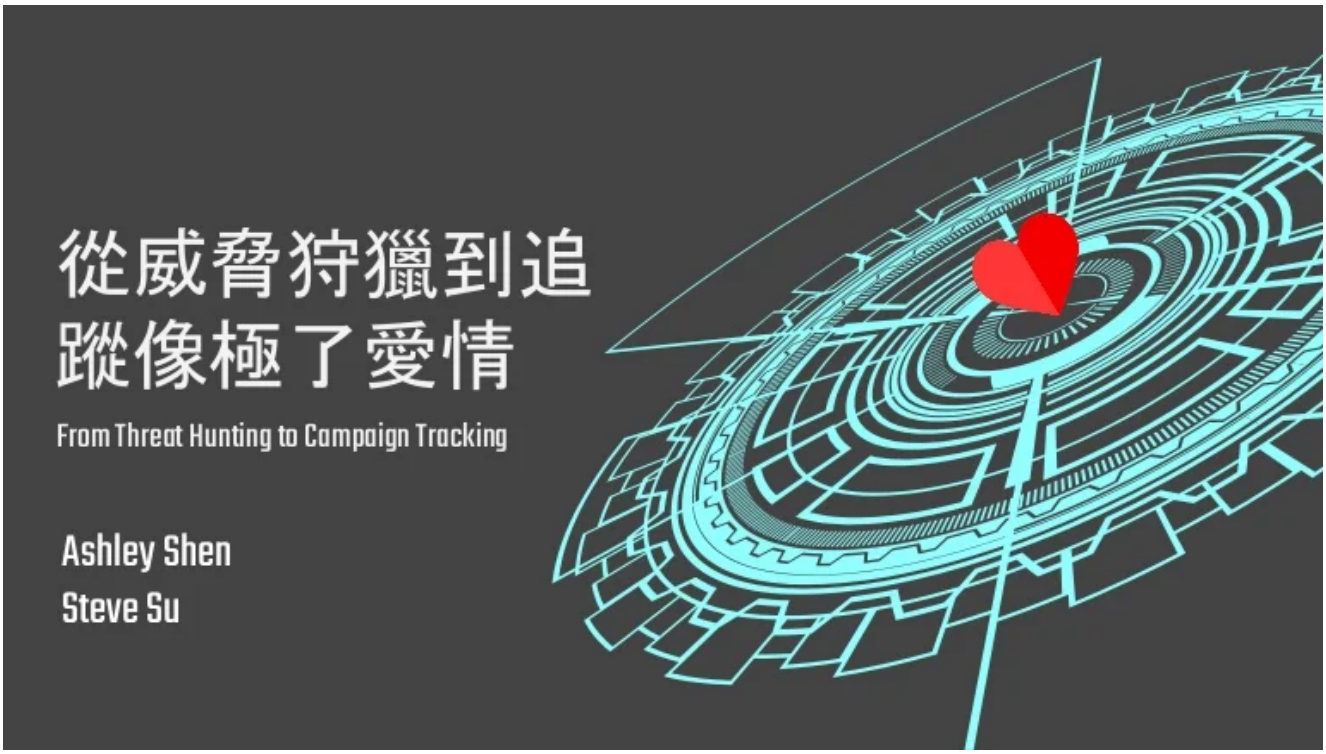
[HITCON 2020 CTI Village] Threat Hunting and Campaign Tracking Worksh…

www2.slideshare.net/ChiEnAshleyShen/hitcon-2020-cti-village-threat-hunting-and-campaign-tracking-workshoppptx/1

