


Threat Intel Reads – January 2019

 threatintel.eu/2019/02/02/threat-intel-reads-january-2019

andreas.sfakianakis

February 2, 2019

January was an interesting month for CTI practitioners! I took some time and collected the major articles and presentations that I read and watched during January 2019.

I hope you enjoy it.

1. Robert M. Lee – Attribution is not Transitive – Tribune Publishing Cyber Attack as a Case Study – <http://www.robertmlee.org/attribution-is-not-transitive-tribune-publishing-cyber-attack-as-a-case-study/>
2. Politico – Suspect’s Twitter messages played role in NSA hacking-tools leak probe – <https://www.politico.com/story/2018/12/31/nsa-hacking-case-twitter-1077013>
3. Maarten Goet – Windows Defender ATP: harnessing the collective intelligence of the InfoSec community for threat hunting – <https://medium.com/@maarten.goet/windows-defender-atp-harnessing-the-collective-intelligence-of-the-infosec-community-for-threat-1758ec987db8>
4. z3roTrust – The APT Chronicles_December 2018 edition – <https://medium.com/@z3roTrust/the-apt-chronicles-december-2018-edition-e3e5125ffcd2>
5. BBC – German politicians targeted in mass data attack – <https://www.bbc.com/news/world-europe-46757009>
6. ZDNet – NSA to release a free reverse engineering tool – <https://www.zdnet.com/article/nsa-to-release-a-free-reverse-engineering-tool/>
7. Florian Roth – My Take on the Massive Data Leak Affecting German Politicians and Public Figures – <https://medium.com/@cyb3rops/my-take-on-the-massive-data-leak-affecting-german-politicians-and-public-figures-e7ca8d2b2513>
8. Threatpost – First-Ever UEFI Rootkit Tied to Sednit APT – <https://threatpost.com/uefi-rootkit-sednit/140420/>
9. FI-ISAC – TaHiTI – Threat Hunting Methodology – <https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf>
– <https://www.mbsecure.nl/blog/2018/12/tahiti-threat-hunting-methodology>
10. The Register – Cops: German suspect, 20, ‘confessed’ to mass hack of local politicians
https://www.theregister.co.uk/2019/01/08/german_20_yr_old_confess_mass_hack_angriff/
11. Lenny Zeltser – A Short Cybersecurity Writing Course Just for You – <https://zeltser.com/cybersecurity-writing-course/>
12. Reuters – Exclusive: New documents link Huawei to suspected front companies in Iran, Syria – <https://www.reuters.com/article/us-huawei-iran-exclusive/exclusive-new-documents-link-huawei-to-suspected-front-companies-in-iran-syria-idUSKCN1P21MH>
13. Julia Reda – In January, the EU starts running Bug Bounties on Free and Open

- Source Software – <https://juliareda.eu/2018/12/eu-fossa-bug-bounties/>
14. Politico – Exclusive: How a Russian firm helped catch an alleged NSA data thief – <https://www.politico.com/story/2019/01/09/russia-kaspersky-lab-nsa-cybersecurity-1089131>
 15. FireEye – Global DNS Hijacking Campaign: DNS Record Manipulation at Scale – <https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html>
 16. WSJ – America’s Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It – <https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112>
 17. SG Government – PUBLIC REPORT OF THE COMMITTEE OF INQUIRY INTO THE CYBER ATTACK ON SINGAPORE HEALTH SERVICES PRIVATE LIMITED’S PATIENT DATABASE ON OR AROUND 27 JUNE 2018 – <https://www.mci.gov.sg/~media/mcicorp/doc/report%20of%20the%20coi%20into%20the%20cyber%20attack%20on%20singhealth%2010%20jan%202019.pdf?la=en>
 18. Cyberwarcon – Are US Cyber Deterrence Operations Suppressing or Inciting Attacks? – <https://www.youtube.com/watch?v=cp0rjgEpWEw>
 19. Hackmageddon – 2018: A Year of Cyber Attacks – <https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/>
 20. bit_of_hex – ATT&CKing the Singapore Health Data Breach – <https://bitofhex.com/2019/01/13/attack-and-singapore-breach/>
 21. CERT-OPMD – DNSPIONAGE – Focus on internal actions – <https://blog-cert.opmd.fr/dnspionage-focus-on-internal-actions/>
 22. CrowdStrike – Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware – <https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/>
 23. New York Times – Poland Arrests 2, Including Huawei Employee, Accused of Spying for China – <https://www.nytimes.com/2019/01/11/world/europe/poland-china-huawei-spy.html>
 24. The Register – Cyber-insurance shock: Zurich refuses to foot NotPetya ransomware clean-up bill – and claims it’s ‘an act of war’ – https://www.theregister.co.uk/2019/01/11/notpetya_insurance_claim/
 25. Cyberscoop – How sloppy OPSEC gave researchers an inside look at the exploit industry – <https://www.cyberscoop.com/mobile-zero-days-lookout-shmoocon-2019-android-barracuda-ios-stonefish/>
 26. Recorded Future – The History of Ashiyane: Iran’s First Security Forum – <https://www.recordedfuture.com/ashiyane-forum-history/>
 27. US DoJ – Two Ukrainian Nationals Indicted in Computer Hacking and Securities Fraud Scheme Targeting U.S. Securities and Exchange Commission – <https://www.justice.gov/opa/pr/two-ukrainian-nationals-indicted-computer-hacking-and-securities-fraud-scheme-targeting-us>
 28. EU ATT&CK community – third workshop – 9-10 May 2019 – <https://www.attack-community.org/2019-01-15-Third-Workshop-At-Eurocontrol-Brussels/>
 29. Nextron Systems – 50 Shades of YARA – <https://www.nextron-systems.com/2019/01/02/50-shades-of-yara/>

