Open Web Application Security Project

Red Teaming – OSINT – Phishing

Miltiadis Kandias, Phd

Red Team Analyst – Fortune 500 Company

Outline

- Narcissistic Self-Reference
- Red Teaming
- OSINT
- Phishing

Narcissistic Self-Reference

- PhD, “Insider Threat Prediction via Psychosocial Characteristics Extracted by Applying Security Data Science Techniques on OSN OSINT”, Athens University of Economics and Business
- Training in Counseling and Psychotherapy
- Red Team Analyst, focusing on OSINT, Social Engineering, Post-Exploitation, Physical
- Also interested in D&D, stand up comedy, science, philosophy

https://twitter.com/_Zaknafein_

https://www.linkedin.com/in/kandiasm/

Red Team Definition

- Independently led team of diversely skilled people, with different backgrounds, experiences, opinions and ways at looking at problems.
- Humble in nature, co-operative, focused, disciplined and persistent enough to efficiently and effectively emulate the activities and thought processes of real world adversaries.
- Goal is to aid company in understanding what it is doing well, and where it has gaps and improvement opportunities across protect, monitor, and response.
- Help understand/predict likelihood of successful attack, and aid risk decision making. Red Teaming is threat centric, not vulnerability centric like many other forms of security assessment tend to be.

Definition from Dale Pearson's presentation "Building and Leading Corporate Red Teams" at 2018 x33fCon, available at: https://www.slideshare.net/dalepearson/building-and-leading-corporate-red-teams
Also take a look at: http://www.subliminalhacking.net/2016/02/26/corporate-red-teaming-to-me/

Threat Centric Perspective

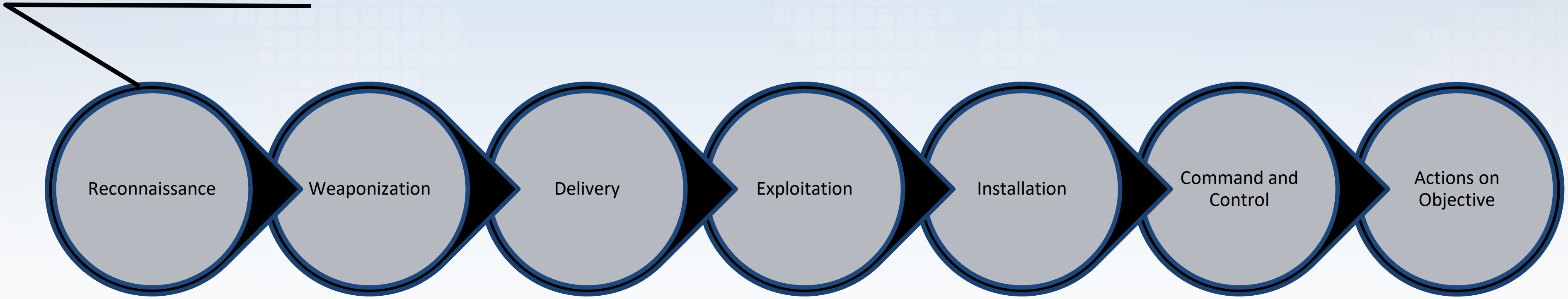
- Red Team should challenge ways of thinking, perceptions, assumptions, validate strengths, and identify weaknesses.
- Focus on organisation’s ability to detect, monitor and respond effectively.
- Different and **NOT** better than other approaches.
- Findings relate to attack paths and could be anything from vulnerabilities to usage of internal tools.
- Might find known issues, but update their impact.
- Emulate the bad guys, go after crown jewels, learn, help fix, wash, rinse, repeat.

Red Team Execution Process

1. Define objectives based on risk appetite, intelligence, and business parameters
2. Get what is needed from the client (i.e. breach points, info, targets etc.)
3. Get your attack infrastructure ready
4. Gather OSINT about your target
5. Deploy your phishing, physical, external attacks
6. Move on with breach simulation
7. Go after objectives. Internal recon, persistence, lateral movement, and privilege escalation may help
8. Report in a way that helps fixing stuff
9. Support remediation, verify fixes

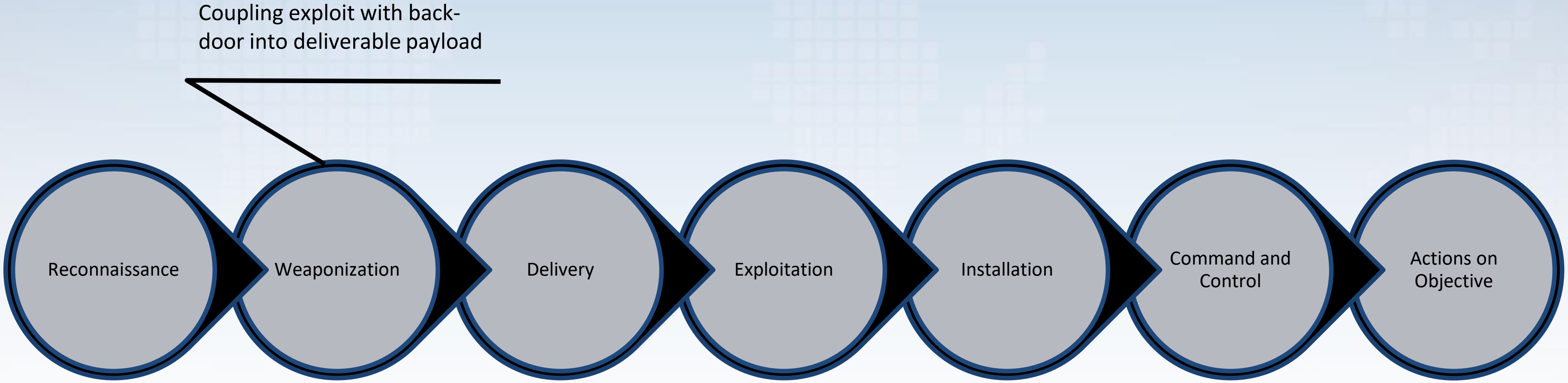
Cyber Kill Chain [1]

Harvesting email addresses, conference information, etc.



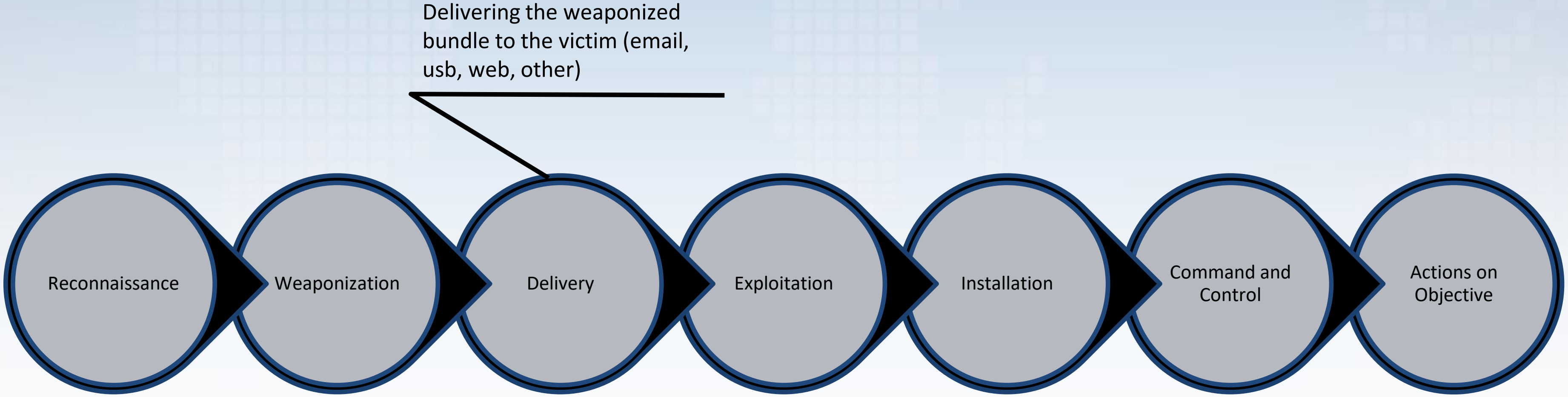
[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Cyber Kill Chain [1]