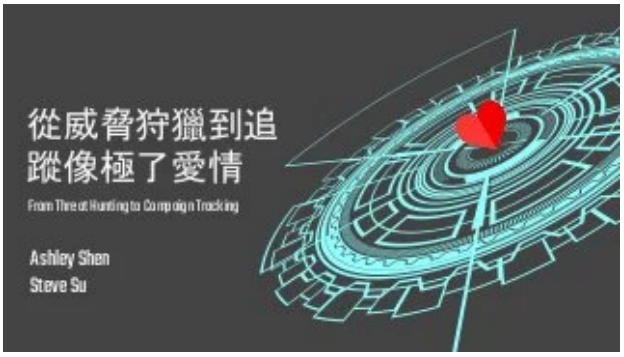
Chi En (Ashley) Shen

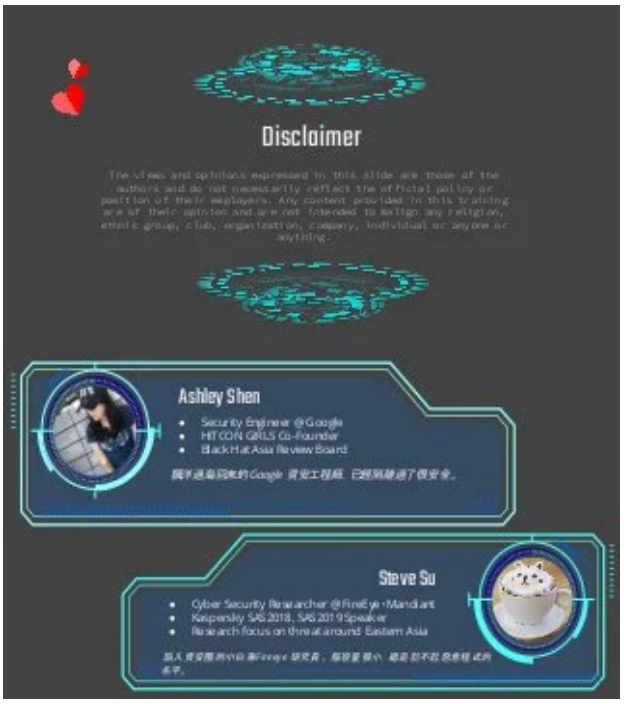


[HITCON 2020 CTI Village] Threat Hunting and Campaign Tracking Workshop.pptx

4

Share





Next SlideShares

Upcoming SlideShare

BSides IR in Heterogeneous Environment

Loading in …3

×

1 of 86

1 of 86

[HITCON 2020 CTI Village] Threat Hunting and Campaign Tracking Workshop.pptx

4

Share

Download to read offline

Technology

Speakers: Ashley Shen, Steve Su
This is a threat hunting and campaign tracking 101 workshop Ashley Shen (Google) and Steve (FireEye) prepared for the HITCON 2020 CTI Village. In this presentation we share the threat hunting concept with some basic techniques and explain the process and guidance for campaign tracking. The presentation was only 65 mins so we couldn't covered everything. However through this talk we hope to share our experience and insight to the beginners.

Chi En (Ashley) Shen
Follow
Security Engineer at Google

Speakers: Ashley Shen, Steve Su
This is a threat hunting and campaign tracking 101 workshop Ashley Shen (Google) and Steve (FireEye) prepared for the HITCON 2020 CTI Village. In this presentation we share the threat hunting concept with some basic techniques and explain the process and guidance for campaign tracking. The presentation was only 65 mins so we couldn't covered everything. However through this talk we hope to share our experience and insight to the beginners.

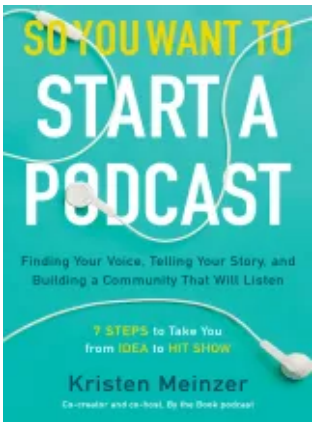
Technology

More Related Content

Related Books

Free with a 14 day trial from Scribd

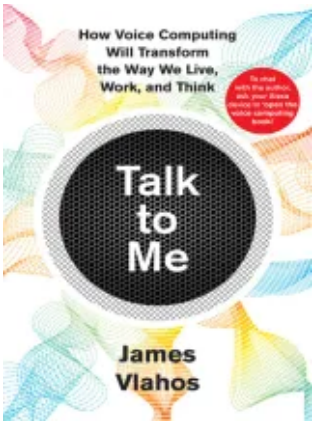
See all



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)

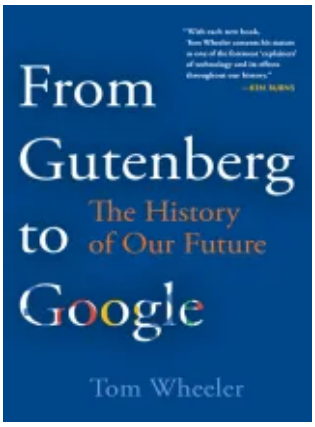
Free



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

(4/5)

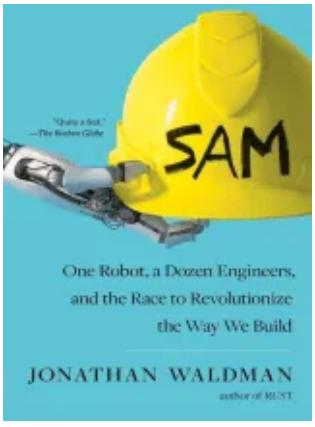
Free



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

(3.5/5)

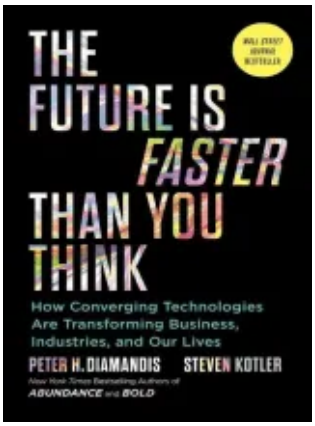
Free



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

(5/5)

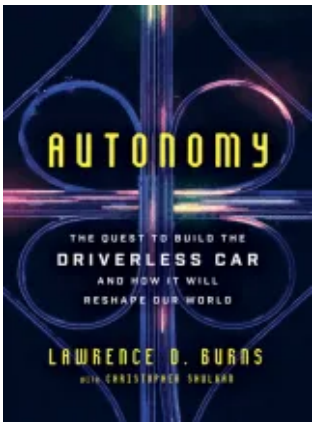
Free



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

(4.5/5)

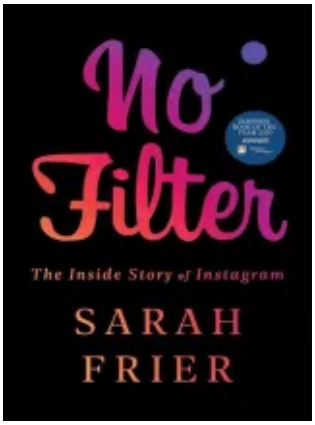
Free



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

(5/5)

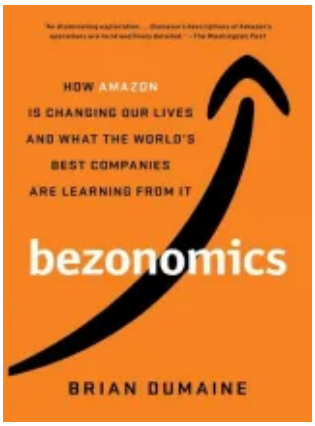
Free



No Filter: The Inside Story of Instagram Sarah Frier

(4.5/5)

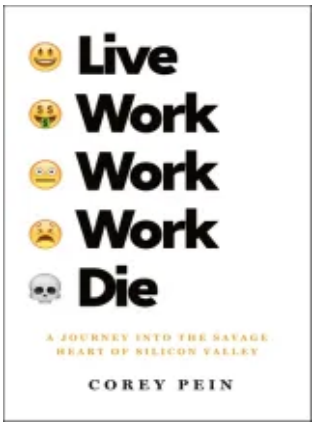
Free



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

(4/5)

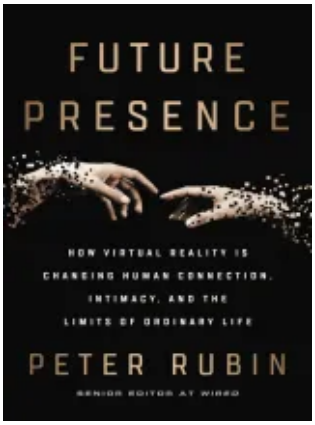
Free



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

(4.5/5)

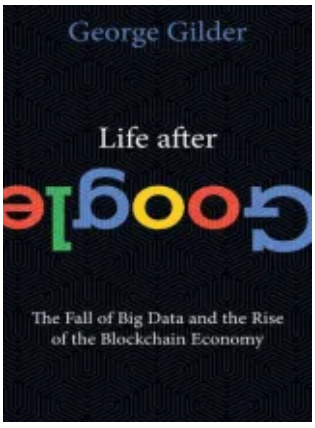
Free



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

(4/5)

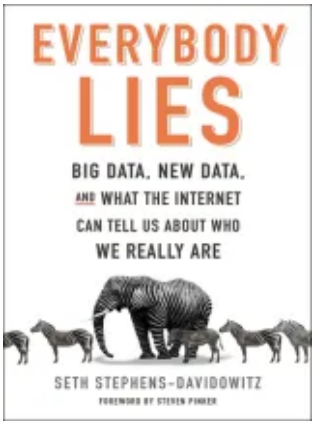
Free



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

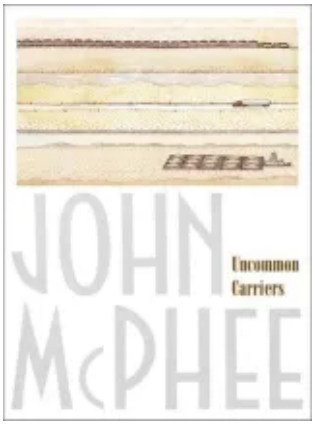
(4/5)

Free

The Art of War Sun Tsu

(3/5)

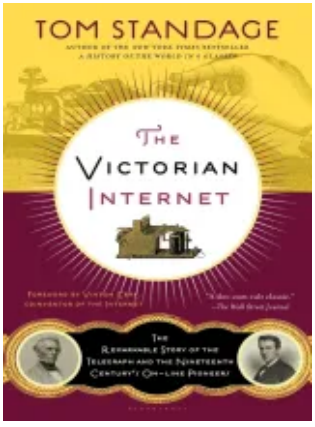
Free



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

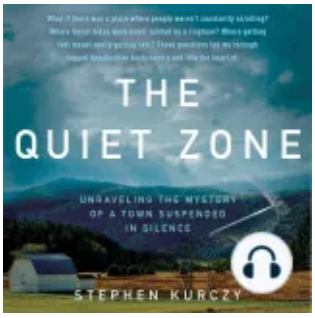
(3.5/5)

Free

Related Audiobooks

Free with a 14 day trial from Scribd

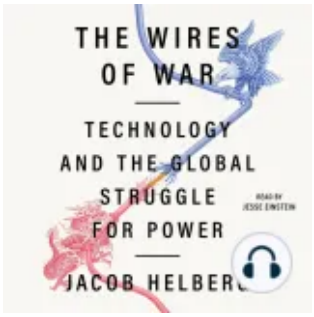
See all



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

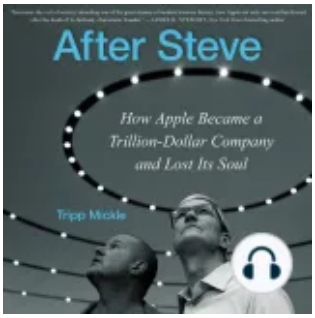
(4/5)

Free

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

(4.5/5)

