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

Archived: 2026-04-05 21:04:11 UTC

- 1.
- 2.

  The views andopinions 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.

  ● 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.

  Agenda ThreatHunting101 What is ThreatHunting? 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.
- 6.
- 7.

  WHATISTHREATHUNTING? Threat hunting isthe 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.
- 9.

  KnowntoSelf NotKnowntoSelf Knowto Others ● Internallydetected 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 ThreatHuntingservesdifferentpurposefordifferentroles. ● Orgs performthreat 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.
- 12.
- 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.

ThreatHuntingDrivers Analytics-Driven ● Aggregated data gatheredfrom 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.
- 16.

ThreatHuntingProcess Investigate the scenarioswith 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.
- 18.
- 19.
- 20.
- 21.
- 22.
- 23.
- 24.
- 25.

Reconnaissance HuntingReconnaissanceActivities In Reconnaissance stageattacker 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.

Hypothesis ● Attackers aredoing 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/puppeteer https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967 https://www.youtube.com/

- 27.

Uncover TTPs ● IPswith 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.

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.
- 30.

Reconnaissance HuntingReconnaissanceActivities 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.

HuntingWeaponizationActivities Common Techniques ● Uploadmalware 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.

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.
- 34.

  Example1:FindingnewmalwarehostedonDrive itw:docs.google.com p:20+ fs:2020-09-01T00:00:00+ firstSeen 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.

  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.

  Upload in ~2mins ~ 7 mins difference Same Submitter 10 times bigger?? https://www.virustotal.com/

- 37.

  MalwareAnalysis Importantskillforathreathunter! Why doing malwareanalysis? ● 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.

  StaticAnalysis Examining any givenmalware 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.
- 40.
- 41.

  SandboxAnalysis Automatethedynamicanalysis,detectionandhuntingpipeline. ● Execute aprogram 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.
- 43.

- 44.
- 45.

IngestOSINTwithCriticalThinking Whatinformationhavewegotsofar? ● Potential attackerfrom 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.

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.
- 48.
- 49.

UndergroundForumMonitoring Some attackers (speciallycrime) 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.

HoneypotHunting Present opportunity insteadof 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.
- 52.

IsCampaignTrackingUseless??? Purpose High level intelligencecould 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.
- 54.
- 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.

CyberAttributionModel CyberThreatActorProfiling ● Who couldbe 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.

  ASolidGroundforStart? OSINT Report Communities Resource SecurityConference/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.

  CAMPAIGNTrackingAttributes ● Any intrusioncan 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.

  Buildagoodattributevector? Malware Customized Hacking tool UniquesStrings 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.
- 61.
- 62.
- 63.

  Malware Analysis Monitoring System Incident Response System forensic reportfor 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.
- 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.

  InfrastructureInvestigation What matters? ● ServerType ○ 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.

  VictimInvestigation PassiveDNSRecords Passive DNS recordscan 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.

  VictimInvestigation CertificateInformation SSL certificate serialnumber, 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.

  VictimInvestigation CertificateInformation SSL certificate serialnumber, 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.

  * Malicious EXEfile 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.

  CampaignTrackingCaseStudy * User IDcould 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.

  In August, anew 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.
- 74.
- 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.

  ● Depends tooheavily 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.
- 78.

  CiscoTalos OlympicDestroyer shared same techniquesin 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.
- 80.
- 81.

  AttributionGuide Best Practices forDetermining 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.

  AttributionGuide Best Practices forPresenting 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.

  AttributionGuide [7] A Guideto Cyber Sep. 2018 Attributionhttps://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf

- 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.
- 86.

  Reference/Resource ◂ Icon materialattribution: ◂ Flaticon ◂ smalllikeart ◂ Nhor Phai ◂ Freepik ◂ Xtreme RAT ◂ https://malpedia.caad.fkie.fraunhofer.de/de tails/win.extreme_rat

---