30. Alex Jäger – Autotimeliner to CyberChef to Timesketch – <https://www.alexanderjaeger.de/autotimeliner-to-cyberchef-to-timesketch/>
31. Cyberscoop – Trisis investigator says Saudi plant outage could have been prevented – <https://www.cyberscoop.com/trisis-investigator-saudi-aramco-schneider-electric-s4x19/>
32. ENISA – Analysis of the European R&D priorities in cybersecurity – <https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity>
33. Flashpoint – Why Executive-Protection Teams Need Finished Intelligence – <https://www.flashpoint-intel.com/blog/why-executive-protection-teams-need-finished-intelligence/>
34. WEF – The Global Risks Report 2019 – <https://www.weforum.org/reports/the-global-risks-report-2019/>
35. Christian Haschek – The curious case of the Raspberry Pi in the network closet – <https://blog.haschek.at/2018/the-curious-case-of-the-RasPi-in-our-network.html>
36. CERT.PL – MWDB – our way to share information about malicious software – <https://www.cert.pl/en/news/single/mwdb-our-way-to-share-information-about-malicious-software/>
37. ENISA – Supporting the Fight Against Cybercrime: ENISA report on CSIRTs and Law Enforcement Cooperation – <https://www.enisa.europa.eu/news/enisa-news/supporting-the-fight-against-cybercrime-enisa-report-on-csirts-and-law-enforcement-cooperation>
38. Bleeping Computer – DarkHydrus APT Uses Google Drive to Send Commands to RogueRobin Trojan – <https://www.bleepingcomputer.com/news/security/darkhydrus-apt-uses-google-drive-to-send-commands-to-roguerobin-trojan/>
39. MITRE's ATT&CK – Part 1: Would a Detection by Any Other Name Detect as Well? – <https://medium.com/mitre-attack/would-a-detection-by-any-other-name-detect-as-well-part-1-1577eba255bc>
40. Lenny Zeltser – How can a single report appeal to both executives and technologists? – <https://www.linkedin.com/pulse/how-can-single-report-appeal-both-executives-lenny-zeltser/>
41. Measured Response – Threat Modeling – <https://measuredresponse.org/threat-modeling>
42. Cyberscoop – DHS releases emergency order to prevent DNS hijacking – <https://www.cyberscoop.com/dhs-dns-directive-government-shutdown/>
43. DHS – Emergency Directive 19-01 – <https://cyber.dhs.gov/ed/19-01/>
44. Microsoft – Contextualizing Attacker Activity within Sessions in Exchange Online – <https://blogs.technet.microsoft.com/exchange/2019/01/04/contextualizing-attacker-activity-within-sessions-in-exchange-online/>
45. ZDNet – Zerodium will now pay \$2 million for Apple iOS remote jailbreaks – <https://www.zdnet.com/article/zerodium-will-now-pay-2-million-for-apple-ios-remote-jailbreaks/>
46. WSJ – Inside Google's Team Fighting to Keep Your Data Safe From Hackers – <https://www.wsj.com/articles/inside-googles-team-battling-hackers-11548264655>
47. TrustedSec – Learn the basics of post-exploitation from advanced infosec

