

1 person clipped this slide

Clip slide

# OSINT x UCCU

## Open Source Intelligence

• miasoski @ UCCU •

◀ 1 of 72 ▶



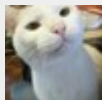
# OSINT x UCCU Workshop on Open Source Intelligence

248 views

Share

Like

Download



[Philippe Lin](#), Senior Threat Researcher at Trend Micro

[+ Follow](#)

in

f

🐦

Published on Nov 17, 2017

OSINT is a reconnaissance of intelligence from publicly available information

...

Published in: [Software](#)

License: [CC Attribution License](#)



1 Comment



2 Likes



Statistics



Notes



Share your thoughts...

Post










[Mohammed Azam M.](#), Network Security Specialist & JoB L00king at UAE

nice share

3 months ago

# OSINT x UCCU Workshop on Open Source Intelligence

1. OSINT x UCCU Open Source Intelligence miasoski @ UCCU 2017.11.18
2. miasoski • Senior threat researcher in Trend Micro • Threat intelligence • Smart City • SDR • Arduino, RPi, embedded
3. Outline • Module 1: What is OSINT? • Module 2: Using Search Engine • Module 3: Social Media Profiling • Module 4: Domain / IP Profiling 3
4. References 林豐裕、李鎮宇、黃健誠、張佩嫻 編譯 4/e Michael Bazzell 5/e <https://inteltechniques.com/menu.html>
5. Disclaimer 1. Sponsored by UCCU + ITRI 2. Respect privacy and laws 3. Make sure you know what you're doing 4. Be responsible
6. Before we start • Download VirtualBox • Download Tails or Buscador • <https://inteltechniques.com/buscador/index.html> • <https://tails.boum.org/>
7. Module 1 What is OSINT?
8. What is OSINT? • 主體是人 • Reconnaissance of intelligence • From publicly available information • To address a specific intelligence requirement  
• Newspaper, blog, search engine ... • Government documents • Often undervalued though significant
9. Why OSINT? • New employee • Criminal investigation • Missing children / Runaway children • Human trafficking • Vandalism • Stealing • NOT to manhunt or SJW on Dcard / PTT / ... 肉搜請洽 lionbug 正義魔人可以去 [reddit.com/r/rbi](https://www.reddit.com/r/rbi) Dcard 請洽 lionbug
10. OSINT Includes but Not Limited to • Location • Real Name • Online ID / group / community • Phone number • Email • Credit card number / Bank account • Date / Time • Documents • Domain / IP address • URL
11. Example: Android Malware
12. Example: Keylogger
13. Example: from a Mutex • Mutex: awdaw2214a • ayool2day[.]biz • born in 1984 • Lives in KL • ma2dayzs[.]com (domain)  
<http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/staying-safe-from-irs-scammers-tax-fraud>
14. Protect Yourself! (1) • Firefox plugins • LiveUSB • VM • Buscador • Tails • VPN and/or Tor • PIA • NordVPN • Hola!VPN
15. Protect Yourself! (2) • New email • New Facebook account • New Twitter • New cell phone • New laptop
16. Firefox (1)
17. Firefox (2) Not in Firefox 57: • Copy all links • Search Image Anywhere • NoScript Manual install: • YouTube downloader • wget
18. Module 2 Search Engines
19. In this Module ... • Google dorks • Email recon (X) • Middle name (X) • Education • Genealogy • Real estate or rent-a-car • Tax records
20. Google Dorks (1) • "someone@gmail.com" • site:ntu.edu.tw "Some Document" • Cisco filetype:pptx • bazzell -fbi -osint -amazon -books -intelligence • inurl:ftp -inurl:(http|https) filetype:pdf osint • intitle:osint • "osint \* training" • "osint \* training" "2015..2017" • ext:pdf trendmicro
21. Google Dorks (2) • [https://www.google.com.tw/search?q=osint+tools&tbs=cdr:1,cd\\_min:1/1/0](https://www.google.com.tw/search?q=osint+tools&tbs=cdr:1,cd_min:1/1/0) • <https://www.google.com/inputtools/try/> • Google image reverse search
22. Google Dorks (3) • site:newspaperarchive.com "this archive is hosted by" • [google.com/search?q=nsa&tbs=nws&tbs=nrt:b](https://www.google.com/search?q=nsa&tbs=nws&tbs=nrt:b)
23. Bing / Yandex • linkfromdomain:trendmicro.com • contains:ppt site:trendmicro.com

