CERIAS

The Center for Education and Research in Information Assurance and Security

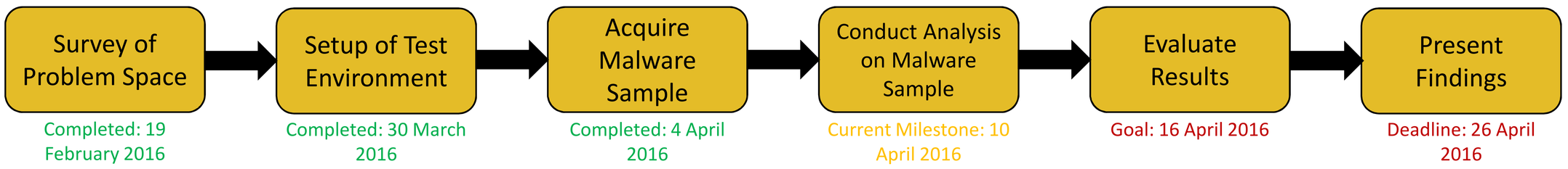
Anatomy of IoT Malware: A Practical Case Study

(*Work in Progress*)

Robert Haverkos
Purdue University
rhaverko@purdue.edu

Work being conducted to fulfill the capstone requirement for the Cyberforensics of Malware course under the direction of Visiting Assistant Professor Marcus Thompson, thomps35@purdue.edu

Project Timeline



Abstract

The purpose of this study is to identify key differences, if any exist, between malware that targets IoT (Internet-of-Things) devices and more traditional computing environments such as PCs and smartphones. This is being done by way of an observational case study of a malicious code sample with a focus on high level qualitative constructs. The observation will be conducted primarily through static analysis of the source code of the malicious program. The goal of this study is to present the findings in a way that is accessible to a wider range of stakeholders in the IoT sphere.

Problem Space Overview

- IoT (Internet-of-Things) devices, for this project, are considered to be network connected devices with hardware capable of general computation and are not a member of more traditional categories (ie. PC, smartphone, or tablet). This definition was adapted from an AT&T industry report. [1]
- Number of IoT devices estimated to exceed 20 million. [1]
- Market estimated to reach $7.1 billion with $11 trillion in economic impact by 2025. [2][3]
- Security of IoT devices is a rising concern. [4][5][6]
- Attacks on IoT devices are increasing rapidly. [7]
- Botnet malware has already been observed on these devices. [8]

Sample Analysis Goals

The goal of this work is to make comparisons between the characteristics of IoT malware and more traditional and well established varieties. In order to do this, a number of observations must be made regarding the properties of the IoT malware sample. The following characteristics have been compiled from the malware traits and analysis objectives from the book *Practical Malware Analysis* by Sikorski and Honig, and will be used to guide the analysis and describe the malware sample. [9]

- Intent
- Infection Vector
- Obfuscation Scheme
- Command and Control Interface
- Data Collection and Exfiltration
- Propagation Mechanism
- Persistence Mechanism

Sources

[1] “What You Need to Know About IoT” AT&T, 2015. Available at http://www.business.att.com/content/whitepaper/what-you-need-to-know-about-IoT.pdf
[2] “Data loss considered to be biggest risk of IoT, followed by malware and unauthorized access” Fortinet, 2014. Available at http://search.proquest.com/docview/1539510667?accountid=13360
[3] J. Manyika *et al*. “Unlocking the Internet of Things. McKinsey & Company”, 2015. Available at http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world
[4] J. Oltsik. “The Internet of Things: A CISO and Network Security Perspective” Enterprise Security Group, 2014. Available at http://www.cisco.com/c/dam/en_us/solutions/industries/docs/energy/network-security-perspective.pdf
[5] “Network-level security to be on government and operator agendas in 2015; mobile malware and IoT set to define new mobile security challenges” M2 Presswire, 2014. Available at http://search.proquest.com/docview/1636649036?accountid=13360
[6] “2016 Threat Predictions” McAfee Labs, 2016. Available at http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf
[7] Y. Pa *et al.* “IoTPOT: Analyzing the Rise of IoT Compromises” USENIX WOOT, 2015. Available at https://www.usenix.org/sites/default/files/conference/protected-files/woot15_slides_papa.pdf
[8] “Proofpoint Uncovers Internet of Things (IoT) Cyberattack: More than 750,000 Phishing and Spam Emails Launched from “Thingbots” Including Televisions, Fridge” Proofpoint 2014. Available at http://investors.proofpoint.com/releasedetail.cfm?ReleaseID=819799
[9] M. Sikorski, A. Honig *Practical Malware Analysis* San California: No Starch Press, 2012

CERIAS

PURDUE UNIVERSITY