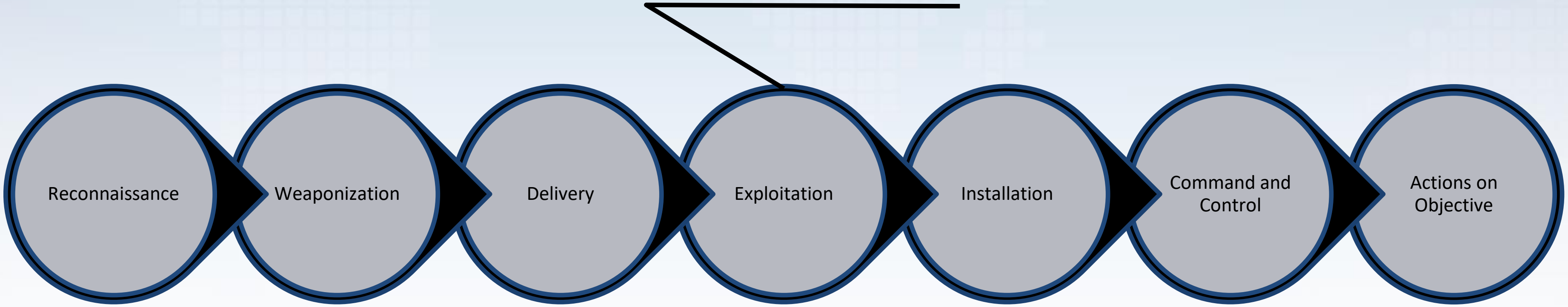
[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Cyber Kill Chain [1]



[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

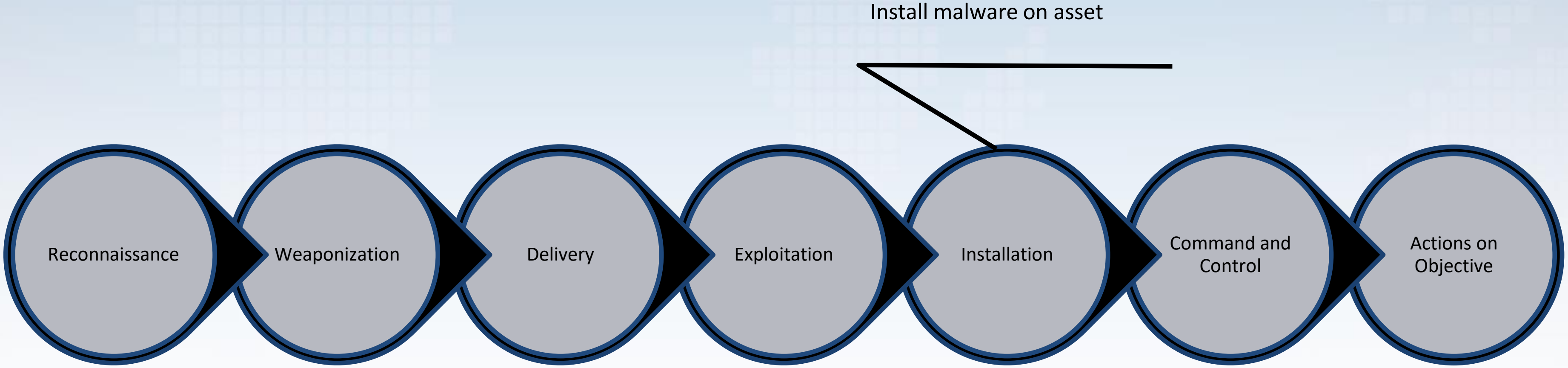
Cyber Kill Chain [1]



Exploiting a vulnerability to execute code on victim's system

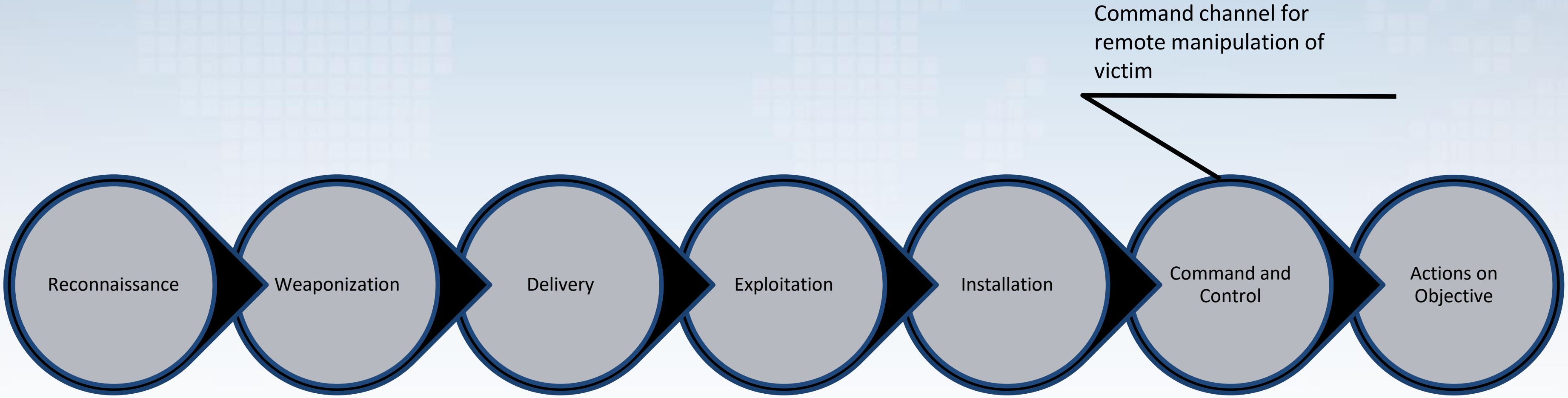
[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Cyber Kill Chain [1]



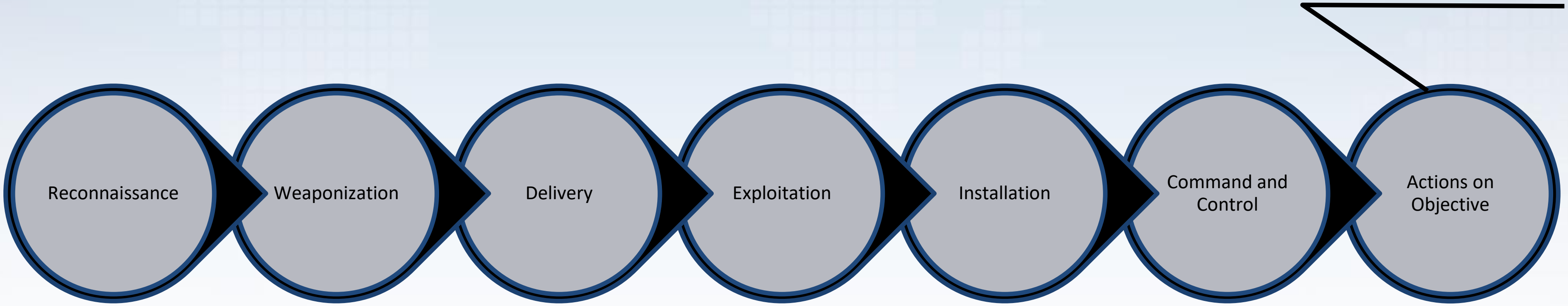
[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Cyber Kill Chain [1]