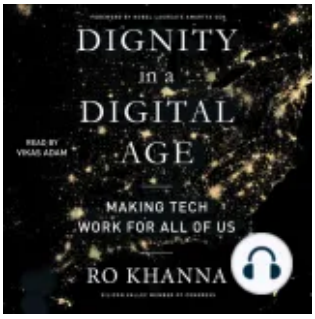
Free



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

(4.5/5)

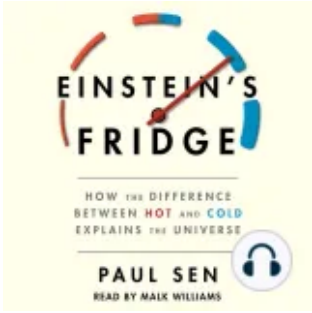
Free



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

(4/5)

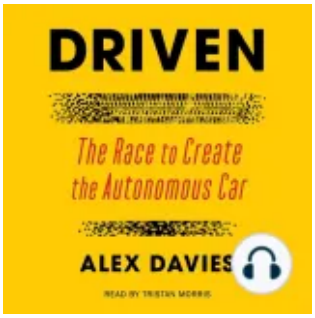
Free



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

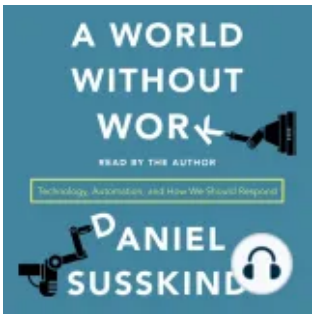
(5/5)

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

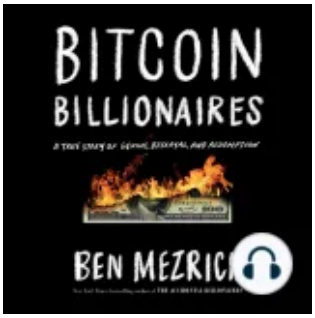
(4/5)

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

[HITCON 2020 CTI Village] Threat Hunting and Campaign Tracking Workshop.pptx

1. 1. AshleyShen SteveSu 從威脅狩獵到追 蹤像極了愛情 FromThreatHuntingtoCampaignTracking
2. 2. The views and opinions expressed in this slide are those of the authors and do not necessarily reflect the official policy or position of their employers. Any content provided in this training are of their opinion and are not intended to malign any religion, ethnic group, club, organization, company, individual or anyone or anything. Disclaimer
3. 3. ● Security Engineer @ Google ● HITCON GIRLS Co-Founder ● Black Hat Asia Review Board 飄洋過海回來的Google 資安工程師，已經隔離過了很安全。 AshleyShen ● Cyber Security Researcher @ FireEye・Mandiant ● Kaspersky SAS2018, SAS2019 Speaker ● Research focus on threat around Eastern Asia 誤入資安圈的小白兼Fireeye 研究員。 腦容量很小，總是記不起惡意程式的 名字。 SteveSu

4. 4. Agenda ThreatHunting101 What is Threat Hunting? Who and why do we do threat hunting?01 How and what tools can we use? 02 What is campaign tracking? How to do it? 03 Case Study. 04 ThreatHuntingTools/Techniques CampaignTracking101 CampaignTrackingCaseStudy
5. 5. 01 ThreatHunting101 5
6. 6. WHATISTHREATHUNTING? Crime Nation-State ARETHE S Hacktivism Disinformation
7. 7. WHATISTHREATHUNTING? Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in your network environment. (Crowdstrike & Me) ● Network ● System ● Service / Platform ● Application (Mobile / Desktop) ● Forums
8. 8. TraditionalDefenseStrategy ProactiveDefenseStrategy 8 Response (or not) when incident happen Hunting the adversary source:freepik source:smashicons
9. 9. KnowntoSelf NotKnowntoSelf Knowto Others ● Internally detected threats shared to partners. ● Threat Intelligence shared by 3rd party. ● Undetected threats discovered by 3rd party and not shared to us. > can be makeup by ingesting more intelligence. NotKnownto Others ● Internally detected threats not shared externally. ● Undetected threats not discovered by anyone but lurking in the shadow. > Most dangerous threat ThreatHuntingfocusThreatDetectionFocus
10. 10. 10 ThreatHuntingservesdifferentpurposefordifferentroles. ● Orgs perform threat hunting to discover threats intruding org environment. ● Leverage Internal telemetry, hunting on internal infrastructure. ProtectingOrg ● Service providers (e.g. Twitter, Facebook, Google) needs to protect services from the abuser and protect users/org from abuses. ● Hunting on platforms, applications, services infrastructure. Protecting Services/Users ● Security vendors perform threat hunting to provide threat intelligence or services (MDR). ● Threat intelligence hunt on external resources (VirusTotal, OSINT...etc). ● Vendors hunts with endpoint telemetry and data. Protecting Customers
11. 11. ThreatHuntingDrivers Awareness-DrivenAnalytics-DrivenIntelligence-Driven
12. 12. ThreatHuntingDrivers Intelligence-Driven ● Threat intelligence provides leads for hunting. ● What is most relevant to me? (Too much information = no information) picture from: malpedia.caad.fkie.fraunhofer.de
13. 13. Quality?ConfidenceLevel?Visibility? Golden Time Operation? Freemilk Operation? Evil New Year Operation? APT10? Menupass? Or not the same elephant?picture from: https://ltcinsurancece.com/the-blind-leading-the-blind-through-ltc-insurance/
14. 14. ThreatHuntingDrivers Analytics-Driven ● Aggregated data gathered from automatic and analytics tools (include but not limit to ML systems, User and Entity Behavior Analytics （UEBA). ● Service provider create customized tools to capture threat signals. https://github.com/Cyb3rWard0g/HELK
15. 15. ThreatHuntingDrivers Awareness-Driven ● Situation-awareness analysis gathered from risk analysis. (e.g. Crown Jewels Analysis (CJA)). https://www.slideshare.net/DougLandoll/finding-and-protecting-your-organizations-crown-jewels

16. 16. ThreatHuntingProcess Investigate the scenarios with tools. Investigate improve existing detection mechanisms with the TTPs and create automatic detection. Create a possible attack scenario that your hunting is focus on. Inform&Enrich CreateHypothesis From the investigation results, find the techniques used by attacker and the pattern to build the actor TTPs profile. UncoverTTPs
17. 17. Leads/Intelligence/Outcome(MyVersionofPyramidofPain) HashValue IPAddress/Domains Network/HostArtifacts Tools/Family TTPs Actors Simple Tough
18. 18. TheThreatHuntersCapabilities TechnicalWritingand ReportingSkills CodingSkill Understandthethreatlandscape AnalyticsSkills(Data,Problems) KnowledgetoMalware,OS,Network, attacker'stechniques...etc. UnderstandingtheInfrastructure/ environment inyourorg What's normal and what's not? To make your hunting tools So you know where to hunt How is this relevant? How strong is the indicator? So you can collaborate and express the threat So you understand what it means? What's the intention?
19. 19. 02 ThreatHunting Tools/Techniques 19
20. 20. CreateHypothesis
21. 21. UnderstandtheThreatIntelligence https://content.fireeye.com/apt-41 /rpt-apt41/ https://securelist.com/winnti-more-than-just-a-game/37029/ https://blog.google/threat-analys is-group/updates-about-govern ment-backed-hacking-and-disinf ormation/
22. 22. MITREATT&CKDesignforIntrusionScenario https://attack.mitre.org/
23. 23. But! LikeImentioned,ThreatHuntingisnotjustfor intrusion.
24. 24. Reconnaissance Weaponized Deliver Exploit Control Execute Maintain TheAttackKillChain MITREATT&CKCoveredWecanactuallyhuntthesetoo!
25. 25. Reconnaissance HuntingReconnaissanceActivities In Reconnaissance stage attacker collects data for the following campaigns. ● Try to catch the attackers before it enter intrusion stages. Common Techniques ● Bots, crawlers, spiders scrapping ○ e.g. Scraping email addresses for targeted attack ● Port Scan
26. 26. Hypothesis ● Attackers are doing scrapping on webpage to collects target's email address. Investigate ● Identify data sources: ○ Proxy logs ○ IIS logs ○ reCaptcha logs ● What is abnormal activities ○ known scripting JA3 fingerprints, known bad IPs from Intelligence ○ Identical outdated User-Agent ○ Traffic without referrers ○ Short sessions and high frequency / high bounce rate https://github.com/puppeteer/pupp eteer https://engineering.salesforce.com/tls-finge rprinting-with-ja3-and-ja3s-247362855967 https://www.youtube.com/
27. 27. Uncover TTPs ● IPs with high solve rate, frequency and speed. ● Comparing request IPs with internal intel, some scrapping IPs were used to send phishing emails. ● Attackers are using reCaptcha farm service to solve reCaptcha. Inform & Enrich ● Leverage phishing emails sender IPs to detect scraping activities or vice versa. ● Using the collected reCaptcha farm solving score to improve reCaptcha service and detection. ● Using the JA3 to detect scripting. https://datadome.co/bot-detection/how-to-detect-captcha-farms-and-block-captcha-bots/ https://anti-captcha.com/

28. 28. JA3/JA3SFingerprint What is this? ● The JA3 algorithm extracts SSL handshake settings for fingerprinting the SSL stack. ● JA3 - client SSL setting fingerprint ● JA3S - server SSL setting fingerprint How can it be useful for threat hunting? ● Detect / identify malware traffic. ● Fingerprint attacker. (Note, not 100% high confident.) https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967
29. 29. JA3/JA3SFingerprint https://sslbl.abuse.ch/ja3-fingerprints/
30. 30. ReconnaissanceHuntingReconnaissanceActivities What to hunt? ● IP address ○ Comparing access IPs with intelligence. ○ Attacker use the scraping IP to send phishing emails ● User-Agent ● JA3 SSL Fingerprint. (identify what kind of tools, or custom tools used by attacker) ● Customized signals
31. 31. HuntingWeaponizationActivities Common Techniques ● Upload malware sample to public scanning service (e.g. VirusTotal) for testing anti-detection. How to hunt? ● With known intelligence, writing Yara rule to hunt on scanning service. ● Monitoring underground with intelligence service. Weaponized https://www.bleepingcomputer.com/news/security/garmin-outage-caused-by-confirmed-wastedlocker-ransomware-attack/
32. 32. VirusTotal ● The "Google" of malware. One of the world's largest malware intelligence services. ○ 2+ Billion malware samples ○ 1 Million files uploaded per day ● Basic and advanced research capabilities. ● Crowdsourced verdicts (basic, free). ● Threat hunting, investigation, relationship analysis (advanced, paid tiers) ● Powerful intelligence tools: YARA, Hunt, Graph. ● Part of Chronicle, Alphabet's cybersecurity company.
33. 33. https://support.virustotal.com/hc/en-us/articles/360002160378-Full-list-of-VirusTotal-Intelligence-tag-modifier
34. 34. Example1:FindingnewmalwarehostedonDrive itw:docs.google.com p:20+ fs:2020-09-01T00:00:00+ first Seen Filters the files to be returned according to the first submission datetime to VirusTotal. positives Filters the files to be returned according to the number of antivirus vendors that detected it upon scanning with VirusTotal. itw Return all those files that have been downloaded from a URL containing the literal provided.
35. 35. Example2:FindingAttackerstestingActivities p:20+ type:peexe subspan:500- pets:2020-09-0500:00:00+ submissions:2+ sources:1 type Type of file. (e.g. pdf, doc..etc) pets Filter PE according to their compilation timestamp. submissions number of times they were submitted to VirusTotal. subspan The difference (in seconds) between the first submission time and the compilation timestamp. source Number of distinct sources that submitted the file to VirusTotal
36. 36. Upload in ~2 mins ~ 7 mins difference Same Submitter 10 times bigger?? https://www.virustotal.com/
37. 37. MalwareAnalysis Importantskillforathreathunter! Why doing malware analysis? ● Understand malware capability to understand the motivation and threat levels. (infostealer? RAT? miner?). ● Extract IoC (indicator of compromise) to hunt in the network environment, track the campaign and attribution. ● Identify malware family to understand attacker's TTPs. (Is this malware only use by Group A? or shared among different groups?) ● Produce detection rules. To hunt in the network and deploy detection.

38. 38. StaticAnalysis Examining any given malware sample without actually running or executing the code. DynamicAnalysis Analysis while running the code in a controlled environment. https://www.amazo n.ca/Practical-Mal ware-Analysis-Han ds-Dissecting/dp/1 593272901 https:// tenor.c om/vie w/pand a-offic e-pisse d-tantr um-ma d-gif-5 14682 5
39. 39. Sample A: 966db7bc4279c82ac613be3aa2df5cd15a185c3365215631edbe68872290541e Sample B: 1c89f3f5e4cd72d87514c33b8d9ec60f3429dd02bad1c27e61af9f55a98153ba CFF Explorer DNSpy Sample A Sample B
40. 40. Hello Penguins!
41. 41. SandboxAnalysis Automatethedynamicanalysis,detectionandhuntingpipeline. ● Execute a program in an instrumented environment and monitor their execution. ● They are increasingly used as the core of automated detection processes. https://www.hybrid-analysis.com/ https://any.run/ https://twitter.com/joe4security https://cuckoosandbox.org/
42. 42. Sample: 1c89f3f5e4cd72d87514c33b8d9ec60f3429dd02bad1c27e61af9f55a98153ba %TEMP%Encryptado.exe ebc58454aa9f614685b72c6b212836ce246549ab119b505e6cd72fa4f256ae99 %WINDIR%InstallDirsvchost.exe ebc58454aa9f614685b72c6b212836ce246549ab119b505e6cd72fa4f256ae DROP Copy DNSLookup http://googleinternals.sytes.net:1177/1234567890.fu nctions 170.238.150.143 :1177
43. 43. Sample: ebc58454aa9f614685b72c6b212836ce246549ab119b505e6cd72fa4f256ae99 Key:HKUs-1-5-21-2626073106-1507677243-2163061170-1000s-1-5-21- 2626073106-1507677243-2163061170-1000softwarextremeratmutex Value: TNev6fVkdvSI6V75BecB REG EXPAND VirusTotal image:Vectors Market
44. 44. WhatisXtremeRAT? Molerats?????????? MiddleEast? https://malpedia.caa d.fkie.fraunhofer.de/ details/win.extreme_ rat https://krebson security.com/t ag/xtreme-rat/
45. 45. IngestOSINTwithCriticalThinking Whatinformationhavewegotsofar? ● Potential attacker from Brazilian IP. ● C&C domain resolved to a Brazilian IP. MoreinformationaboutXtremeRAT. ● Xtreme RAT is a commodity RAT that was first publicly sighted in 2010. ● The RAT is available for free and the source code for it has been leaked. Wedon’thaveenoughinformationforattributioninthiscase!
46. 46. YaraRule What is Yara? ● Tool to assist malware researchers identify and classify malware ● Identify malware in string or binary patterns ● YARA rule = strings + condition ● Useful to catalog threat actors and associated IOCs
47. 47. XTremeRATYara(StringBased) https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat
48. 48. XTremeRATYara(codebased) Bypass! https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat
49. 49. UndergroundForumMonitoring Some attackers (specially crime) are not low-profile ● Recruiting hackers. ● Buying ransomware, malwares, stealers..etc. ● Selling stolen data, accounts. How to hunt? ● 3rd party intelligence. ● Monitoring service. ● Forum crawlers.

50. 50. HoneypotHunting Present opportunity instead of finding needle in haystack ● Honeypot mimics a target for hackers, and uses their intrusion attempts to gain information about attacker's intrusion techniques. ● Honeypot can be a virtual system, a fake database, a fake email address, or a webpage. ● Collects intelligence from monitoring attacker's behaviors in the pot. ○ TTPs ○ IoC ○ What are they most interested?
51. 51. 03 CampaignTracking101 51
52. 52. IsCampaignTrackingUseless??? Purpose High level intelligence could be useless in tactical level. Understand your purpose and use proper intelligence Ingest Without ingest, intelligence report won't be your security assets. Note: Definition of Operation Level & Tactical Level might swap in other materials.
53. 53. CyberSecurityLandscape source:FireEye
54. 54. Attributionisaverydelicatetopic. Itshouldbehandledwithgreatcare!
55. 55. CyberAttributionModel CyberAttackInvestigation ● 3W1H : Who / Why / What / How ● Four Components ○ Victimology / Adversary ○ Infrastructure ○ Capabilities ○ Motivation [1] https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00048-4
56. 56. CyberAttributionModel CyberThreatActorProfiling ● Who could be the perpetrator ● What infrastructure have they used for the attack and What capabilities and motivation might they have. [1] https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00048-4
57. 57. ASolidGroundforStart? OSINT Report Communities Resource Security Conference/Summit Company Online Seminar Incident Response Report IngestInformation AttributionAnchor Attributes that are relatively unique, would be difficult for an adversary to change, and exist across multiple phases of the kill chain.
58. 58. CAMPAIGNTrackingAttributes ● Any intrusion can be modeled into 7 phases (Kill Chain) ● An intrusion can be considered as a highly-dimensional set of indicators, called "attributes" Nowadays, signatures are far from sufficient to detect malicious files Against high-value targets for specific purpose Backdoor C2INFRASTRUCTURE TargetScope EXPLOITTOOL Zero-day exploits are rarer and more expensive than ever Adversaries might use same infrastructure for years
59. 59. Buildagoodattributevector? Malware Customized Hacking tool Uniques Strings Publicly Available Tools Actor Controlled Domain Resolution Watering Hole Compromised IP/Port Combination DNS provider Same Netblock Unique Password Unique Code Snippet Overall Methodology Spear-Phishing Sender Domain Registrant Email Phishing Target Methodology Spear-PhishingEmail Infrastructure
60. 60. MalwareTriage Spyware Virus Trojan Worms Ransomware Bot Adware Rootkit
61. 61. DiveDeepintoInfrastructure [1] https://cybersecurity.springeropen.com/articles/10.1186/s42400-020-00048-4
62. 62. DiveDeepintoMethodology [7] https://medium.com/@jym/a-survey-of-attack-life-cycle-models-8bd04557af72
63. 63. Malware Analysis Monitoring System Incident Response System forensic report for Lateral movement tools, Rootkit, Deleted scripts/ malware/logs ... Information from Firewall, EDR, SIEM, UTM, WAF, or even SOAR... ExpandYourAttributes Malware triage, Operational IoCs, C2 Infrastructure, Modified registries... Honeypot DarkForumTracking C2Tracker Passive Proactive yarahunting

64. 64. CaseStudy:EnterpriseVPNCredentialLeaked [2] https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/
65. 65. * Actor profiling - Ability of intrusion - Purpose & target - TTPs * Victim profiling - Affected industry - Scale of damage - Root cause of the intrusions DataPreprocess Investigation For identify all of the possible victims in the leaked data, information likes IP, domain, organization name, personal credentials are useful. * Separated IPs by GEO-location information. * Separated Domains by WhoIs information. * Back trace routing path. Routing server name might reveal host identity. * Credential Analysis Triage RetrieveIndicator
66. 66. InfrastructureInvestigation What matters? ● Server Type ○ VPS ○ Webhosting server ○ CDN server ○ Compromised site ○ Sinkholed ○ Private server ● Timestamp ○ Resolve timestamp ○ Info update timestamp ● Registrant information ○ Registrant name, organization, address, phone ● Certificate ○ Hash / Serial Number ○ Organization Name ○ Common Name PassiveDNSRecords Passive DNS records can help you to trace back domains which associated to the IP address https://community.riskiq.com/
67. 67. VictimInvestigation PassiveDNSRecords Passive DNS records can help you to trace back domains which associated to the IP address RegistrantInformation Most of the registrant info. might be masked due to GDPR regulation. Information still available for normal company, service provider. [3] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en https://www.nic.ad.jp/ https://community.riskiq.com/
68. 68. VictimInvestigation CertificateInformation SSL certificate serial number, contact name, email, address, ...etc are useful indicators RegistrantInformation Most of the registrant info. might be masked due to GDPR regulation. Information still available for normal company, service provider. PassiveDNSRecords Passive DNS records can help you to trace back domains which associated to the IP address https://community.riskiq.com/
69. 69. VictimInvestigation CertificateInformation SSL certificate serial number, contact name, email, address, ...etc are useful indicators RegistrantInformation Most of the registrant info. might be masked due to GDPR regulation. Information still available for normal company, service provider. PassiveDNSRecords Passive DNS records can help you to trace back domains which associated to the IP address
70. 70. * Malicious EXE file disguised with Doc Icon in June * Use “Hong Kong security law” related issue as lure theme * Lure document is a letter from Vatican ThreatDetected CampaignTrackingCaseStudy * A delicate malware downloader for infecting system by 2nd stage. * The 2nd stage backdoor is a variant of PlugX. * PlugX is a malware widely used by many APT groups. MalwareAnalysis * Abuse Google Drive for deliver compressed malicious files * Use service from CN based service providers * Infrastructure appears in many Mustang Panda related report InfrastructureAnalysis source: any.run sandboxsource: FireEye
71. 71. CampaignTrackingCaseStudy * User ID could be found in many programing forum, blogger, github...etc * From the self-introduction page of the services above, we found the surname overlap. Got you! * Personal CV found in the wild. PossiblePersona * A personal blog domain associated to the C2 infrastructure used for this operation. * Registrant Name: “Ma Ge Bei Luo Xiang Gang Jiu Dian” InterestingOverlap [4] www.xuepojie.com

72. 72. In August, a new sample with Tibet-Ladakh Relationship lure content discovered in the wild... What we learn from tracking? ◂ Get updated anchors for future reference ◂ Understand the whole landscape not separated incidents. ◂ Learning history is helpful in that we can review the past and predict the future. Afterstory... BackwardTracing * Found related sample on google drive from the same account with file title “QUM, IL VATICANO DELL'ISLAM”. * They used Middle East related lure in June as well. Lure Document source: FireEye
73. 73. Loveyou!NicetoSeeyouagain! Source: Virustotal Lure Document / Motivation Tool / Timestamp like XOR Key Infrastructure
74. 74. CampaignTrackingFail? Do you sacrifice the accuracy of your research to opportunistically promote business!
75. 75. ● Source Reliability / Fidelity ● Mixing Fact with Assessment ○ Differentiate KNOW & THINK ○ Public research & Media might not differentiate them ● Failure to Consider Visibility ● Failure to Account for Human Action ● Failure to Consider Alternate Explanations CommonErrors
76. 76. ● Depends too heavily on an initial piece of information offered to make subsequent judgments during decision making. ○ Quick Tweet from Community ○ Similar Exploit Template ○ Same Malware/Hacking Tool from forensic ○ Detect Code Snippet Overlapped ○ Detect C2 Infrastructure Overlapped ● Don’t ignore evidence conflict with your initial vector Decide attribution when you have sufficient evidence ! AnchoringEffect
77. 77. ClassicFalseFlagCampaignCase [5] TechRepublic Feb.2018 (https://www.techrepublic.com/article/pyeongchang-olympic-committee-hacked-during-opening-ceremony-of-2018-winter-games/)
78. 78. CiscoTalos OlympicDestroyer shared same techniques in Badrabbit and NotPetya Intezer They found code in the OlympicDestroyer that connects to known Chinese threat actors. RecordedFuture Found similarities to malware loaders from BlueNoroff/Lazarus.A North Korea based APT group. FalseFlag&Disinformation [6] Securelist Mar. 2018 https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/
79. 79. FalseFlag&Disinformation [6] Securelist Mar. 2018 https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/
80. 80. Lesson? NO Rush with Attribution.
81. 81. AttributionGuide Best Practices for Determining Attribution ● Looking for Human Error ○ Almost all cyber attribution successes have resulted from attackers’ operational security errors ● Timely Collaboration, Information Sharing, and Documentation. ○ Acquisition, documentation, and recovery of data within twenty-four hours of a cyber incident ● Rigorous Analytic Tradecraft ○ Must be careful to avoid cognitive bias [7] A Guide to Cyber Sep. 2018 Attributionhttps://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf
82. 82. AttributionGuide Best Practices for Presenting Attribution Analysis ● De-layer the Judgment ● Provide Confidence Level ○ High: The totality of evidence and context with no reasonable alternative ○ Moderate: The totality of evidence and context to be clear and convincing, with only circumstantial cases for alternatives ○ Low: More than half of the body of evidence points to one thing, but there are significant information gaps ● Identify Gaps ○ Do not have enough data for a judgment or confidence statement

83. 83. AttributionGuide [7] A Guide to Cyber Sep. 2018 Attributionhttps://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf
84. 84. Summary ● Threat Hunting ○ Threat hunting serve different purposes from different roles. ○ Create hypothesis before developing a threat hunting program. ○ Threats do not started from intrusion. Reconnaissance and weaponization stages are also threat hunting's playgrounds. ● Campaign Tracking ○ Decide a solid anchor as reference base for tracking. ○ Attribution is a very delicate topic. It should be handled with great care. ○ Avoid possible cognitive bias and de-layer your Judgment ○ NO rush with attribution.
85. 85. AnyQuestion? AppreciateFor YourJoin HITCON&CTIVillageToday Seeyou...
86. 86. Reference/Resource ◂ Icon material attribution: ◂ Flaticon ◂ smalllikeart ◂ Nhor Phai ◂ Freepik ◂ Xtreme RAT ◂ https://malpedia.caad.fkie.fraunhofer.de/details/win.extreme_rat