International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:8, 2016

Experimental Analysis of Tools Used for Doxing and Proposed New Transforms to Help Organizations Protect against Doxing Attacks

Parul Khanna, Pavol Zavarsky, Dale Lindskog

***Abstract*—**Doxing is a term derived from documents, and hence consists of collecting information on an organization or individual through social media websites, search engines, password cracking methods, social engineering tools and other sources of publicly displayed information. The main purpose of doxing attacks is to threaten, embarrass, harass and humiliate the organization or individual. Various tools are used to perform doxing. Tools such as Maltego visualize organization's architecture which helps in determining weak links within the organization. This paper discusses limitations of Maltego Chlorine CE 3.6.0 and suggests measures as to how organizations can use these tools to protect themselves from doxing attacks.

***Keywords*—**Advanced Persistent Threat, FOCA, OSINT, PII.

I. Introduction

DOXING is the collection of personal information of an individual or organization using social media networks, web search engines, social engineering, password cracking methods etc. [3]. Doxing can be carried out either by attackers to launch a sophisticated attack on a target or by intelligence agencies for investigation and surveillance purpose. Various tools and applications including open-source software are available online to facilitate the collection of information from the internet and other sources.

TABLE I
Tools Used for Collecting Information [2]

Category	Information Collected	Tools/Sites Used
Collecting Information	Name, Username	Google, Bing
Location	Geo IP, Geo-tag, Employer address, Time Zone	Facebook, Pipl, lpInfoDB, PeekYou, ExifTool
Age information	Chat Logs, pictures, comments, Employment	IM, Skype, IRC, TinEye
Network Information	Domain IPs, Domain information	Whois, Netcraft, dig, DNSDigger
Combine data	Update records, rinse and repeat	Text editor, Maltego, spreadsheet

Parul Khanna is a graduate and research assistant in Information Systems Security Management at Concordia University of Edmonton, Alberta, Canada (phone: +1587-785-9999, email: pkhanna@student.concordia.ab.ca)

Dr. Pavol Zavarsky is professor and director of research at Concordia University of Edmonton, Alberta, Canada, for Master of Information System Security Program (MISSM). He is CISSP and CISM certified with PHD in Electrical Engineering from Japan (phone: +1780-413-7810, e-mail: pavol.zavarsky@concordia.ab.ca)

Dale Lindskog is associate professor at Concordia University of Edmonton, Alberta, Canada in Information System Security Management. He did his PHD from York University (phone: +1780-491-6899, e-mail: dale.lindskog@concordia.ab.ca)

Taking into consideration the huge volume of information to be collected, a single tool cannot be trusted to collect the entire information at one go. Most of these tools have to be used separately to collect the information. Often the findings and results obtained using different tools have to be consolidated to get a better understanding before launching a doxing attack. Tools like Maltego facilitate this by organizing the data collected online to give a visual representation which helps in determining relationship links between people, groups of people, professional and personal affiliations [3].

Maltego is an open-source tool which gathers information from open sources [4]. It works on "transforms" and "entities" which are synonymous to "queries" and "objects". Transforms are code snippets generally written in Python and can be modified to suit the needs of a user. Often the in-built transforms of Maltego function by scanning popular (or limited) social media sites. As such, new transforms can be coded and integrated within the Maltego framework to identify critical information available on other sites. For instance, if an organization wants to know what all critical information is available on a particular website (such as Gravatar, which is not scanned by in-built transforms of Maltego), the organization can add or modify transforms (or queries) for the website.

The main contribution of this paper is identification of limitations of doxing tools such as Maltego through experimental analysis and primarily focus on measures by which an organization can protect itself from doxing attacks. In addition, this paper also discusses briefly proposed new transforms which can help the organization to identify and aware itself of crucial information available publicly.

The paper reviews the working of existing transforms of Maltego as discussed in [11]. Then, limitations of the transforms are identified and new transforms are proposed so that if an organization has a proper understanding of the behavior of Maltego transforms, then it can build its own transforms to customize the search and search for user-defined sites.

The remaining sections of the paper are organized as follows. In Section II, the related works are discussed. Section III presents methodology while Section IV discusses limitations of Maltego transforms and proposes solution to protect organization from doxing attacks. The conclusion and future work are presented in Section V.

II. Related Work

In [8], doxing is defined as a mode of Open-Source Intelligence (OSINT) [1] and is usually considered an advanced persistent threat. OSINT involves the collection of personally identifiable information (PII) available publicly about any organization and using this information for harassing, blackmailing or hacking purpose to gain revenge, financial benefit or other cause. This paper focusses on creating awareness about the risks involved and impacts of doxing any individual or organization. It presents the need of a risk model to mitigate the effects of doxing and suggests an ISO.IEC 27005 risk model which can be integrated into an organization's risk management framework. The research aligns the domains of ISO/IEC 27002 ISMS Controls with the proposed risk model as shown in Table II.

TABLE II
Table Aligning Domains of ISO/IEC 27002 with Risk Model [8]

No	ISO/IEC 27002 ISMS Controls	Features of Proposed Model Enabling these Controls
1.	Risk Assessment and Treatment	Policy & Procedures-Formulation and Review (A.1), HR Pre-Hire Controls (A.2), Continuous Monitoring (B.1), Security Audits (B.2), Detection (C.1), Analysis (C.2), Containment (C.3)
2.	Security Policy	Policy & Procedures-Formulation and Review (A.1), Security Audits (B.2), Post Incident Review (C.4)
3.	Organization of Information Security	HR Pre-Hire Controls (A.2), Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Continuous Monitoring (B.1), Security Audits (B.2)
4.	Asset Management	Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Security Audits (B.2)
5.	Human Resource Security	Education Training and Awareness (A.7)
6.	Physical and Environmental Security	N/A
7.	Communications and Operations Management	Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Security Audits (B.2)
8.	Access Control	Data Encryption (A.5), Access Controls (A.6)
9.	Information Systems Acquisition, Development and Maintenance	HR Pre-Hire Controls (A.2), Data Sanitization (A.3), Data Disposal (A.4), Data Encryption (A.5), Access Controls (A.6), Continuous Monitoring (B.1), Security Audits (B.2)
10.	Information Security Incident Management	Detection (C.1), Analysis (C.2), Containment (C.3), Post Incident Review (C.4)
11.	Business Community Management	N/A
12.	Compliance	Policy & Procedures- Formulation and Review (A.1), Security Audits (B.2)

Reference [9] provides an extension to the Maltego framework to provide exploration and reaction to a phishing campaign. This research aims to come up with a new software that can be used to analyze phishing campaigns so as to provide useful information on countermeasures related to phishing attacks. The authors of this paper first create a sample scenario wherein phishing attack is deployed locally on a machine. Then useful information is collected from the huge volume of data gathered from a phishing campaign. The paper also provides useful information on countermeasures related to this phishing attack and different types of phishing attacks. The research explains how Maltego framework works in case of phishing attacks and how transforms can be used to collect information. The Maltego framework for this research provides a means of exploring, analyzing, correlating and reacting to phishing campaigns by illustrating relationships between actors in a phishing campaign, deriving useful information from existing data and facilitating response mechanisms. The given framework also provides the ability to integrate existing solutions into the framework through the use of directory monitoring which means that the project has the potential to perform central role within an anti-phishing system.

In [1], authors have carried out a vector and cognitive attack on a given company. The attacker makes use of the software tools like Maltego and simple phishing toolkit to harness the open source information available and bring about a successful vector attack. There are other tools available for gathering information briefly discussed in [5]. These are FOCA (Fingerprinting Organizations with Collected Archives) [6], SamSpade, Necrosoft Scan [7] and Paros Proxy.

III. Methodology

A. Assessment of Maltego and Its Transforms

Available transforms in community version of Maltego Chlorine CE (3.6.0) downloaded from [10] were used to collect information on sample entities or objects. The information collected by these transforms was analyzed and verified for accuracy. The information was then aggregated to establish relationships or "links" between them. Further, transforms written in Python were studied to get more understanding.

B. Identifying the Limitations of Maltego Transforms by Searching for Missing Links in Information Gathered in A

This phase involved Searching/scanning for useful information on sites not scanned by Maltego transforms and identifying missing links. It also involved understanding functioning of transforms in Python and discovering loopholes or limitations. This phase also suggests new transforms which could help the organization to detect useful information present on social media sites in advance.

C. Understanding How an Organization Can Protect Itself from Doxing Attacks

This phase analyzes and provides measures as to how an organization can prevent itself from doxing attacks.

