SAND2018-7821C

The Center for Cyber Defenders

Expanding computer security knowledge

Time-to-Discovery

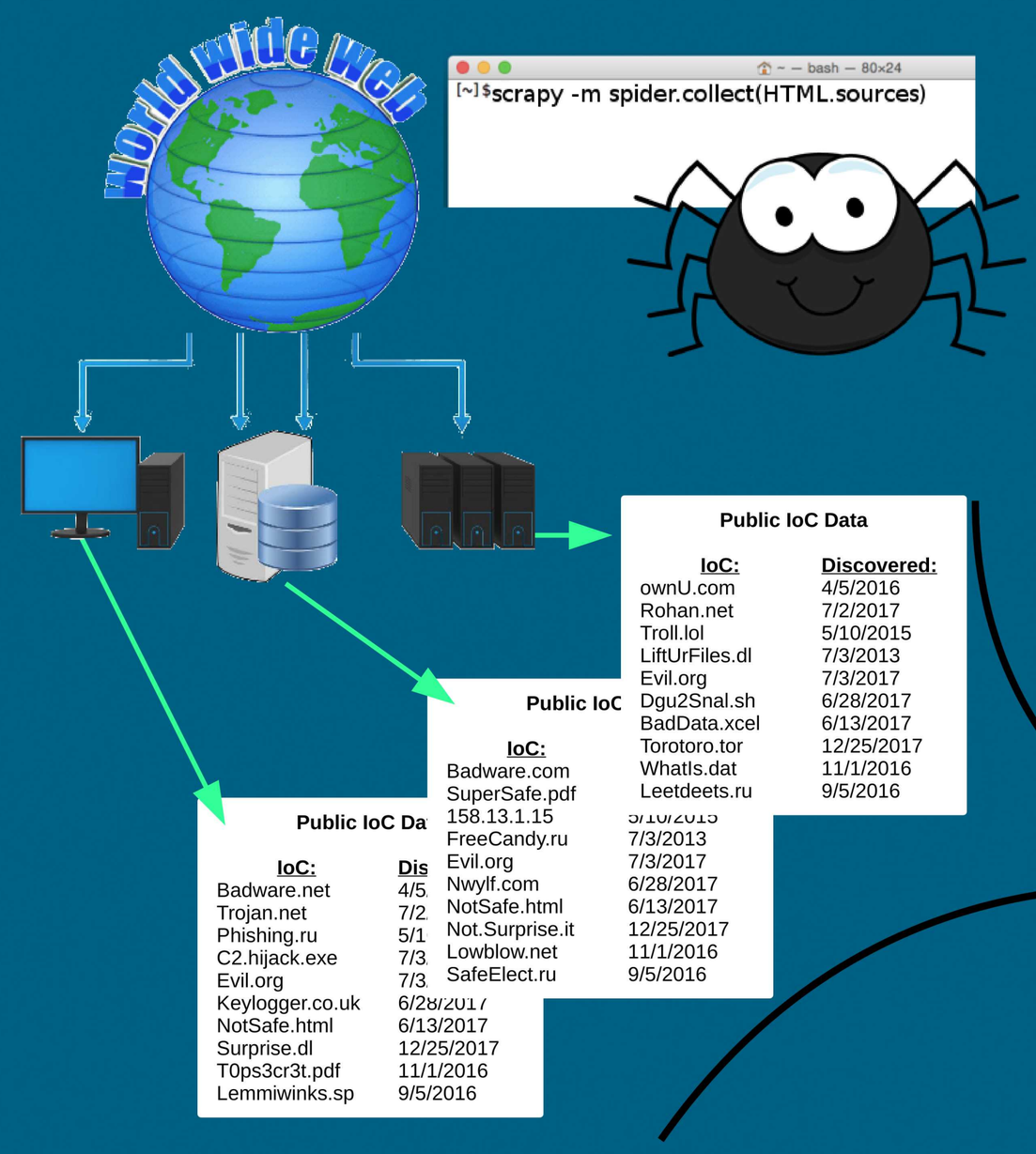
Testing efficiency with open-source data

Michael Symonds, Roy Nehoran

Project Mentors: Steve Hurd, Elijah Agbayani

Problem Statement:

When someone tries to attack a network, a security system can catch the malicious network traffic, preventing it from infecting the network and the users connected to it. When such traffic is discovered, the data about each attack is classified and remembered, which we call an **Indicator of Compromise**, or **IoC**.

