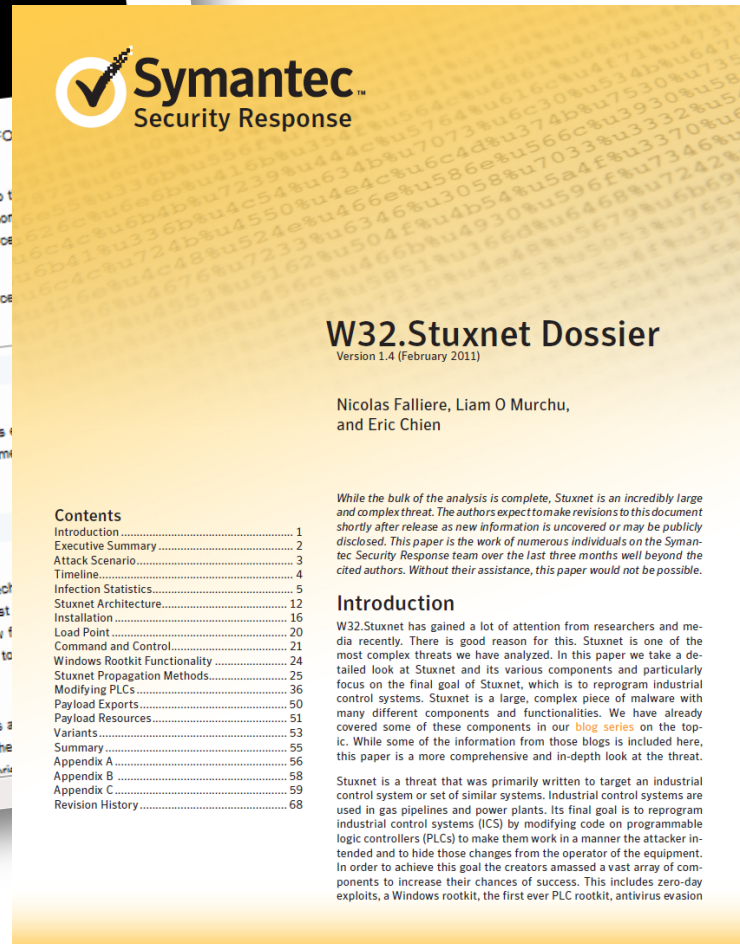




Security Concerns for Flash-Based Storage

Sandler Rubin
Symantec Corp.

An Organizational Nightmare

Symantec
Security Response

W32.Stuxnet Dossier

Version 1.4 (February 2011)

Nicolas Falliere, Liam O Murchu, and Eric Chien

While the bulk of the analysis is complete, Stuxnet is an incredibly large and complex threat. The authors expect to make revisions to this document shortly after release as new information is uncovered or may be publicly disclosed. This paper is the work of numerous individuals on the Symantec Security Response team over the last three months well beyond the cited authors. Without their assistance, this paper would not be possible.

Contents

- Introduction 1
- Executive Summary 2
- Attack Scenario 3
- Timeline 4
- Infection Statistics 5
- Stuxnet Architecture 12
- Installation 16
- Load Point 20
- Command and Control 21
- Windows Rootkit Functionality 24
- Stuxnet Propagation Methods 25
- Modifying PLCs 36
- Payload Exports 50
- Payload Resources 51
- Variants 53
- Summary 55
- Appendix A 56
- Appendix B 58
- Appendix C 59
- Revision History 68

Introduction

W32.Stuxnet has gained a lot of attention from researchers and media recently. There is good reason for this. Stuxnet is one of the most complex threats we have analyzed. In this paper we take a detailed look at Stuxnet and its various components and particularly focus on the final goal of Stuxnet, which is to reprogram industrial control systems. Stuxnet is a large, complex piece of malware with many different components and functionalities. We have already covered some of these components in our [blog series](#) on the topic. While some of the information from those blogs is included here, this paper is a more comprehensive and in-depth look at the threat.

Stuxnet is a threat that was primarily written to target an industrial control system or set of similar systems. Industrial control systems are used in gas pipelines and power plants. Its final goal is to reprogram industrial control systems (ICS) by modifying code on programmable logic controllers (PLCs) to make them work in a manner the attacker intended and to hide those changes from the operator of the equipment. In order to achieve this goal the creators amassed a vast array of components to increase their chances of success. This includes zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion

Military Analyst. Malicious Insider.



Bradley Manning

All About Protecting Data from Loss and Breach

Keeping out of the Headlines

- 46 U.S. states now have mandatory data breach notification laws

Avoiding Escalation and Lost Business Costs

- An average data breach costs \$214/record in the U.S., £64/record in the U.K., and €138 in Germany

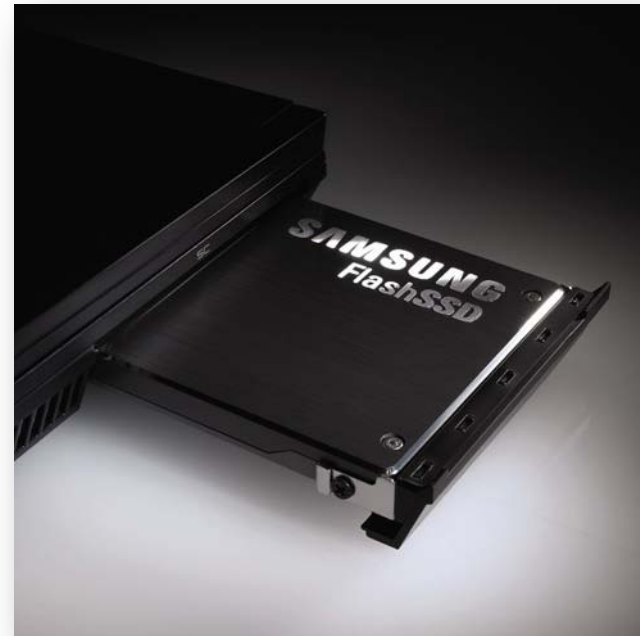
Avoiding Government Fines and Criminal Charges

- \$1.5M – HITECH Act maximum fine by U.S. HHS and FTC
- £3M – HSBC fined by U.K. FSA
- £500K – U.K. Data Protection Act (ICO) maximum fine

Avoiding Lawsuits

- \$1,000+/customer/breach – Massachusetts and Nevada encryption laws

Self-Encrypting Devices: Part of the Solution



Information-Centric Security is Required



AWARENESS

- Where is the sensitive data?
 - How is it being used?
-



IDENTITY

- Who should have access to sensitive data?
 - Who shouldn't have access?
-



PROTECTION

- How to enforce data policies?
 - How to prevent breach?
-

Information-Centric Approach



AWARENESS

Content- and Context-Aware DLP



IDENTITY

User Identification and Authentication



PROTECTION

Storage Encryption



Messaging Encryption



Device Encryption





Questions

