NTNU – Trondheim
Norwegian University of
Science and Technology

TDT39 Empirical Studies in ICT

Research Plan

Title:
Cyber Crime Economy

Written By:
Yara Bayoumy

Supervised By:
Guttorm Sindre
Per Håkon Meland

Period of Study:
Fall 2017 and Spring 2018

Amount of resources planned:
20 hours per week

Submitted: December 1, 2017

Purpose

Security risk assessment methods heavily rely on historical data to make predictions on possible future security threats and often disregard the attacker's background. Attacker-centric risk assessment methods have failed to capture the true attacker's intent because it is either difficult to obtain or not accurate enough. Added to that, not much research has been done to improve attacker profiling methods. Modern day attackers are no longer script kiddies, but organizations with the goal to achieve profits through the selling of malicious software.

Retrieving information of the various attacker facets can be done in a number of ways. One common example is the use of honeypot frameworks to capture an attempt to attack from an adversary and create a network decoy [4]. They have been used to defend systems against automated attacks and human intruders by conning. However, the costs of a honeypot deployment can be extremely expensive [1]. Added to that, it does not distinguish the behaviour intent of the attacker.

Another method of estimating an attacker's behaviour is by using the stochastic game theory in which the attacker is assumed to know all vulnerabilities of the system [5]. The model that was implemented in the process was simple and was just an indicator to the expected behaviour of the attacker but not exactly how the attacker will behave. It was also limited to a specific set of attacker profiles, such as attackers that are willing to take a greater risk.

Both these methods are obsolete, the criminal territory behind security attacks has changed drastically. In May 2017, the global business industry witnessed an unprecedented spread of ransomware, a type of malware that forbids access to a computer files unless a ransom is paid. From this encounter, researchers have discovered how easy it is to obtain ransomware from the dark net and use it to exploit any computer.

What I wish to achieve with this research is to capture the attacker's intent by observing their social activities on the dark net. None of the aforementioned studies retrieve attacker profiles from the dark net. It succeeds in obscuring ones identity, therefore it offers a safe harbor for criminal activity. Observing the forums and online markets within the dark net will give us a clear insight on how they communicate, the costs incurred on services and products needed to perform an attack, and the structure of organized crime. These observations are perfectly aligned to the parameters needed for attacker profiling. The following lists the research questions based on the my motivations:

- **RQ1:** What data provided by the dark net can be used to estimate the likelihood of a ransomware attack?
  - *RQ1.1:* What is the social structure of the vital actors involved in developing and selling ransomware-as-a-service?
  - *RQ1.2:* What costs and risks are imposed on the involved actors?
- **RQ2:** How can the accuracy of attacker profiling methods be improved?

Contributions

This research will contribute in providing a thorough analysis of the hidden services of the dark net that are responsible for planning cyber security attacks, particularly ransomware. This includes the social structure of the different participants and their roles, the costs of the resources needed to develop the ransomware (such as hosting services) and the costs of selling it on the dark net marketplaces.

The results from this analysis will help create attacker profiles that will be applied to an attacker-centric threat modelling technique. A detailed comparison between the most common method of attacker profiling and the results of this research will contribute in justifying the improvements in threat prediction. This offers a new efficient methodology of attacker profiling within the field of cyber security.

Research Methods

The research questions were refined based on two sources of information: the latest research studies in attacker profiling and the most recent developments in malicious software distributed through the dark net. For the former, an investigation on the relevant literature is carried out to define a conceptual framework for this research. As for the latter, the unprecedented distribution of ransomware in May 2017 has inspired me to narrow down the focus of this research on the development and distribution of ransomware through the dark net.

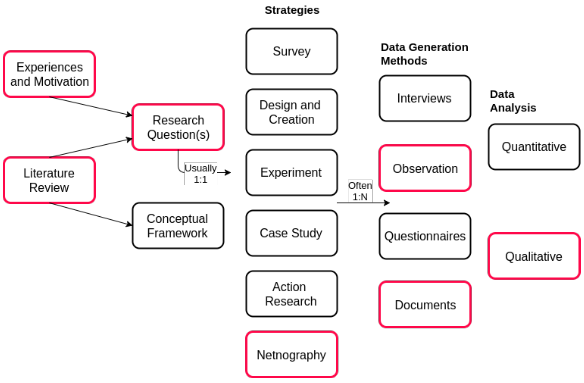

Figure 1: Research Process [3]

Netnographic study is the chosen strategy because it is used to describe the culture of an online community. In this research, the dark net markets and forums represent the community I plan to observe. The type of netnography will mostly be semiotic in the sense that the researcher will not emphasize with the subjects but inspect the intentions and behaviours of the users.

Data will be collected through regularly documented field notes of observations. However, a problem that may arise during the process is that some online markets and forums are shut down by law enforcement officials. In most cases, officials release reports of the operation which may include relevant data such as vendor profits, and user popularity. The research questions are best answered with analysis of qualitative data with the support of quantitative data. Quantitative data can be used to generalize and visualize a specific phenomenon experienced during the observations.

Participants

The research will be conducted by me with the supervision of Professor Guttorm Sindre and Senior Researcher Per Håkon Meland. Sindre is the lead supervisor who will be frequently monitoring my research progress. Meland is the co-supervisor and will be providing feedback and technical advice on netnographic strategies and threat modelling practices based on his expertise in the field. Both supervisors own the right to preview the outcomes.

Users of the online markets and forums of the dark net are directly involved in this research since the netnographic study includes observations of their social activities. These users can be site operators, service vendors and buyers. Since the dark net fosters illegal activity, ethical implications were addressed early on in the research process with the supervisors. The main source of reference was the Internet Research Ethics (IRE), a discipline that provides codes of conduct for research in the internet including ethics of dark net research. Ethical regulations provided by the IRE strictly advise researchers not to get involved in any criminal activity provided by the participants of the dark net [2]. Collected data should also not pose any threat to the users of the dark net. All users use anonymous usernames, but to avoid any possible data that can possibly be used for prosecution, all usernames are not publicized in the research.

Research Paradigm

The netnographic strategy involves the researchers understanding of the social activities between the hackers that develop the ransomware, the vendors that sell them, and the consumers that buy them. Therefore it has a strong connection to interpretive paradigm. Despite the fact that there is very little researcher involvement, it still does not relate to a critical research paradigm because the observations will be presented from my personal perspective. The conversations between the different users in the dark net will be an important source for qualitative data analysis, and researchers may have different interpretations of the motives of the users involved.

Final Deliverables and Dissemination

The research process and its outcomes will be documented and delivered in a project report and master thesis.

References

[1] Dornseif and May. "Modelling the costs and benefits of Honeynets". In: (2004).

[2] James Martin and Nicolas Christin. "Ethics in cryptomarket research". In: *International Journal of Drug Policy* 35 (2016), pp. 84–91.

[3] Briony J Oates. *Researching information systems and computing*. Sage, 2005.

[4] Provos et al. "A Virtual Honeypot Framework." In: *USENIX*. Vol. 173. 2004, pp. 1–14.

[5] Sallhammar et al. "Using stochastic game theory to compute the expected behavior of attackers". In: *Applications & the Internet Workshops*. IEEE. 2005, pp. 102–105.