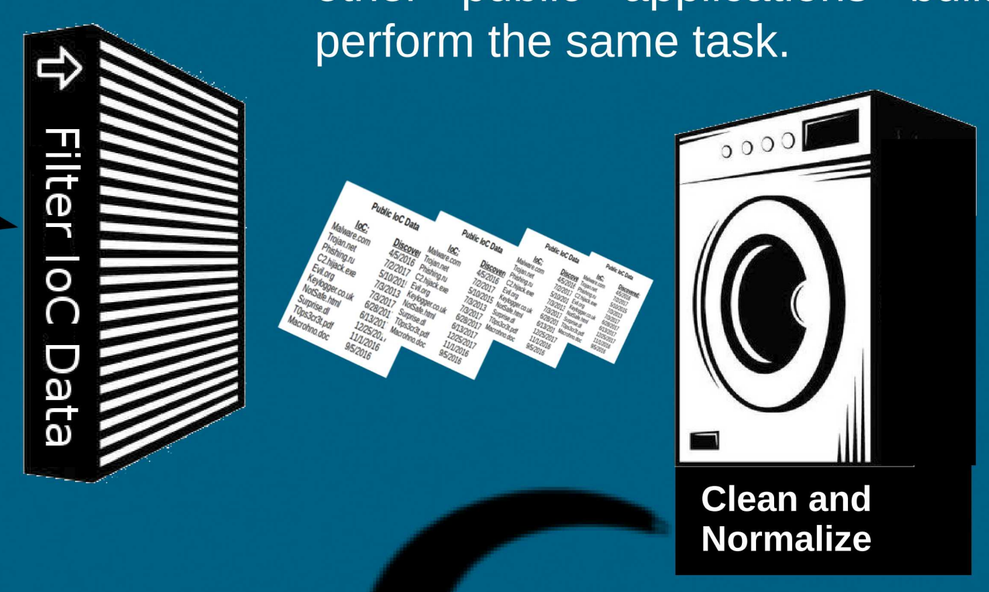


Captured IoC Data

IoC:	Discovered:
Malware.com	4/5/2016
Trojan.net	7/2/2017
Phishing.ru	5/10/2015
C2.hijack.exe	7/3/2013
Evil.org	7/3/2017
Keylogger.co.uk	6/28/2017
NotSafe.html	6/13/2017
Surprise.dl	12/25/2017
T0ps3cr3t.pdf	11/1/2016
Macrohno.doc	9/5/2016

A Network Security System

The security system may be very good at discovering IoCs, but there needs to be a way of measuring just how effective it can be. One of the best ways to do this is to compare how fast the system in question can catch IoCs before they're caught by other public applications built to perform the same task.



Our Approach:

One strategy for solving this is to collect all of the publicly available IoC data on the Internet, along with the date for when they were first discovered, into a single source. We can then compare the "first discovery" times of each IoC with those of any same IoC that the security system we want to test has also found. If the security system discovered them first, or it has IoCs that are not even yet known to the public, this is a strong indication of the effectiveness of the security system.

PUBLIC DATA		SECURITY SYSTEM DATA		
IoC:	Discovered:	IoC:	Discovered:	
Badware.com	3/9/2017	Malware.com	4/5/2016	✗
Trojan.net	8/1/2017	Trojan.net	7/2/2017	✓
Phishing.xxx	5/10/2015	Phishing.ru	5/1/2015	✗
C2.hijack.exe	7/3/2014	C2.hijack.exe	7/3/2013	✓
Evil.org	7/7/2017	Evil.org	7/3/2017	✓
Nwylf.com	4/6/2018	Keylogger.co.uk	6/28/2017	✗
NotSafe.html	6/13/2017	NotSafe.html	6/13/2017	✓
Not.Surprise.it	3/6/2009	Surprise.dl	12/25/2017	✗
T0ps3cr3t.pdf	11/1/2016	T0ps3cr3t.pdf	11/1/2016	✓

This project is focused on the collection and organization of the publicly available IoC data. Our application continuously collects IoC data daily from dozens of public sources, with careful attention to when each indicator was first discovered and the strength of each source. The strength of a source can be measured by how many new IoCs are collected daily from the source, which of them are false positives (IoCs which aren't really "bad actors" after all), and how much information is collected about them. We channel that collected data to a central database where other teams can then compare what we found to the IoC data captured by the security detection system being evaluated.

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration