insignary

(In)secure Things

How to lower costs and manage risk around Open Source in IoT

Open Source is Everywhere

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

78%

78% of surveyed companies run on Open Source and less than 3% do not use Open Source in any way.

Reference: Black Duck 2015 Future of Open Source Survey

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

89%

89% of surveyed companies said that Open Source impacts the speed of innovation and improves time to market for new products.

Reference: Black Duck 2015 Future of Open Source Survey

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

What’s the catch?

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Open Source and Security

There have been significant vulnerabilities discovered in widely used Open Source.
Each was present in applications tested using static and dynamic tools for years without being detected.
The issues were disclosed by security researchers conducting manual code reviews.

	Heartbleed	Shellshock	Freak	Ghost	Venom
Since :	2011	1989	1990's	2000	2004
Discovered :	2014	2014	2015	2015	2015
Component :	OpenSSL	Bash	OpenSSL	GNU C Library	QEMU

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Dirty Cow – A Threat To The Kernel

This vulnerability has been present in the Linux kernel since version 2.6.22 in 2007 and is easy to exploit.

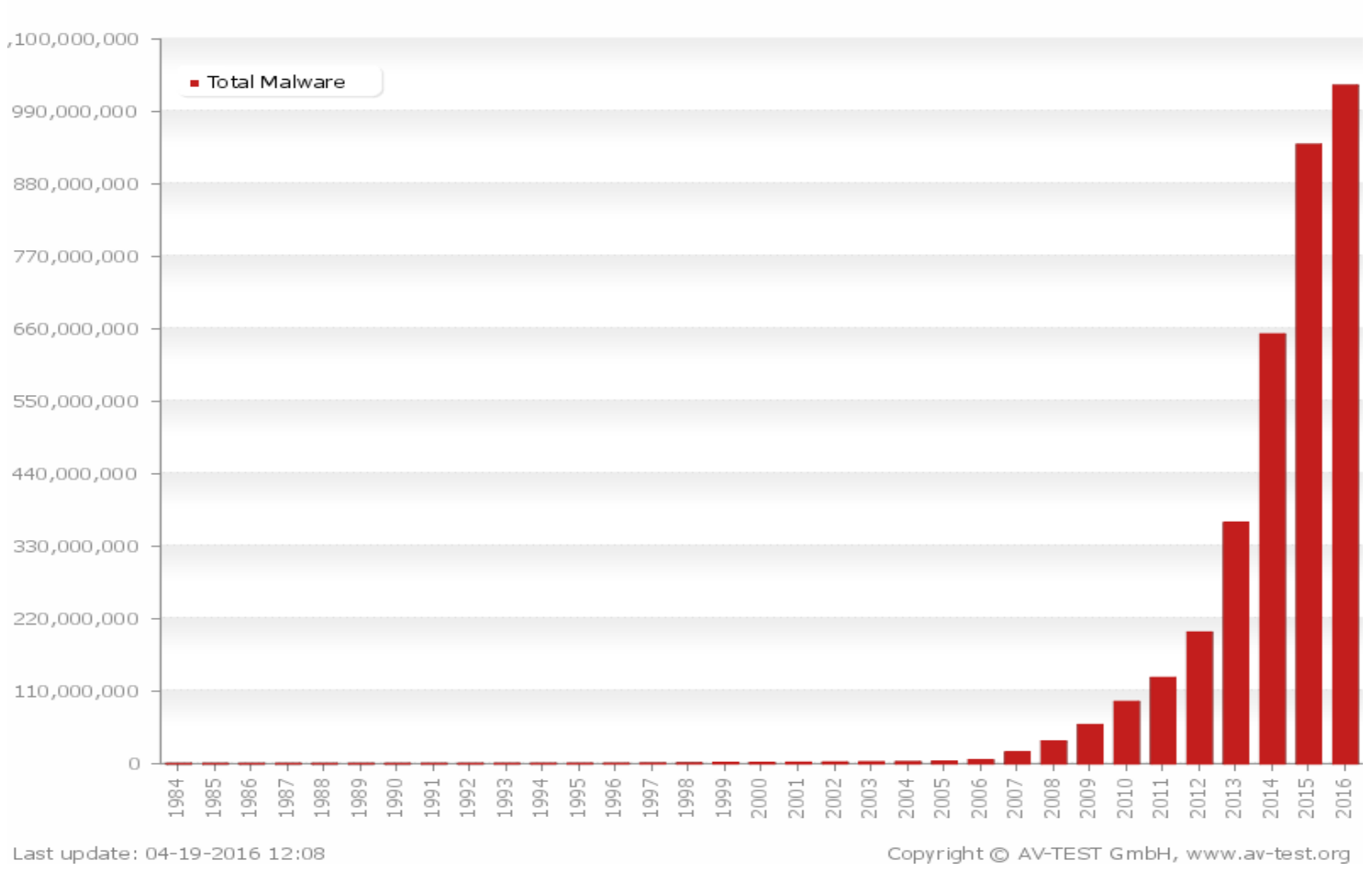
It is also present in Android.

Exploit code to gain control of devices is already being used against internet-facing systems.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

This Matters



Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

“Through 2020, security and quality defects publicly attributed to OSS projects will increase significantly, driven by a growing presence within high-profile, mission-critical and mainstream IT workloads.”

Gartner, Road Map for Open-Source Success: Understanding Quality and Security, Mark Driver, 3 March 2014.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

The DROWN attack left more than 11million websites using OpenSSL at risk.

http://thehackernews.com/2016/03/drown-attack-openssl-vulnerability.html

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

IoT breaches expose infrastructure.

Example: a transport informtion screen was hacked in Korea to display pornography.

http://m.chosun.com/svc/article.html?sname=news&contid=2016042601303

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Open Source Security is a big deal

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

What Do We Do?

There are a lot of process documentation and tooling options available for Open Source licensing compliance.

We are only starting to see the emergence of similar process documentation and tooling for Open Source security.

Most companies do not use any yet.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

67%

67% of surveyed companies said that they do not monitor Open Source Code for security vulnerabilities

Reference: Black Duck 2015 Future of Open Source Survey

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

The Big Picture

What will happen next regarding Open Source and Security?

The Community Evolves

This is not something that can be neglected.

Critical areas like IoT, automotive and Smart Infrastructure need security to be a first-class citizen.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

The Community Adapts

The global Open Source community has dealt with improving processes and tooling before. Let's talk compliance.

The basic approach is to collaborate to create deliverables:

1. Identify the core problems
2. Decide what needs documenting (processes)
3. Decide what can be automated (tooling)

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

It Starts With Deployment Processes

This is about managing your supply chain

OpenChain is the Open Source Supply Chain Process Specification

- OpenChain formally launched on the 4th of October with an awesome keynote speech from Jilayne Lovejoy from ARM.
- Check it out here: www.openchainproject.org

OPENCHAIN

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Great Processes are Supported by Great Training Materials

- OpenChain has a curriculum committee that released a set of slides under CC-0 licensing to help everyone integrate compliance best practices into their organization, regardless of size.
- Check them out here: https://wiki.linuxfoundation.org/openchain/curriculum

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Then You Need an Update Process

There will always be errors to fix

Update Processes Go Far Beyond Features

- Software will always have bugs.
- Whether you are deploying a lightbulb, a car or a smart home, part your security process needs to include lifecycle management.
- This area is still immature in compliance and security areas.
- For mobile devices pushing updates is relatively easy. However, there are challenges for large infrastructure deployments, for automotive systems and for billions of connected IoT devices.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

The Next Step is Automation

Humans can only do so much

Automation Supports Compliance Teams

- Automation usually comes in the form of tools to check source code or binary code in your supply chain and meet process requirements.
- For example, some tools help companies confirm their source code has the correct licensing.
  - Examples include FOSSology and Black Duck ProTex
- Other tools may help to identify issues in binary code.
  - Examples include the Binary Analysis Tool (BAT) and Insignary Clarity

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

What Is Coming Next?

Wishlist

- Security as a first class citizen in Open Source supply chain management
- Freely available materials to help support security training and process management
- A selection of projects and commercial solutions dedicated to helping address the challenge of Open Source security in deployment processes, update processes and automation.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Case Study: The Binary Analysis Tool

An Open Source Project for Open Source binary analysis

Technology

BAT uses symbol and string table comparisons (fingerprinting) to read binary code in firmware and compare it to source code without undertaking any reverse engineering.

It works by (1) extracting binary files from firmware, (2) locating identifiers such as strings, function or variable names to compare against a database of Open Source code and (3) using other information such as file names and package databases to increase fidelity.