24. Cache • Google • Bing • Yandex • Baidu • Archive.is • Coralcdn.org (?) • Archive.org
25. Other Search Engines • duckduckgo • keywordtool.io • carrot2.org • millionshort.com • globalfilesearch.com • mmnt.ru (?)   
<https://inteltechniques.com/menu.html>
26. Phone / Name • opencnam.com • Calleridservice è Free API key • next caller è Need to contact sales • Truecaller è like Whoscall  • Spokeo • Genealogy
27. Exercise • Google First! Donald J Trump Jr. • 1977.12.31 (Wikipedia) • Tips: Need phone numbers to exercise? Search backpage or craigslist.  
11/17/17 32
28. Example – Spokeo ß Birth place
29. Example – Pipl • (Optional) Register for API trial key
30. Example – Ancestry • www.ancestry.com è 14-day free trial
31. Example – True People • Family Tree Now (?) • True People (X)
32. Example – ZabaSearch
33. Example – Others WPNumbers Quanki
34. Example – Make a Table (212) 421-7136 (561) 835-9470 Donald Trump 1110 S Ocean Blvd, Palm Beach FL. (864) 292-9070 David Hanna 109 E 50th St NY 10022 IP Address 208.99.198.79 David I Hanna (916) 920-4631 Teresa Blake Scrm North, CA Teresa A Blake (954) 684-9492 Hanh Pham DonaldTrump 1211 White Stone Way, Davie FL. IP Address 134.170.109.165 (916) 920-4631 might have nothing to do with Donald J Trump Jr. Visit zillow.com for real-estate
35. Tea Time     
36. Module 3 Social Media Profiling
37. Social Media • Facebook • Instagram • VK • Twitter • Dating • OkCupid / Match / Plenty Of Fish / eHarmony / Ashley Madison • 中國特色 • 人人 / QQ / 淘寶 / 微博 / 陌陌
38. Create New Accounts 1. KeePassX 2. Email account #1 è Google 3. Email account #2 ProtonMail 4. Phone è TextNow, Google Hangout 5. Twitter\* 6. Instagram 7. Facebook\*\* \*Don't associate with a phone number. \*\* Virgin account is not as precious.
39. Facebook ...
40. Facebook Dorks • <https://inteltechniques.com/menu.html> • users-named • pages-named/employees/present • users-born • Location • Likes • Education • Search by email • Search by phone number\* • It doesn't tell what's not public anymore L
41. Facebook Graph API • Before you start – Use yourself as the target • Use or switch to English (US) • <https://inteltechniques.com/menu.html> • Get userid • Populate all • Check all the details
42. Twitter • [twitter.com/search-advanced](https://twitter.com/search-advanced) • [twitter.com/#!/who\\_to\\_follow](https://twitter.com/#!/who_to_follow) • Twitter Deck • [moz.com/followerwonk/bio](https://moz.com/followerwonk/bio) • [ctrlq.org/first/](https://ctrlq.org/first/) • [sleepingtime.org](https://sleepingtime.org) • [twiscy.com](https://twiscy.com) • Google Dork è [site:twitter.com/username](https://www.google.com/search?q=site:twitter.com/username) • Last 2 digits of cellphone !!!

43. Twitter – GPS • tweetpaths.com • mapd.com/demos/tweetmap • <https://twitter.com/search?q=geocode%3A25.0220839%2C121.5471991%2C2km&src=typd> • <https://pbs.twimg.com/media/DOW91xRW0AAEjSO.jp> g:orig
44. Twitter – Ecosystem • fakers.statuspeople.com • trendsmap.com • twitonomy.com • mentionmapp.com
45. Instagram • 4K Stogram or DownloadGram • Strips EXIF data • Facebook / Instagram / Twitter strip EXIF data. • Not much we can do L
46. Tools and Sites • social-searcher.com • del.icio.us • Flickr map search • mypicsmap.com • www.topix.com/pick-local • craigslist.org 11/17/17 51
47. "Add Friend" Does Not Help You • Don't believe in "Add Friend" and cancel. Facebook has removed the feature.
48. Module 4 Domain / IP Profiling
49. Common Sites • Whois • viewdns.info • VirusTotal • PassiveTotal (RiskIQ) • MaxMind GeoIP2 • Bing IP • sameid.net • NerdyData
50. Whois • Again, check <https://inteltechniques.com/menu.html> • whois swiftco.net / host DOMAIN / host IP
51. Historical Whois Data Registrant Name: Henry Goss Registrant Organization: swift communications Registrant Street: 2001 6th avenue Suite #3020 Registrant City: Seattle Registrant State/Province: WA Registrant Postal Code: 98121 Registrant Country: US Registrant Phone: +2067282736 DomainTools or DomainHistory.net
52. Reverse Whois • viewdns.info or DomainTools
53. Historical IP of 216.9.6.248 Domain Last Resolved Date aerospacetacomapierce.com 2017-11-05 aerospacetacomapierce.org 2017-11-10 aniota.com 2017-11-05 becomenala.com 2017-11-05 cannonconstructioninc.com 2017-11-05 capitolhillarts.org 2017-11-10
54. Lookup Domain from IP Domain Last Resolved Date chrisandhyeyoung.com 2016-02-01 lordofthepipe.com 2016-02-01 swiftco.org 2017-11-10 traffictrader.net 2017-11-06 City: Seattle Zip Code: 98138 Region Code: WA Region Name: Washington Country Code: US Country Name: United States Latitude: 47.6062 Longitude: -122.332 Just like GeoIP, not accurate
55. Spyonweb + DomainTools 11/17/17 61
56. Censys + Shodan Basic Information OS Unix Network 25700 - SWIFT VENTURES Inc (US) Routing 204.13.167.0/24 via AS7922 , AS11404 , AS18530 , AS18530 , AS25700
57. VirusTotal
58. VirusTotal – Subdomains \$ curl -s 'https://www.virustotal.com/ui/domains/swiftco.net/subdomains?limit=10' | grep self | awk -F/ '{print \$6}' | awk -F¥ '{print \$1}' rwhois.swiftco.net mail.swiftco.net kb.swiftco.net vh2.swiftco.net tim.swiftco.net support.swiftco.net prvtrc.swiftco.net klaus.vh.swiftco.net games.swiftco.net blog.swiftco.net swiftco.net
59. PassiveTotal (RiskIQ) 65
60. GeoIP2 • <https://www.maxmind.com/ja/geoip-demo>
61. DomainTools (Not Free) (1)
62. DomainTools (Not Free) (2)
63. Miscellaneous

64. Miscellaneous Tools • nsfwyoutube.com • anonymousmail.me • Social Traffic on IntelTechniques • karmadecay.com • wogle.net
65. Epilogue • API will change • Paywall will be built • Webpage will disappear • Not covered ... • Radio monitoring • Localization • Government documents • DMV data • Reverse video searching • Etc.
66. Be Responsible! Contact: @miaooski

## Recommended



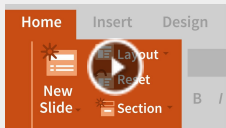
### Blackboard 9.x Essential Training: Instructors

Online Course - LinkedIn Learning



### PowerPoint 2016: Tips and Tricks

Online Course - LinkedIn Learning



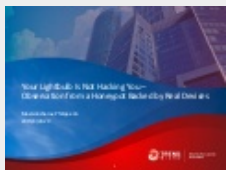
### PowerPoint 2016 Essential Training

Online Course - LinkedIn Learning



### 33C3: Code BROWN in the Air

Philippe Lin



### HITCON 2015: Your Lightbulb Is Not Hacking You: Observation from a Honeypot B...

Philippe Lin

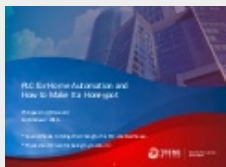
### HITCON 2015 - Building Automation and Control: Hacking Subsidized Energy Savi...

Philippe Lin



## PLC for Home Automation and How to Make It a Honeypot

Philippe Lin



## 基於機器學習的惡意軟體分類實作：Microsoft Malware Classification Challenge 經驗談

Philippe Lin



## AI and Machine Learning Demystified by Carol Smith at Midwest UX 2017

Carol Smith



## The AI Rush

Jean-Baptiste Dumont

[English](#) [Español](#) [Português](#) [Français](#) [Deutsch](#)  
[About](#) [Dev & API](#) [Blog](#) [Terms](#) [Privacy](#) [Copyright](#) [Support](#)