IV. Limitations of Doxing Tools and Proposed Solution

A. Limitations of Maltego Chlorine CE 3.6.0

Maltego Chlorine CE 3.6.0 version includes transforms which cover social networking sites like – Facebook, Twitter or hashtags. Therefore, it scans only these limited sites for gathering information. It doesn't include in built transforms to scan other popular social media websites such as – Skype, Instagram, Yahoo or, in fact, YouTube. In addition, inbuilt transforms available with Maltego Chlorine CE 3.6.0 for scanning from popular sites such as Facebook are limited in their functionality. These transforms do not provide the following features:

- Returning Facebook profile by e-mail
- Searching Facebook profile by a combination of alias, person name, company name, city, college, age or website
- Returning data about a Facebook user from the password recovery page.
- Extrapolating search by combining results from other useful/popular sites such as Gravatar.
- Searching for similar hashtags within Facebook's social network.

Apart from this, Maltego transforms do not scan other well popular sites such as Instagram. Transforms do not return results based on Instagram profile nor do they search for the user in Instagram social network. Also, they do not scan for a person or entity on Google plus.

Maltego Chlorine CE 3.6.0 runs transforms on a single entity (e.g. Name, IP addresses etc.). It cannot take a combination of entities such as name and location. It doesn't come with inbuilt transforms which allow translation (or conversion) between two languages. Maltego transforms do not help in predicting how vulnerable a website is to attacks or vulnerabilities such as Heartbleed. These transforms also do not yield any information on the privacy settings of a profile. The transforms also don't tell any information related to geolocation of any object.

Maltego does not allow the use of transforms to extract any particular information from a company's profile. Maltego doesn't allow to search within the company the name of a particular employee. It does not have in-built transforms to extract emails, phone numbers or names of persons from a document text.

This paper highlights some of the limitations of doxing tools such as Maltego and proposes new transforms which can help organizations to know the useful or confidential information available publicly. As such, these simple basic transforms can be further integrated into a large framework used by organizations and contribute successfully in achieving the goals of preventing doxing attacks. Further, testing of these transforms/modules leads to better understanding of how these tools can be actually used by organizations to protect them against doxing attacks.

B. How Organizations Can Protect Themselves from Doxing Attacks

A single tool does not provide entire information. In addition, tools such as Maltego makes use of in-built transforms to dox information. Even if a hacktivist wants to customize the search by, for example, a combination of name, age and location, it's not possible with in-built Maltego transforms. Therefore, if an organization develops transforms as per its own requirements which allow in customizing the searc2, it will be able to aware itself of the crucial information available publicly. Actions and precautions can always be taken to protect this confidential information in future.

Other countermeasures to prevent doxing attacks include:

Dox Yourself: Use the tools such as Maltego to find as much publicly available information as possible and then take measures to protect that information if it is confidential. The information collected from different sources should be examined carefully to establish "connections" or "links". Doxing attacks can be prevented by not disclosing personal information on chat rooms and message boards. For instance, disclosure of Facebook ID might help the hacktivist to predict the skype ID, if the user maintains the same ID for both. The same is applicable with passwords. Therefore, it's advisable to delete any sensitive information leading to some other information.

At times, there comes situation when an organization might want its employees to have access to important information available on website, but not others. In such cases, it's better to adjust privacy settings, so that only certain groups of people can see that information. The same is applicable with an individual's Facebook profile or LinkedIn account.

Defense-in-depth: This implies having multiple layers of defense to protect internal networks within an organization. For instance, if a hacker successfully predicts password of an individual, two-factor authentication and password manager can prevent the hacker from accessing mails even though he knows the password. In fact, sites like Gmail now encourage two factor authentication, a process in which new login attempts not only require your email address password but also a onetime code texted to your phone. It's good because it increases the protection on email and indicates whether someone else is trying to log into your account or not.

The Onion Router (TOR): This can be used as a safe means of communication if a user wants to mask or conceal its IP address or location from anyone conducting a network surveillance or network analysis over a communication channel. Its main use is to protect the personal privacy of users, and allow them to freely conduct confidential communication by keeping their internet activities from being monitored.

Password managers like Lastpass are convenient and easy to use and help securing passwords. These extensions remember and auto-fill passwords which allow you to generate more complex passwords without having to worry about remembering them. Another good method to protect yourself from doxing attack is to create fake social media accounts with multiple emails so that it misleads the hacker.

Audit yourself: Several websites like Pipl can trace the source of information back to the original source. These websites can be used by organization to audit oneself.