[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Cyber Kill Chain [1]



[1]. Lokheed Martin, 2015. Gaining the Advantage: Applying Cyber Kill Chain® Methodology to Network Defense. URL: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

OSINT [2]

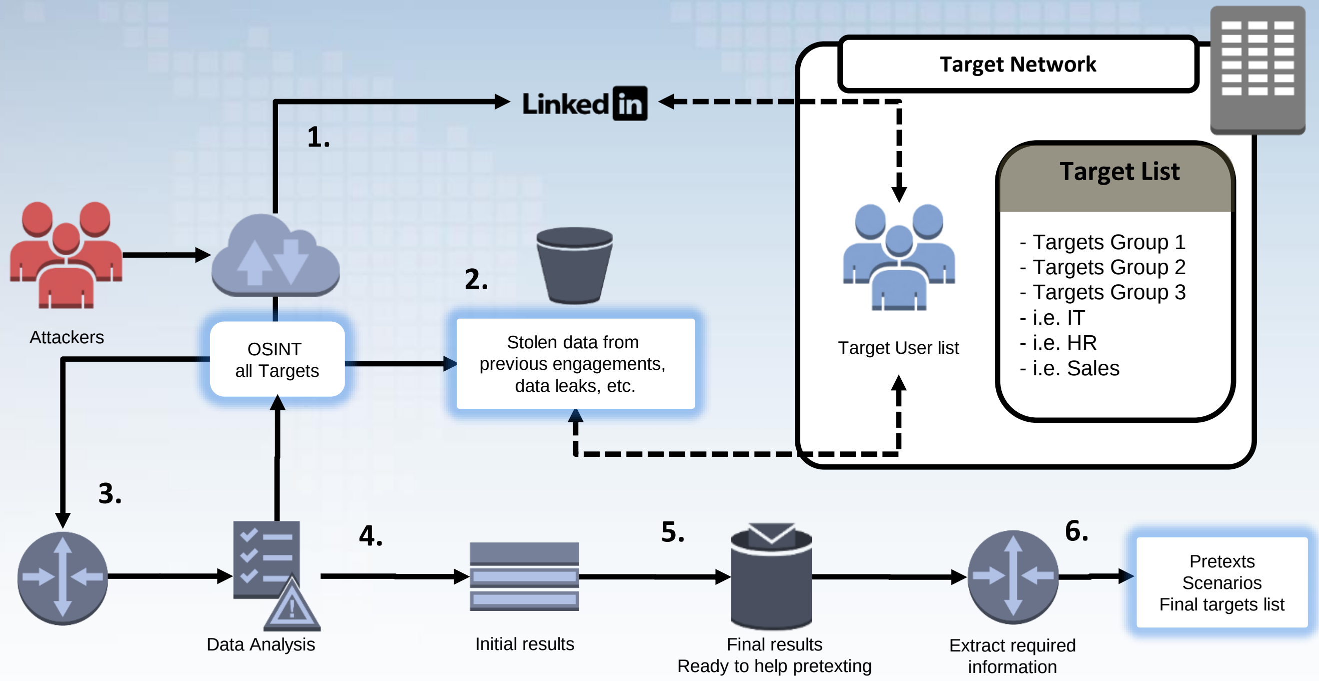
- Open Source Intelligence is produced from publicly available information, which is:
  - collected, exploited and disseminated in a timely manner,
  - offered to an appropriate audience and
  - used for the purpose of addressing a specific intelligence requirement**.**
- Publicly available information refers to (not only):
  - traditional media (e.g. television, newspapers, radio),
  - web-based communities (e.g. social networking sites, blogs),
  - public data (e.g. government reports, official data, hearings) and
  - amateur observation and reporting (e.g. amateur spotters, radio monitors).

[2]. Congress, U.S., 2006. Public Law 109-163, Sec. 931,National Defense Authorization Act for Fiscal Year 2006. URL: http://uscode.house.gov/statutes/pl/109/163.pdf

Generic Approach

- Define your target, what are you after? (in our case creating pretexts for targets)
- Create initial set of sources (search engines, social media, other sources)
- Gather data
- Data cleanup and analysis, extract correlations, extract results
- Wash, rinse, repeat according to limitations
- Respect privacy, legislation, ethical boundaries

OSINT Process



Description

1. Conduct multiple queries on LinkedIn to detect presence in the medium.

2. Update the search capabilities and the depth/breadth of the searches utilising data from previous engagements.

3. Gather a pool of targets and start gathering further OSINT.

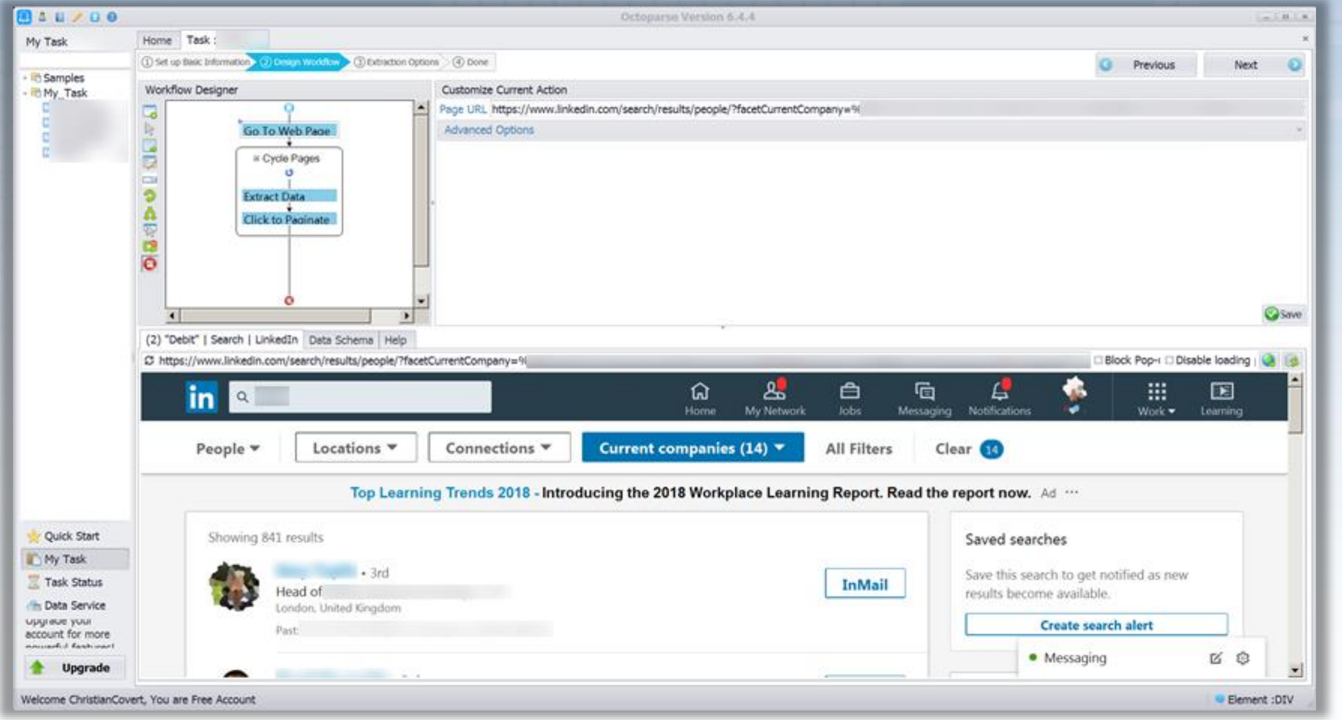
4. Analyse the results and update the OSINT gathering process. In every iteration, more and more precise searches conducted, resulting in less but more focused list of targets.

