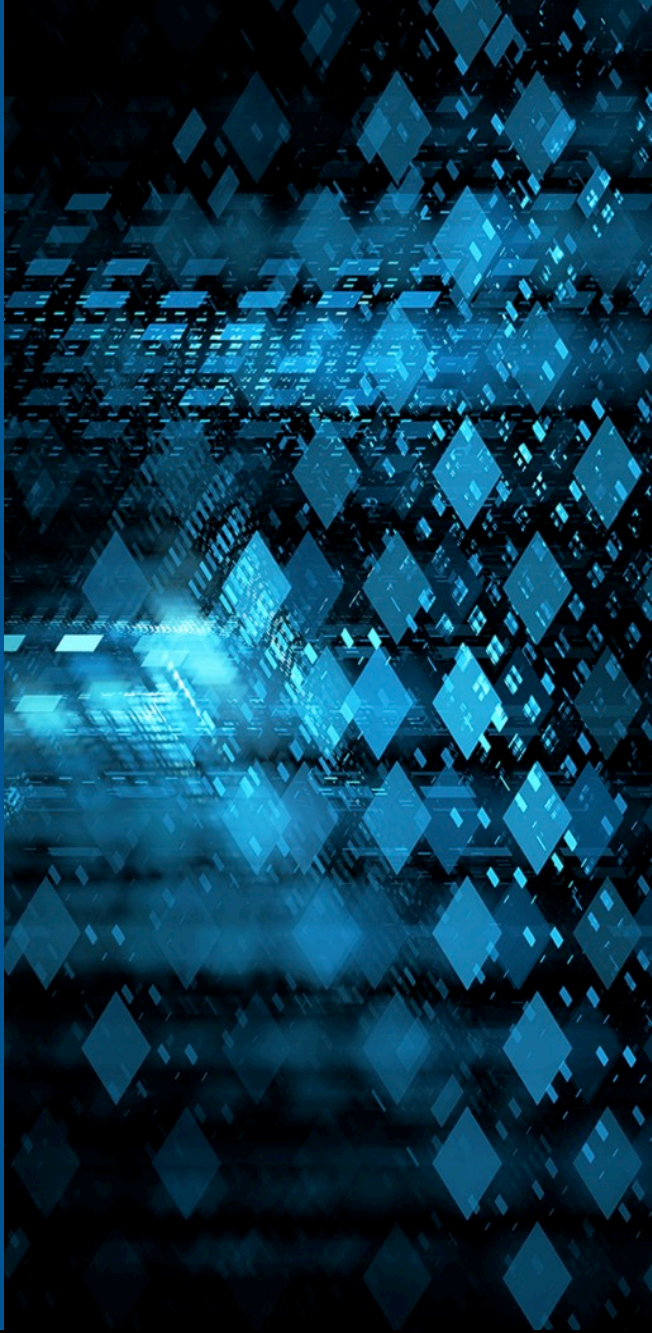
A Unique Approach to Threat Analysis Mapping: A Malware-Centric Methodology to Better Understand the Adversary Landscape

Deana Shick

Kyle O’Meara

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0003530

Software Engineering Institute/CERT Coordination Center (CERT/CC)

- Carnegie Mellon -> SEI -> CERT/CC -> ATA
- Deana Shick
- Kyle O’Meara
- https://github.com/cmu-sei

Motivation

Challenge Problem

- Malware, incident, and network analysts rarely combine efforts
- Researchers and other vendors provide “inside-out” hunting results to the public.
- OSINT is rarely confirmed
- Where to start? Malware efforts

Working From the Outside-In

- Better utilize data at cheap cost to help network defenders and intelligence circles
- Cluster datasets create a more complete picture of CNO
- Starts with understood malware family INSTEAD of incident data alone
- Utilize indicator expansion
- After malware family, the remaining sections are discussed in no particular order

Data Sources and Tools

Data Used (or tried to use)

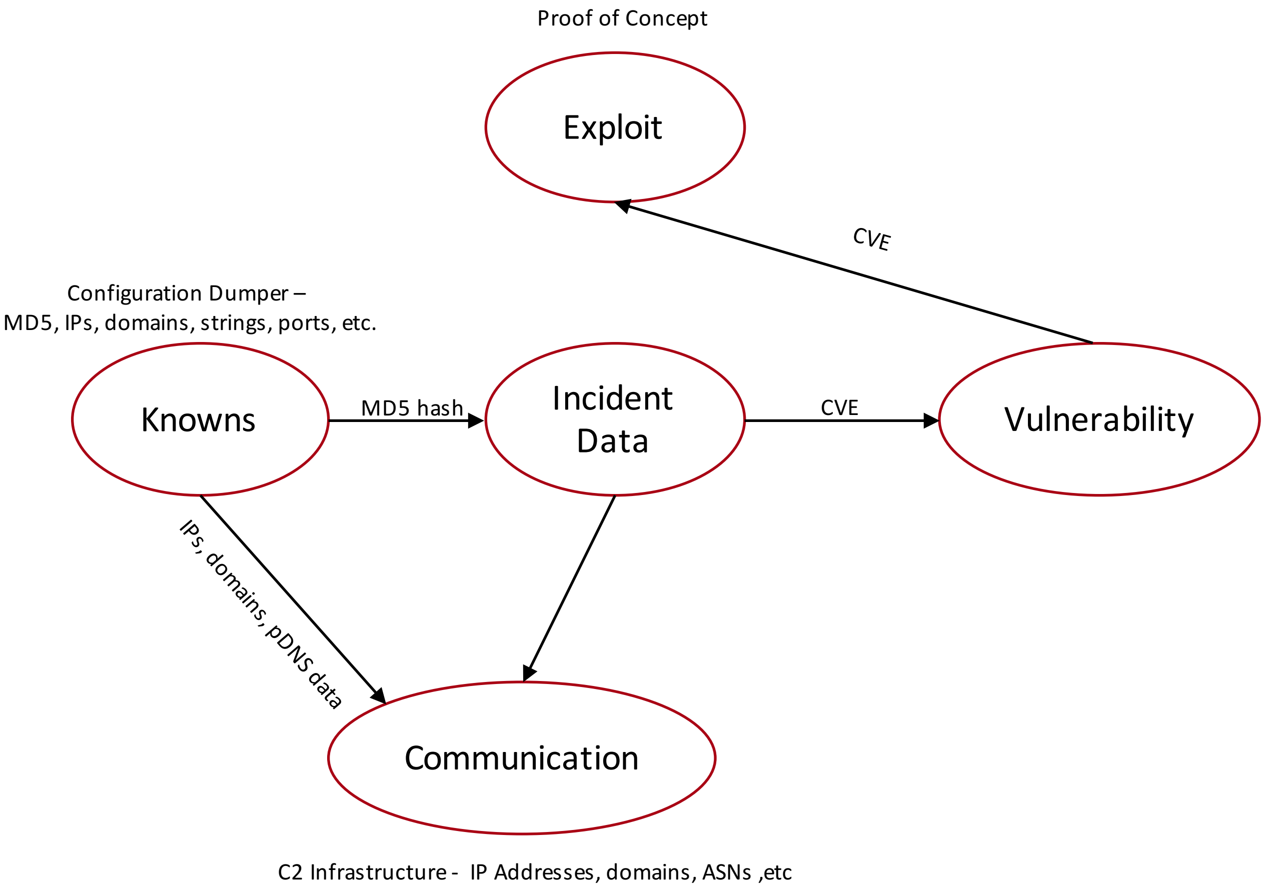
- Malware Family analysis – RE and knowns
- Farsight’s passive DNS (pDNS) – “Indicator Expansion”
- Blacklist Analysis – not helpful
- CVE Database
- Exploit-DB
- Others - Circl.lu MISP, Twitter, Blogs, Vendor articles