- professionals – <https://www.trustedsec.com/2018/12/webinar-series-post-exploitation/>
48. Lenny Zeltser – Write a Strong Executive Summary for Your Security Assessment Report – <https://zeltser.com/executive-summary-for-security-assessment-report-tips/>
 49. Lukasz Olejnik – The French doctrine of offensive cyber operations – <https://blog.lukaszolejnik.com/the-french-doctrine-of-offensive-cyber-operations/>
 50. 360 – Global Advanced Persistent Threat (APT) 2018 Summary Report – <https://www.freebuf.com/articles/paper/193553.html>
 51. Dark Reading – Triton/Trisis Attack Was More Widespread Than Publicly Known – <https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661>
 52. The Intercept – Intellipedia BIOS Threats – <https://theintercept.com/document/2019/01/24/intellipedia-bios-threats/>
 53. NCSC-UK – ALERT: DNS hijacking activity – <https://www.ncsc.gov.uk/alerts/alert-dns-hijacking-activity>
 54. MITRE's ATT&CK – Part 2: Would a Detection by Any Other Name Detect as Well? – <https://medium.com/mitre-attack/would-a-detection-by-any-other-name-detect-as-well-part-2-2b2cf9180e21>
 55. Daily Beast – This Time It's Russia's Emails Getting Leaked – <https://www.thedailybeast.com/this-time-its-russias-emails-getting-leaked>
 56. Kaspersky – GreyEnergy's overlap with Zebrocy – <https://securelist.com/greyenergys-overlap-with-zebrocy/89506/>
 57. Cyberwarcon – Barely whispering – <https://www.youtube.com/watch?v=h8pTjIMxsag>
 58. The Citizen Lab – Statement from Citizen Lab Director on attempted operations against researchers – <https://citizenlab.ca/2019/01/statement-from-citizen-lab-director-on-attempted-operations-against-researchers/>
 59. Steve Micallef – OSINT and the new perimeter – <https://medium.com/@micallst/osint-and-the-new-perimeter-20d19361e18>
 60. Rappler – Russian disinformation system influences PH social media – <https://www.rappler.com/newsbreak/investigative/221470-russian-disinformation-system-influences-philippine-social-media>
 61. ENISA – ENISA Threat Landscape Report 2018 – <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018>
 62. Huawei indictment – <https://assets.bwbx.io/documents/users/iqjWHBFdfxIU/rIz2tT7h2.Fs/v0>
 63. Virus Bulletin – Threat intelligence teams should consider recruiting journalists – <https://www.virusbulletin.com/blog/2019/01/threat-intelligence-teams-should-consider-recruiting-journalists/>
 64. DNI – Threat Assessment of the US Intelligence Community – <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1947-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community>
 65. EclecticiQ – On the Importance of Standard Operating Procedures in Threat Intelligence – <https://blog.eclecticiq.com/on-the-importance-of-standard->

operating-procedures-in-threat-intelligence

66. ENISA – ENISA publishes training course material on network forensics for cybersecurity specialists – <https://www.enisa.europa.eu/news/enisa-news/enisa-publishes-training-course-material-on-network-forensics-for-cybersecurity-specialists>
67. Reuters – The Karma Hack: UAE used cyber super-weapon to spy on iPhones of foes – <https://www.reuters.com/investigates/special-report/usa-spying-karma/>
68. Reuters – Project Raven : Inside the UAE’s secret hacking team of American mercenaries- <https://www.reuters.com/investigates/special-report/usa-spying-raven/>
69. SANS – SANS CTI Summit Presentations – <https://www.sans.org/cyber-security-summit/archives/>
70. Red Canary – Five Great Talks from the SANS CTI Summit – <https://www.redcanary.com/blog/five-great-talks-from-the-sans-cti-summit/>
71. Splunk – Datamodel Endpoint – <https://www.splunk.com/blog/2019/01/17/-datamodel-endpoint.html>
72. Dragos – Uncovering ICS Threat Activity Groups
– <https://dragos.com/blog/industry-news/webinar-summary-uncovering-ics-threat-activity-groups/>
– <https://www.youtube.com/watch?v=23cRqcKWpTI>
73. Dale Peterson – Post Game Analysis: S4 ICS Detection Challenge – <https://dale-peterson.com/2019/01/31/post-game-analysis-s4-ics-detection-challenge/>
74. Dirk-jan Mollema – Abusing Exchange: One API call away from Domain Admin – <https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/>
75. FireEye – State of the Hack: NoEasyBreach REVISITED – <https://www.pscp.tv/w/1BdGYOMvYBDxX>