5. Manually analyse all gathered profiles, roles, descriptions, and related data. End up with a more focused list of targets and finalised data able to help with pretexting.

6. Take final decisions on targets, pretexts, and form scenarios.

OWASP
Open Web Application
Security Project

Examples



Page URL https://www.linkedin.com/search/results/people/?facetCurrentCompany=%

https://www.linkedin.com/search/results/people/?facetCurrentCompany=%

Top Learning Trends 2018 - Introducing the 2018 Workplace Learning Report. Read the report now. Ad ···

Showing 841 results

• 3rd

Head of

London, United Kingdom

Past:

Save this search to get notified as new results become available.

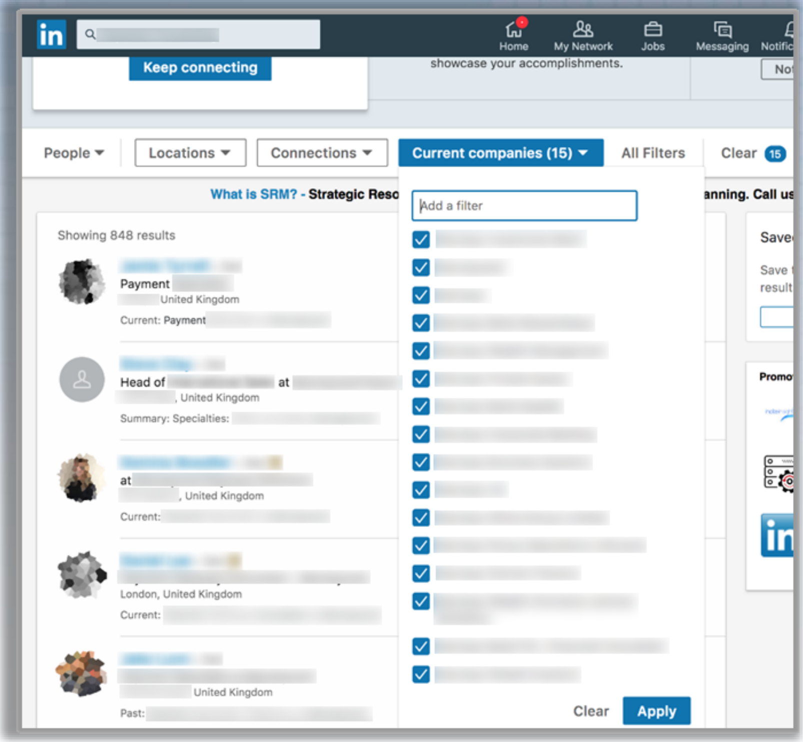
Upgrade your account for more powerful features!

Welcome ChristianCovert, You are Free Account

OWASP

Open Web Application Security Project

Examples



showcase your accomplishments.

People ▾ | Locations ▾ | Connections ▾ | Current companies (15) ▾ | All Filters | Clear 15

What is SRM? - Strategic Reso [redacted] anning. Call us

Showing 848 results

[redacted]
Payment [redacted]
[redacted] United Kingdom
Current: Payment [redacted]

[redacted]
Head of [redacted] at [redacted]
[redacted], United Kingdom
Summary: Specialties: [redacted]

[redacted]
at [redacted]
[redacted], United Kingdom
Current: [redacted]

[redacted]
[redacted]
London, United Kingdom
Current: [redacted]

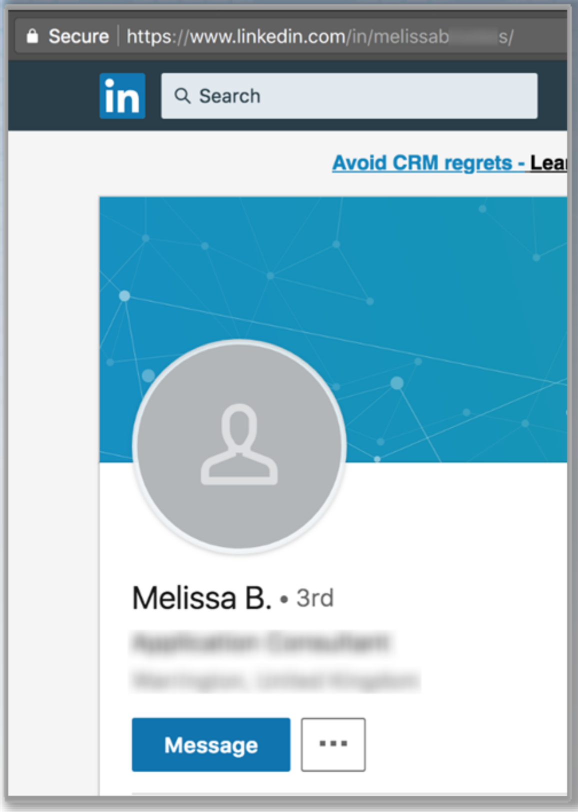
[redacted]
[redacted]
[redacted] United Kingdom
Past: [redacted]

Add a filter

☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]
☑ [redacted]

