Securing the Internet of Things

NG Kai Koon

Director, Government Affairs

Threats to IoT are Real & Current!

Researchers Find New Point-of-Sale Malware Called BlackPOS

Lucian Constantin | March 28, 2013

Researchers Describe New Air-Gap Threat
Demonstrate How Smart Phones Could Be Used to Grab Data

By Matthew J. Schwartz, October 30, 2014

Digitally signed malware is increasingly prevalent

Malware authors are signing their malicious creations with stolen digital certificates to bypass antivirus detection and defense mechanisms

By Lucian Constantin, IDG News Service
March 15, 2012 02:40 PM ET

Sednit Espionage Group Attacking Air-Gapped Networks

BY JOAN CALVET POSTED 11 NOV 2014

How Safe Is Your Quantified Self? Tracking, Monitoring and Wearable Tech
Self-tracking enthusiasts are generating a torrent of personal information through apps and devices. Is this data safe from prying eyes?

By Symantec Security Response, July 30, 2014

Boffins Finds Hundreds of Thousands of Woefully Insecure IoT Devices

By Darren Pauli, 17 August 2014

Owners of Heatmiser WiFi Thermostats Warned of Password Leaks and Other Vulnerabiities

Graham Cluley | September 23, 2014

Smart Meters Can Be Hacked to Cut Power Bills

By Mark Ward, BBC News, October 16, 2014

2

Ploutus – 2013

Symantec Official Blog

Criminals Hit the ATM Jackpot

By: **Daniel Regalado** SYMANTEC EMPLOYEE

Created 11 Oct 2013

0 Comments   Translations   Share

It's well-known that organized crime in Mexico is always finding new ways to steal money from people. Automatic teller machines (ATMs) are one of the common targets in this effort, but the challenge there is actually getting the money out of the machine. The three most common ways to accomplish this are:

Backoff – 2014

Darlloz – 2014

Symantec Official Blog

IoT Worm Used to Mine Cryptocurrency

By: **Kaoru Hayashi**

Created 19 Mar 2014

0 Comments   Translations   Share

Last November, we found an Internet of Things (IoT) worm named Linux.Darlloz. The worm targets computers running Intel x86 architectures. Not only that, but the worm also focuses on devices running the ARM, MIPS and PowerPC architectures, which are usually found on routers and set-top boxes. Since the initial discovery of Linux.Darlloz, we have found a new variant of the worm in mid-January. According to our analysis, the author of the worm continuously updates the code and adds new features, particularly focusing on making money with the worm.

'Ransomwear' – Coming to a Watch near you

An Architecture of Risk

Securing across the IoT Space

Generate Data

Aggregate Data

Manage devices, Store and Analyze Data

Sensors	Devices	Network	Backend Systems

PLCs

Instrumentation

Gateways

Content Servers
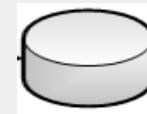
Centralized Database

Identify and Protect my device	Secure my network	Identify threats	Provide unified security view	Ensure compliance
Ensure only trusted apps run	Identify the assets	Prevent data leakage	Protect my data center	
Ensure data is not tampered	Identify anomalies to investigate	Manage devices and apps	Extract Data from devices	Vertical Specific Apps

- Low processor devices
- Regular security updates not possible
- Legacy devices
- Different platforms

- Proprietary protocols

- Privacy of data
- Data quality not always high

Q&A

Thank you!

NG Kai Koon

kaikoon_ng@symantec.com
+65 9002 0214