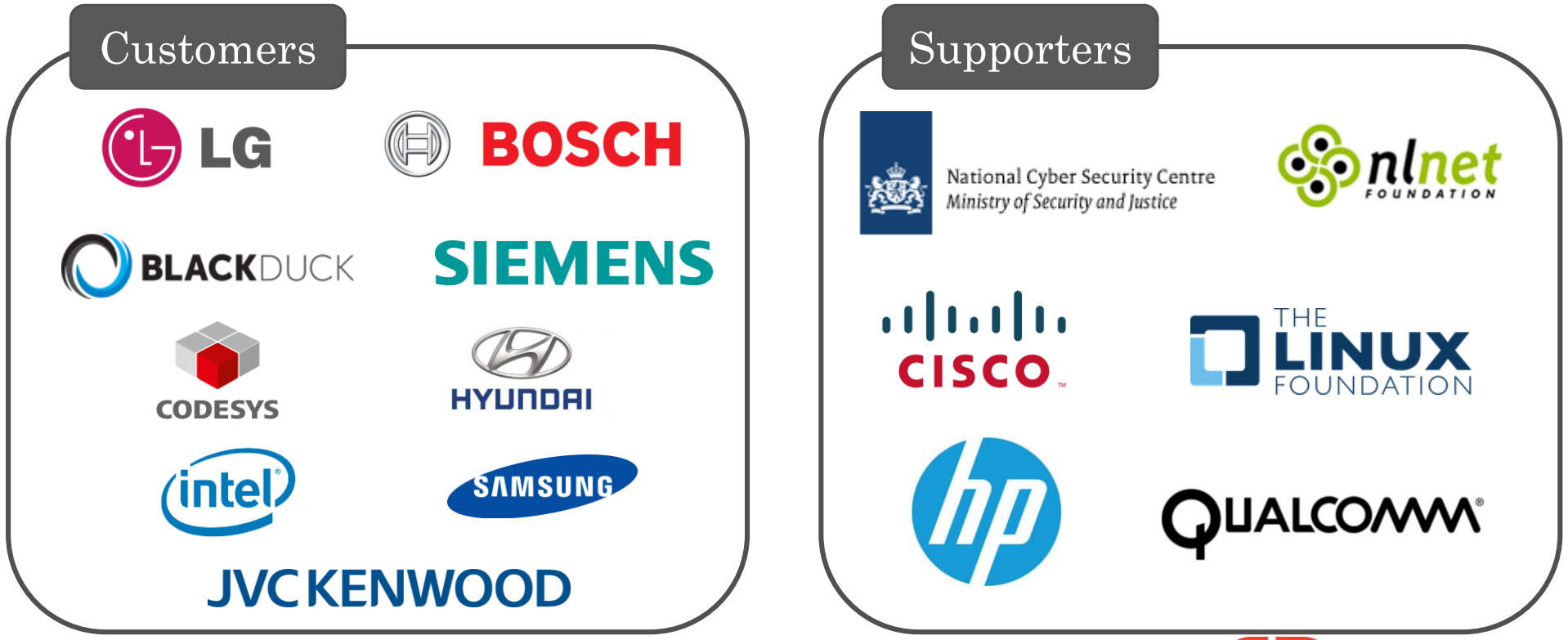
This is effective in discovering real-world Open Source issues. It can help monitor supply chains by automatically identifying Open Source code in firmware.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Customers and Supporters

The Binary Analysis Tool (BAT) framework underlying our technology has been widely adopted and supported across the technology industry.



Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Go Follow the Code

The BAT Project website:

- http://www.binaryanalysis.org

The GitHub repository:

- https://github.com/armijnhemel/binaryanalysis/commits/master

The BAT Project will soon be part of the NLnet Foundation Commons Conservancy. This will ensure it remains a sustainable, independent Open Source project.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

About Insignary Clarity

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

High Level Overview

Insignary Clarity is a next generation evolution of the BAT framework. It increases the fidelity, data sources and usability of BAT for cloud or on-site deployment. This provides an easy upgrade path for existing users and simplified adoption for new users.

Insignary Clarity helps companies identify, prioritize and address potential Open Source issues in the supply chain. It helps provide company security and compliance teams with increased confidence in the deployment of Open Source products and solutions.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

We Are Not Alone

Check out Black Duck Hub and other commercial tools for other types of binary analysis.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Security is what you make of it

Open Source is the same as any other software if used without good processes and best practices.

With good processes and best practices Open Source can be more secure than anything else

.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Improved Security in Open Source is Coming

You can expect more best practices for generic Open Source security, specific material to address development problems, and other material to assist with supply chain challenges.

On the tooling side you can expect the emergence of a range of solutions to support requirements. We have already seen the beginning of this from both security vendors and companies that traditionally focused on license compliance issues.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Open Source has some security challenges

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

It is still as secure as proprietary software

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

It will get even better over time

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

Be part of the solution

Support the Core Infrastructure Initiative, help shape the OpenChain specification, share some of your best practices with the community.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.

insignary

We Need Three Things:

1. Deployment Processes
2. Update Processes
3. Automation

Let’s Talk

Email me at shane@insignary.com to discuss OpenChain, compliance, se curity and supply chain management.

Naturally I’m also happy to tell you more about Insignary and what we do.

Copyright © 2016 Insignary Inc. Not for redistribution without written permission.