Clear | Apply

Save
Save t
result


Secure | https://www.linkedin.com/in/melissab[redacted]s/

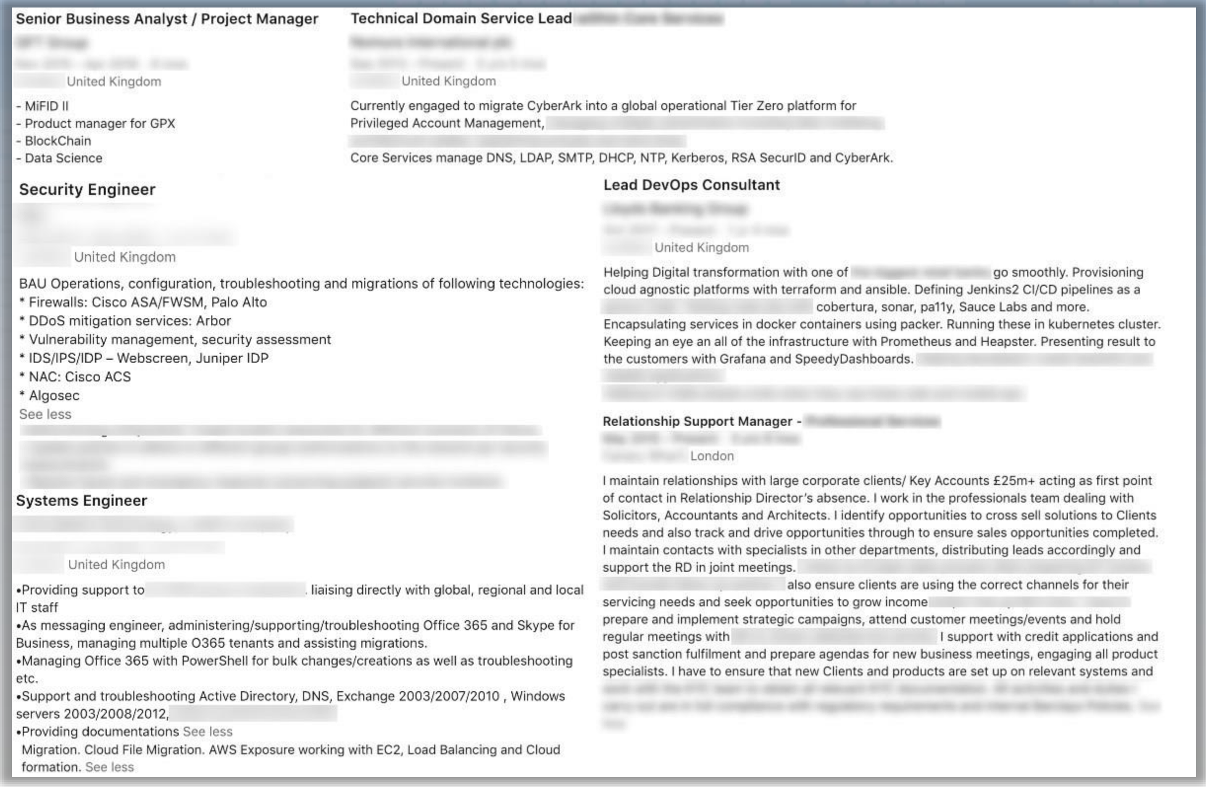
Avoid CRM regrets - Lea

Melissa B. • 3rd

[redacted]

[redacted]

Examples



Senior Business Analyst / Project Manager

[redacted]

[redacted] United Kingdom

- MiFID II
- Product manager for GPX
- BlockChain
- Data Science

Technical Domain Service Lead [redacted]

[redacted]

[redacted] United Kingdom

Currently engaged to migrate CyberArk into a global operational Tier Zero platform for Privileged Account Management, [redacted]

Core Services manage DNS, LDAP, SMTP, DHCP, NTP, Kerberos, RSA SecurID and CyberArk.

Security Engineer

[redacted]

[redacted] United Kingdom

BAU Operations, configuration, troubleshooting and migrations of following technologies:
* Firewalls: Cisco ASA/FWSM, Palo Alto
* DDoS mitigation services: Arbor
* Vulnerability management, security assessment
* IDS/IPS/IDP – Webscreen, Juniper IDP
* NAC: Cisco ACS
* Algosec
See less

[redacted]

Systems Engineer

[redacted]

[redacted] United Kingdom

•Providing support to [redacted]. liaising directly with global, regional and local IT staff
•As messaging engineer, administering/supporting/troubleshooting Office 365 and Skype for Business, managing multiple O365 tenants and assisting migrations.
•Managing Office 365 with PowerShell for bulk changes/creations as well as troubleshooting etc.
•Support and troubleshooting Active Directory, DNS, Exchange 2003/2007/2010 , Windows servers 2003/2008/2012, [redacted]
•Providing documentations See less

Migration. Cloud File Migration. AWS Exposure working with EC2, Load Balancing and Cloud formation. See less

Lead DevOps Consultant

[redacted]

[redacted] United Kingdom

Helping Digital transformation with one of [redacted] go smoothly. Provisioning cloud agnostic platforms with terraform and ansible. Defining Jenkins2 CI/CD pipelines as a [redacted] cobertura, sonar, pa11y, Sauce Labs and more. Encapsulating services in docker containers using packer. Running these in kubernetes cluster. Keeping an eye an all of the infrastructure with Prometheus and Heapster. Presenting result to the customers with Grafana and SpeedyDashboards. [redacted]

Relationship Support Manager - [redacted]

[redacted] London

I maintain relationships with large corporate clients/ Key Accounts £25m+ acting as first point of contact in Relationship Director's absence. I work in the professionals team dealing with Solicitors, Accountants and Architects. I identify opportunities to cross sell solutions to Clients needs and also track and drive opportunities through to ensure sales opportunities completed. I maintain contacts with specialists in other departments, distributing leads accordingly and support the RD in joint meetings. [redacted] also ensure clients are using the correct channels for their servicing needs and seek opportunities to grow income [redacted] prepare and implement strategic campaigns, attend customer meetings/events and hold regular meetings with [redacted] I support with credit applications and post sanction fulfilment and prepare agendas for new business meetings, engaging all product specialists. I have to ensure that new Clients and products are set up on relevant systems and [redacted]

OSINT and Personality

- BIG5 [3] (or OCEAN)
  - **Openness**, depicting appreciation for art, adventure, novel ideas, curiosity, and variety of experience.
  - **Conscientiousness**, depicting tendency to be organised and dependable, being self-disciplined, achievement-oriented, and prefer planned rather than spontaneous behavior.
  - **Extraversion**, depicting being energetic, confident, sociable, talkative, and seeking stimulation in the company of others.
  - **Agreeableness**, depicting tendency to be compassionate, cooperative, trusting, and well-tempered.
  - **Neuroticism**, depicting the tendency to experience unpleasant emotions easily (anger, anxiety, depression, vulnerability etc.) along with emotional instability.

- Dark Triad
  - **Narcissism**, depicting grandiosity, entitlement, pride, egotism, and a lack of empathy.
  - **Machiavellianism**, depicting manipulation and exploitation of others, a cynical disregard for morality, and a focus on self-interest and deception.
  - **Psychopathy**, depicting antisocial behavior, impulsivity, selfishness, callousness, and remorselessness.
- Other Psychosocial Characteristics
  - Stress, depression, happiness, insecure, persuasive, adjusted, impulsive etc.
  - Predispositions toward several parameters
  - Health / food / leisure / work / religion / politics orientation

[3]. John, O.P. and Srivastava, S., 1999. The Big Five trait taxonomy: History, measurement, and theoretical perspectives. Handbook of personality: Theory and research, 2(1999), pp.102-138.

[4]. Paulhus, D.L. and Williams, K.M., 2002. The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. Journal of research in personality, 36(6), pp.556-563.

Correlation Examples

- Not causations!
- **Extraversion** and **neuroticism** significantly associated with social media usage [5].
- **Conscientiousness** negatively related to social media gaming, multiple romantic relationships, and intelligence [6].
- **Conscientiousness** greatly correlates to right-winged conservatism, authority respect, moral inhibitions, the complete opposite from openness [7].
- **Neuroticism** correlates with child trauma, avoid corresponding pretexts [8].
- **Neuroticism** correlates with bad circadian rhythm, observe times of online presence, contact accordingly before or after 16.00 local time [9].
- **Extraversion** (and not neuroticism) has strong correlation with happiness and well-being [10].
- **Agreeableness** correlates well with interpersonal skill, and will to help.
- Also take a look at Professor Michal Kosinski's amazing work: https://www.michalkosinski.com/

[5]. Correa, T., Bachmann, I., Hinsley, A.W. and de Zúñiga, H.G., 2013. Personality and social media use. In Organizations and social networking: Utilizing social media to engage consumers (pp. 41-61). IGI Global.

[6]. Bean, A.M., 2015. Video gamers' personas: A five factor study exploring personality elements of the video gamer. Pacifica Graduate Institute.

[7]. Sibley, C.G., Osborne, D. and Duckitt, J., 2012. Personality and political orientation: Meta-analysis and test of a Threat-Constraint Model. Journal of Research in Personality, 46(6), pp.664-677.