Demilitarized Zones (DMZ), Intrusion Detection and Prevention systems (IDS and IPS): Organizations can setup demilitarized zones to increase level of security by segmenting networks into different segments such as internal or external. This kind of architecture prevents attackers from obtaining all the information in case of data breach. IDS acts as layer of protection to monitor network traffic and patters to detect attacks. IPS, on the other hand, exists to complement IDS alerts as it takes actions against attacks by rejecting the traffic alerted by IDS as possible attack.

Customizing Transforms: If an organization customizes the transforms according to its own needs, then it can aware itself of information being doxed and take necessary precautions and measures. Reference guides to develop local transforms are available easily as mentioned in [12]-[14], and in-depth understanding of the same can protect organizations from being doxed. For instance, new transforms can be built to extract information about a company published by hackers on forums such as Pastebin. Such information is generally used by other hackers to launch attacks, and hence it's important to have new transforms that can extract information from such forums.

Once an information gets exposed in case of doxing attack, it's always better to minimize damage and regain control by taking defensive steps. It's always better to know attackers in advance by, for example, setting up honeypots or websites wherein entry of unauthorized users can be detected.

V. Conclusions and Future Work

Doxing can have an impact on reputation or on competitive advantages of the doxed organization. Furthermore, doxing could lead to further escalations like hacking, fraud, espionage, etc. This paper presents strategies on how tools used for doxing can be used by organizations to protect themselves from doxing attacks. Tools such as Maltego, as illustrated in this paper, work on basis of transforms which are used for collecting information. Same transforms can be customized as per requirements by the organization to dox its own information and identify and analyze the weak links. Similarly, other tools used to dox information can also be improved upon and customized in such a manner that organization can make itself aware of confidential information available publicly. This paper focusses on Maltego Chlorine CE 3.6.0, but future work in this field is open to exploring all other doxing tools and their modules. Measures to help organization protect itself from doxing attacks can be studied in more detail.

References

[1] L. Ball, G. Ewan, N. Coul, "Social engineering using open source intelligence gathering", 2012, Available: https://repository.abertay.ac.uk /jspui/bitstream/handle/10373/1435/Ball_ Undermining_Author_2012.pdf?sequence=2&isAllowed=y

[2] Links for doxing, personal OSINT, profiling, foot printing, cyber stalking", Available: http://www.irongeek.com/i.php?page=security/ doxing-footprinting- cyberstalking

[3] I. N. Norris, "Mitigating the effects of doxing" 2012, Available: http://www.ecii.edu/wpcontent/uploads/2013/06/INorris_MitigatingEffe ctsOfDoxing.pdf

[4] S. Ali, T. Heriyanto, "Backtrack 4: Assuring Security by penetration testing", Available: https://books.google.ca/books?id= SodvK4NMBgwC&pg=PT188&lpg=PT188&dq=limitations+of+malteg o&source=bl&ots=2TlfIzBbUm&sig=E9osiFX4_G5PMbEDZvOVCCh 2iOgO5#v=onepage&q=limitations% 20of%20maltego&f=false

[5] "Lucideus Lab for information about Doxing", Available: http://lucideustech.blogspot.ca/2013/11/doxing.html

[6] "Fingerprinting Organizations with Collected Archives (FOCA)", Available: https://www.elevenpaths.com/labstools/foca/index.html

[7] NScan tool, Available: http://nscan.hypermart.net/

[8] R. S. Mathews, "A study of doxing, its security implications and mitigation strategies for organizations", 2013, Available: http://infosec.concordia.ab.ca/files/2013/02/Roney_Mathews.pdf

[9] M. Marx, "The extension and customization of Maltego data mining environment into anti-phishing system"2014, Available: http://www.cs.ru.ac.za/research/g11m3847/downloads/thesis.pdf

[10] Official page for downloading Maltego: Version: Maltego Chlorine CE 3.6.0 (latest version) Supporting OS: Windows based operating system, Available: https://www.paterva.com/

[11] "Maltego Transforms- A reference guide to understand the Maltego transforms", Available: http://www.paterva.com/web6/documentation/M3GuideTransforms.pdf

[12] "Developing Maltego local transforms", Available: https:// www.paterva.com/web6/documentation/developer-local.php

[13] Official Maltego tutorial: Writing your own transforms, Available: https://www.youtube.com/watch?v=42KhnNQS8AU

[14] "Writing Python transforms", Available: https://www.paterva.com/ web6/documentation/TRX_documentation201 30403.pdf