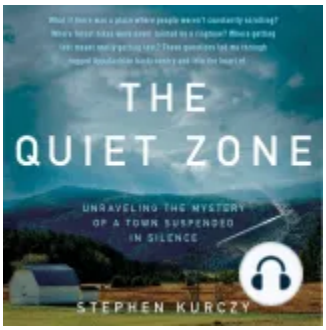
(3.5/5)

Free

Related Audiobooks

Free with a 14 day trial from Scribd

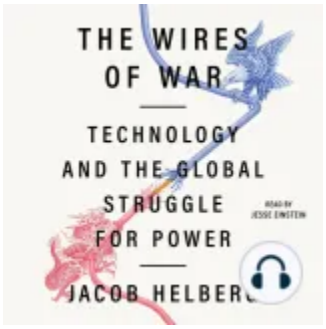
See all



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

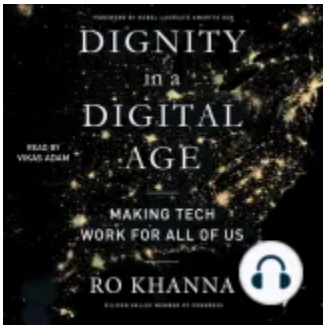
(4.5/5)

Free

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

(4.5/5)

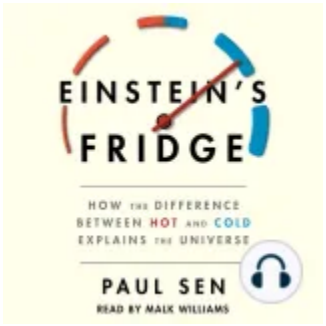
Free



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

(4/5)

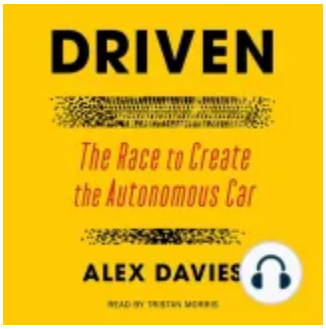
Free



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

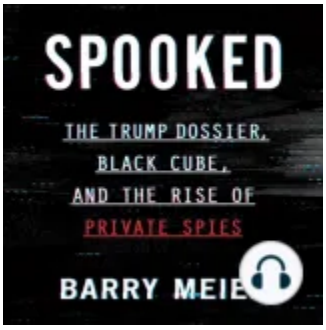
(5/5)

Free

Second Nature: Scenes from a World Remade Nathaniel Rich

(5/5)

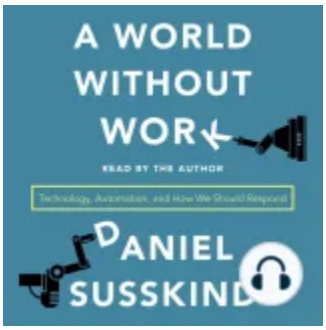
Free



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

BlueHat v17 || 10 Years of Targeted Credential Phishing | Billy Leonard

1. 1. Threat Analysis Group November 2017 - @billyleonard 10 Years of Targeted Credential Phishing
2. 2. Threat Analysis Group Billy Leonard Threat Analysis Group
3. 3. Threat Analysis Group But first, ….
4. 4. Threat Analysis Group What we don't see in targeted phishing.
5. 5. Threat Analysis Group
6. 6. Threat Analysis Group Targeted attacks are all really advanced.
7. 7. Threat Analysis Group
8. 8. Threat Analysis Group
9. 9. Threat Analysis Group The Early Days.
10. 10. Threat Analysis Group
11. 11. Threat Analysis Group Source: https://productforums.google.com/forum/?hl=en#!category-topic/gmail/reading-and-receiving-messages/EndXvDGLoe0
12. 12. Threat Analysis Group Source: http://contagiodump.blogspot.com/2011/02/targeted-attacks-against-personal.html

13. 13. Threat Analysis Group Source: http://contagiodump.blogspot.com/2011/02/targeted-attacks-against-personal.html
14. 14. Threat Analysis Group
15. 15. Threat Analysis Group
16. 16. Threat Analysis Group
17. 17. Threat Analysis Group The Middle Ages.
18. 18. Threat Analysis Group
19. 19. Threat Analysis Group Password Alert.
20. 20. Threat Analysis Group
21. 21. Threat Analysis Group Two Factor Bypass.
22. 22. Threat Analysis Group Source: https://breakingdefense.com/2015/06/strike-back-at-chinese-for-opm-hack-build-a-cyber-strategy/, http://www.seleniumhq.org/, http://phantomjs.org/
23. 23. Threat Analysis Group SMS Interception.
24. 24. Threat Analysis Group
25. 25. Threat Analysis Group Source: https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/, https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/, https://www.howtogeek.com/310418/why-you-shouldnt-use-sms-for-two-factor-authentication/
26. 26. Threat Analysis Group Source: https://www.fredericjacobs.com/blog/2016/01/14/sms-login/, https://www.fredericjacobs.com/blog/2016/04/30/more-on-sms-logins/
27. 27. Threat Analysis Group Source: https://www.fredericjacobs.com/blog/2016/04/30/more-on-sms-logins/
28. 28. Threat Analysis Group Security Keys.
29. 29. Threat Analysis Group Source: https://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/, https://www.ftsafe.com/products/FIDO/Multi
30. 30. Threat Analysis Group OAuth.
31. 31. Threat Analysis Group Source: https://msdn.microsoft.com/en-us/office/office365/api/mail-rest-operations, https://developers.google.com/gmail/api/guides/
32. 32. Threat Analysis Group
33. 33. Threat Analysis Group Source: https://www.bankinfosecurity.com/attackers-unleash-oauth-worm-via-google-docs-app-a-9888, https://qz.com/975002/dont-click-the-google-docs-link-in-that-suspicious-email-you-probably-just-got/
34. 34. Threat Analysis Group
35. 35. Threat Analysis Group Present Day.
36. 36. Threat Analysis Group
37. 37. Threat Analysis Group
38. 38. Threat Analysis Group

39. 39. Threat Analysis Group Source: https://bitly.com/, https://ngrok.com/, https://www.mailstore.com/en/products/mailstore-home/, https://takeout.google.com/
40. 40. Threat Analysis Group Source: https://breakdev.org/evilginx-1-0-update-up-your-game-in-2fa-phishing/
41. 41. Threat Analysis Group Who else do we see targeted?
42. 42. Threat Analysis Group
43. 43. Threat Analysis Group
44. 44. Threat Analysis Group More Recently.
45. 45. Threat Analysis Group
46. 46. Threat Analysis Group
47. 47. Threat Analysis Group Next Gen Password Alert
48. 48. Threat Analysis Group
49. 49. Threat Analysis Group Advanced Protection Program
50. 50. Threat Analysis Group
51. 51. Threat Analysis Group Old habits die hard.
52. 52. Threat Analysis Group
53. 53. Threat Analysis Group Lot's of thanks ... Threat Analysis Group Counter Abuse Technologies Jigsaw SafeBrowsing Chrome MSTIC Yahoo/Apple/FB Intel Teams OGs … and a whole cast of characters that are Kind of a Big Deal.
54. 54. Threat Analysis Group Questions?

1 like

Jessica Wilson Dec. 18, 2021

I like this service ⇒ www.HelpWriting.net ⇐ from Academic Writers. I don't have enough time write it by myself.

Views

Total views

763

On SlideShare

0

From Embeds

0

Number of Embeds

36