[8]. Moskvina, V., Farmer, A., Swainson, V., O'leary, J., Gunasinghe, C., Owen, M., Craddock, N., McGuffin, P. and Korszun, A., 2007. Interrelationship of childhood trauma, neuroticism, and depressive phenotype. Depression and anxiety, 24(3), pp.163-168.

[9]. Duggan, K.A., Friedman, H.S., McDevitt, E.A. and Mednick, S.C., 2014. Personality and healthy sleep: The importance of conscientiousness and neuroticism. PloS one, 9(3), p.e90628.

[10]. Pavot, W., Diener, E.D. and Fujita, F., 1990. Extraversion and happiness. Personality and individual differences, 11(12), pp.1299-1306.

OWASP
Open Web Application
Security Project

OSINT Tools (indicative list)

- https://inteltechniques.com/menu.html
- https://osintframework.com/
- https://github.com/laramies/theHarvester
- https://tinfoleak.com/
- Python + Selenium or Octoparse if you are in a hurry
- https://spiderfoot.net/
- Maltego
- Recon-ng
- Shodan.io

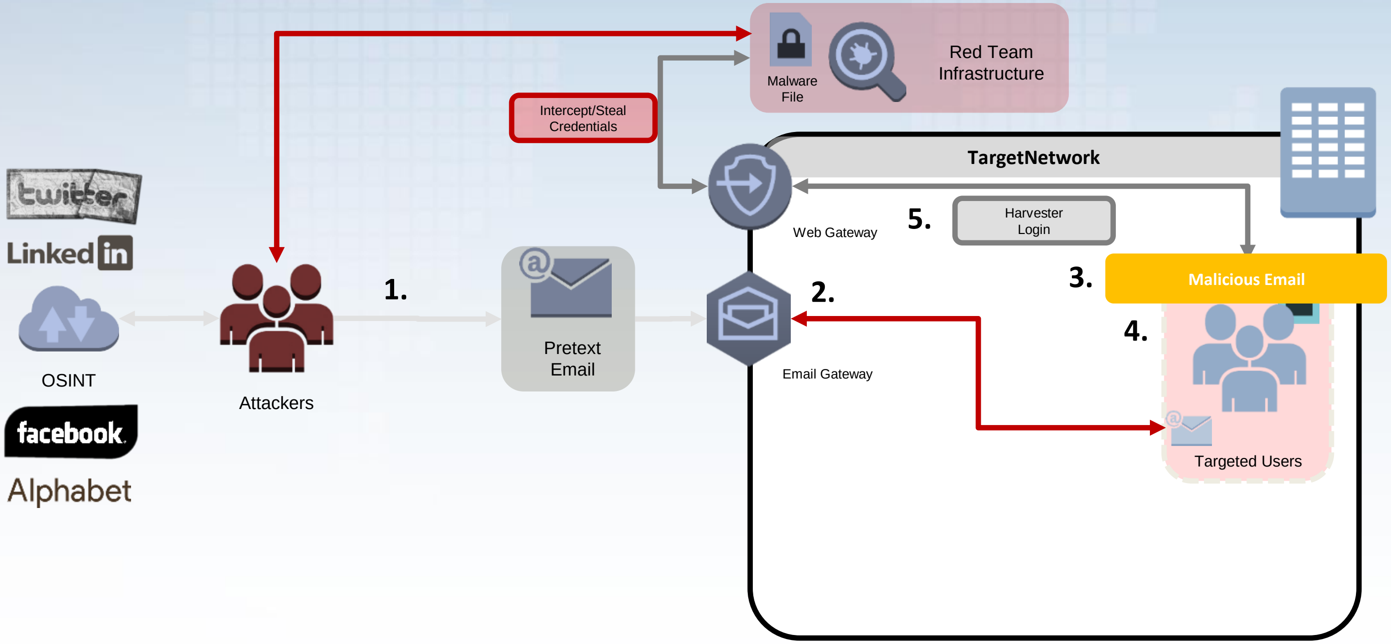
Technical Resources

- https://www.bellingcat.com/tag/osint/
- http://automatingosint.com/blog/
- https://www.osint.fail/
- https://webbreacher.com/
- https://osintframework.com/
- https://inteltechniques.com/
- https://www.exploit-db.com/google-hacking-database

Phishing

- Phishing is a well-known attack vector in which the adversary sends emails to targets in order to trick them into giving out personal information, or executing malicious code.
- In our case we would be mainly interested in the following:
  - Credential harvesting
  - Remote Code Execution
  - Information Gathering
  - Decoy attacks

Abstract Phishing Process



Impact Statement

1. Based on the OSINT gathered, the Red Team prepares a luring email and sends it to the target.

2. The email is delivered to the target.

3. Target clicks on the malicious link and authenticates against our harvester, which can even be a Man-in-the-Middle attack.

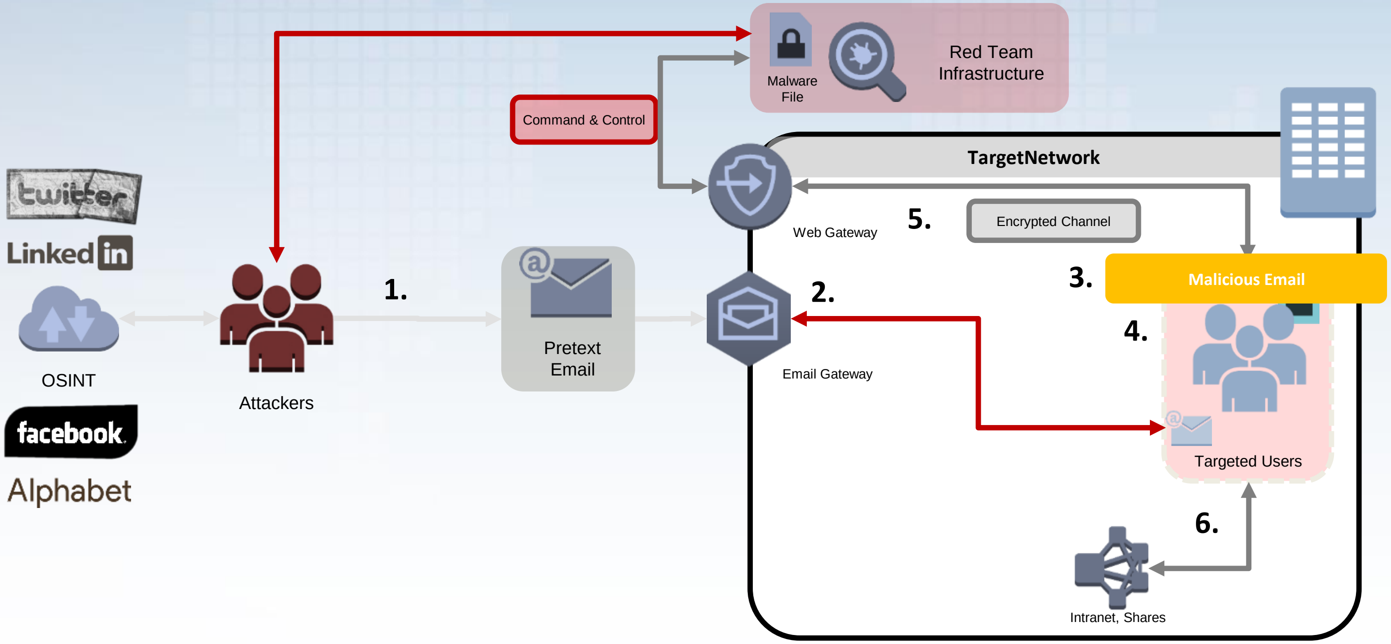
4. Target downloads malicious file, executes it, and enables embedded OLE object / DDE / macro etc.

5. Malicious payload retrieves the malware file and executes it providing the Red Team with access to the internal network.

6. The Red Team gains access to the internal network, shares, might utilize harvested credentials to move laterally, etc.

OWASP
Open Web Application Security Project

Abstract Phishing Process



Impact Statement

1. Based on the OSINT gathered, the Red Team prepares a luring email and sends it to the target.

2. The email is delivered to the target.

3. Target clicks on the malicious link and authenticates against our harvester, which can even be a Man-in-the-Middle attack.

4. Target downloads malicious file, executes it, and enables embedded OLE object / DDE / macro etc.

5. Malicious payload retrieves the malware file and executes it providing the Red Team with access to the internal network.

6. The Red Team gains access to the internal network, shares, might utilize harvested credentials to move laterally, etc.

OWASP
Open Web Application Security Project

Phishing Infrastructure

- Create a mail server as if you hate phishing and spam:
  - https://www.linuxbabe.com/mail-server/ubuntu-16-04-iredmail-server-installation OR
  - https://www.linuxbabe.com/mail-server/ubuntu-18-04-iredmail-email-server
- Now, according to your pretext and OSINT results, create sending profiles (email addresses to send phishing emails from).
- Create the web server that the targets will be asked to get to in the phishing email.
  - Generate a pretty page that looks legit.
  - Make sure the domain is categorised.
  - Letsencrypt will be handy.
  - Oh the wonders of .htaccess file
  - Create landing page, decoy pages, etc.
  - Take a look at Modlishka and Evilnginx
  - Also, check piwik https://builds.piwik.org/piwik.zip for clickstream analysis

Malicious Documents

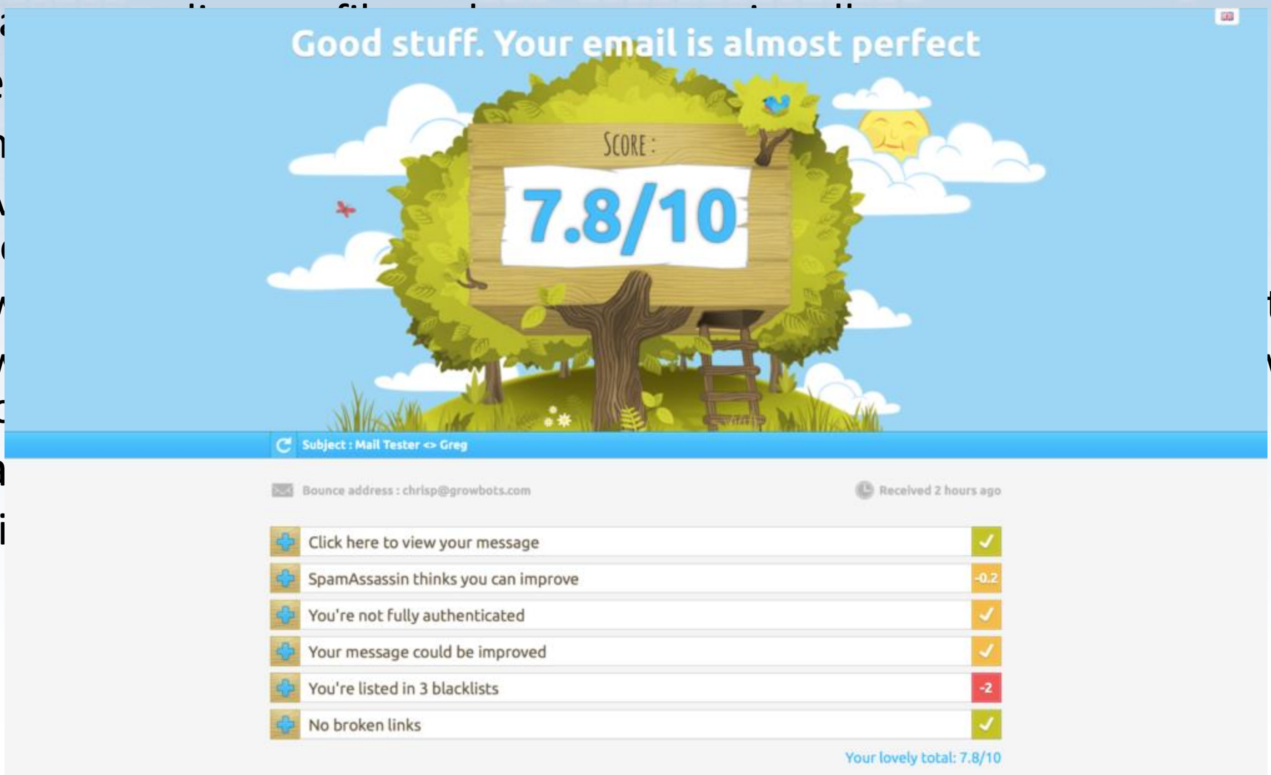
- There are several things you can try.
- Start with macros (Metasploit, Cobalt Strike, Empire, etc.)
  - Obfuscate with VBad https://github.com/Pepitoh/VBad
  - Also, several tricks out there, search and try them.
  - Also, check LoLBins: https://lolbas-project.github.io/
  - And maybe Invoke-DOSfuscation could be handy: https://github.com/danielbohannon/Invoke-DOSfuscation
  - https://outflank.nl/blog/2019/05/05/evil-clippy-ms-office-maldoc-assistant/
  - https://outflank.nl/blog/2019/10/30/abusing-the-sylk-file-format/
- Embedded OLE Objects
- Click-once applications, for a bit more advanced cases

Final Steps

- Generate multiple pretexts (according to OSINT results)
  - You want to personalise but not too much
  - Change sending profile and pretext occasionally
- Create email templates, personalise, update with malicious links
  - Email templates can be anything between plain and very complex
  - Several templates online, especially from marketers (good at bypassing spam filters)
  - Always a good idea to personalise malicious links and landing page, too
  - Always test your email prior to sending, have used mail-tester.com with good success so far
- Send and wait
  - Phishing requires patience
  - Unless you want to combine it with vishing or smishing

Final Steps

- Generate multiple pretexts (according to OSINT results)
  - You want to personalise but not too much
  - Cha
- Create
  - Em
  - Sev ing spam filt
  - Alw too
  - Alw vith good suc
- Send a
  - Phi
  - Un



Good stuff. Your email is almost perfect

SCORE :

7.8/10

Subject : Mail Tester <> Greg

Bounce address : chrisp@growbots.com

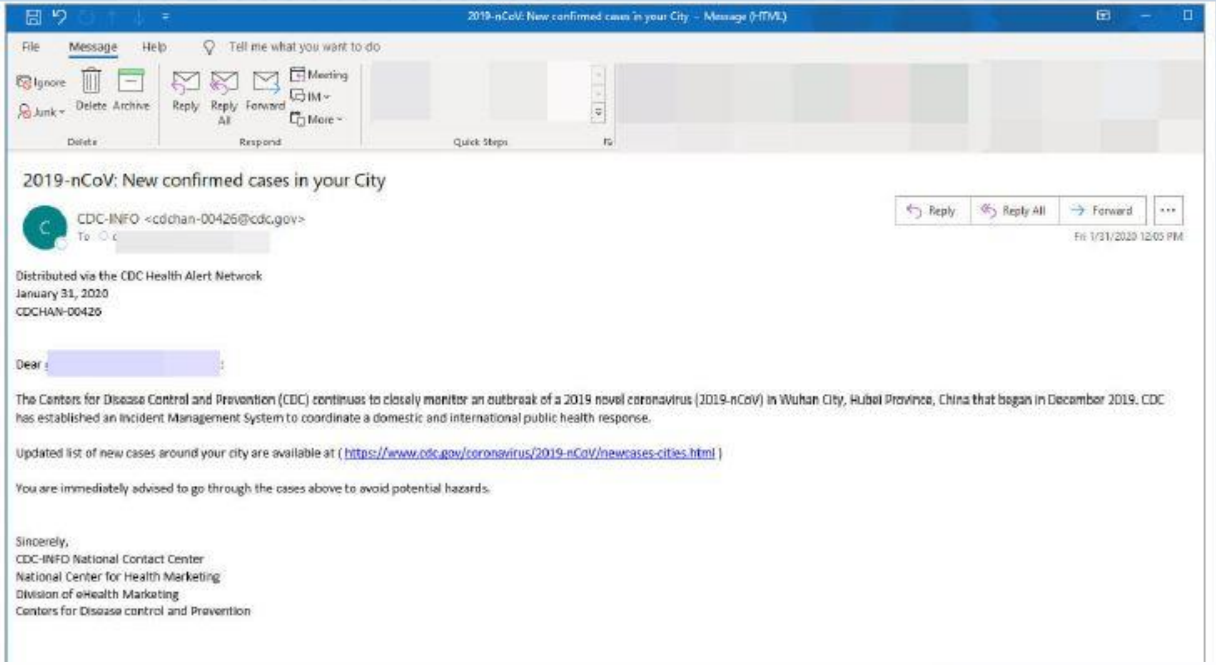
Received 2 hours ago

Click here to view your message	✓
SpamAssassin thinks you can improve	-0.2
You're not fully authenticated	✓
Your message could be improved	✓
You're listed in 3 blacklists	-2
No broken links	✓

Your lovely total: 7.8/10

Realistic (?) Scenario

1. Send a luring email



2019-nCoV: New confirmed cases in your City

CDC-INFO <cdchan-00426@cdc.gov>
To [redacted]

Fri 1/31/2020 12:05 PM

Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

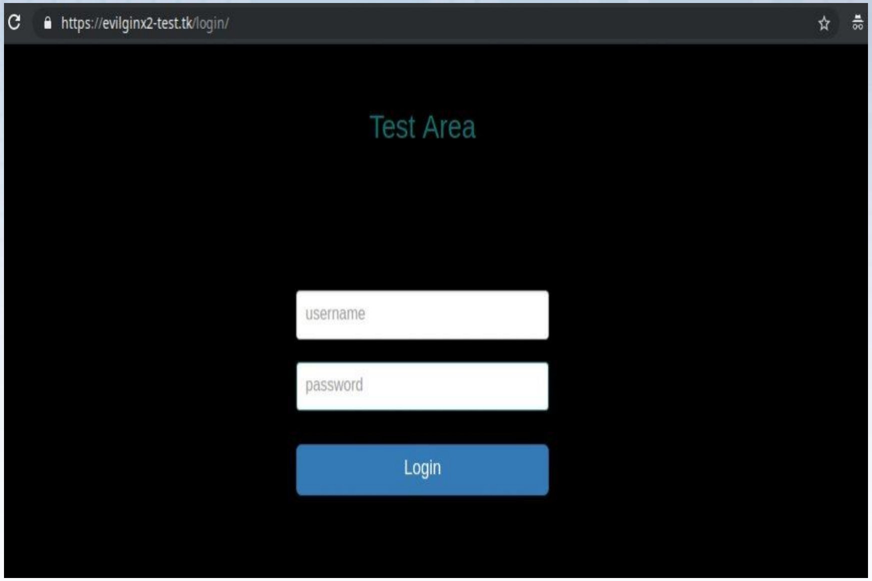
Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

Realistic (?) Scenario

1. Send a luring email
2. Target clicks and is presented with fake-login / harvester



https://evilginx2-test.tk/login/

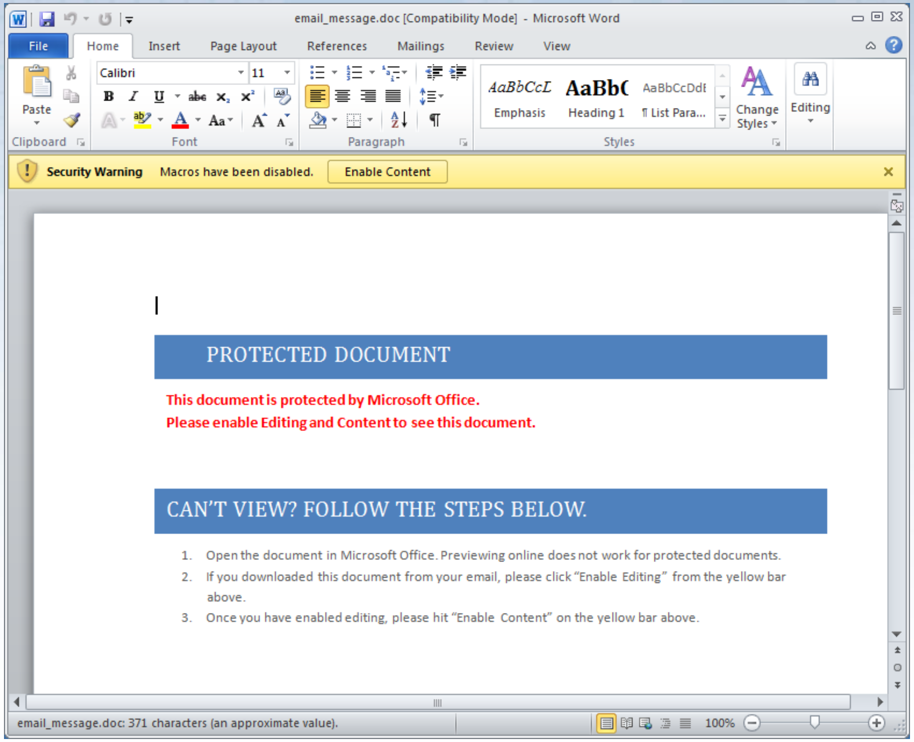
Test Area

Realistic (?) Scenario

1. Send a luring email
2. Target clicks and is presented with fake-login / harvester
3. Target is presented with a download button

Realistic (?) Scenario

1. Send a luring email
2. Target clicks and is presented with fake-login / harvester
3. Target is presented with a download button
4. Downloaded document has some form of RCE (DDE, OLE Object, Macro, etc.)



Security Warning Macros have been disabled.

PROTECTED DOCUMENT

This document is protected by Microsoft Office.
Please enable Editing and Content to see this document.

CAN'T VIEW? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please hit "Enable Content" on the yellow bar above.

email_message.doc: 371 characters (an approximate value).

Red Team Code Of Conduct

- It is important to be as realistic as possible. However, there are ethical, moral, and legal boundaries to consider
- Never break local or regional law
- Big ethical decision on whether you are allowed to impersonate real individuals
- Don’t mention/exploit friends and family of the targets
- Don’t target personal emails, social media, phone numbers
- Don’t share specifics on compromised accounts, avoid witch hunting
- Don’t target 3rd party, providers, suppliers
- Be proactive with data, exfiltration, etc. GDPR still applies

** Exceptions to the above will only be conducted with prior validated approval, from individual and groups with appropriate authority.*

OWASP
Open Web Application Security Project

Thank you :)