Tools

- YARA
- Fn2yara
- System for Internet-Level Knowledge (SiLK)
- Python scripts on a linux system

Methodology

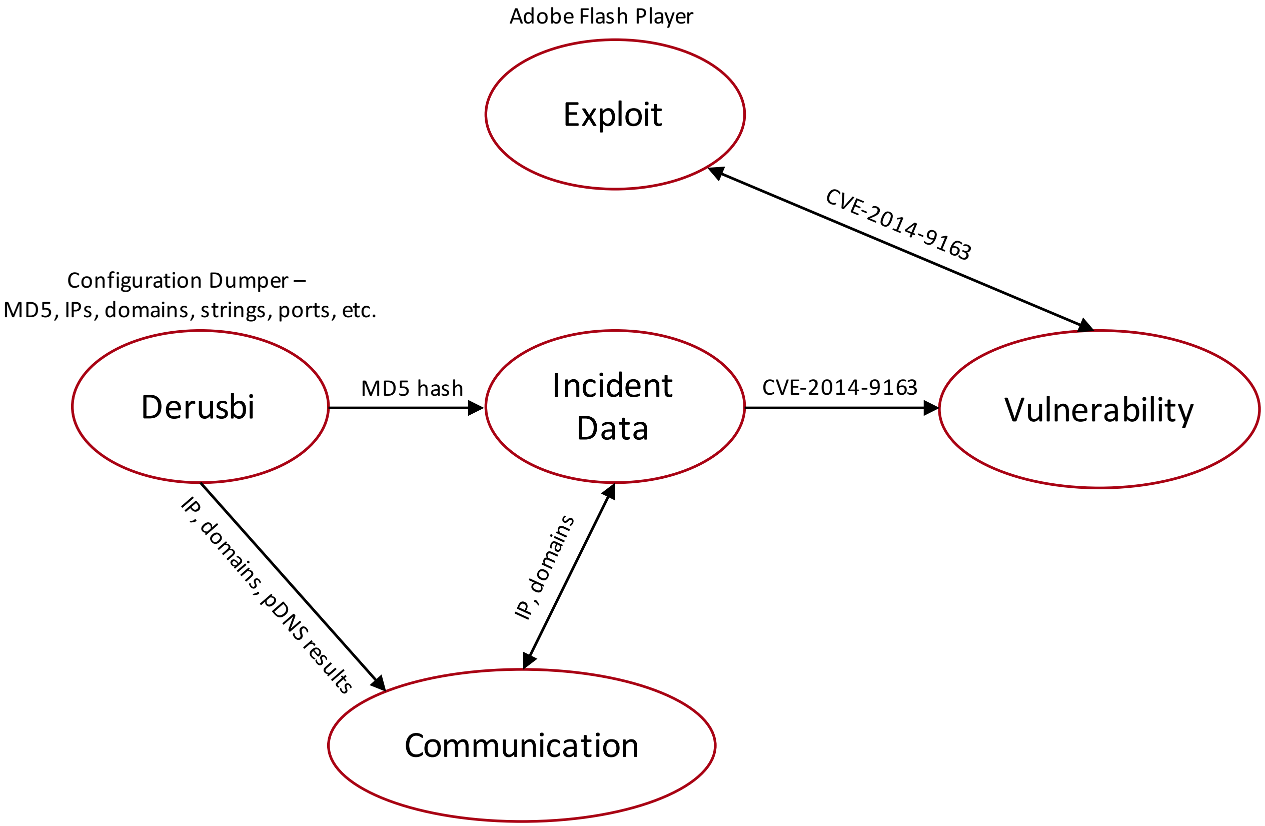
Pivoting Through Data



Results

3 Case Studies: Smallcase, Derusbi, and Sakula

Derusbi Methodology



Derusbi – Background

- At least involved in Office of Personnel Management (OPM), Anthem Health, Forbes.com compromises.

- Most likely developed around 2006
  - Major rewrite in the code

- This malware is NOT C0d0s0 or Briba, contrary to popular belief

Code Comparison

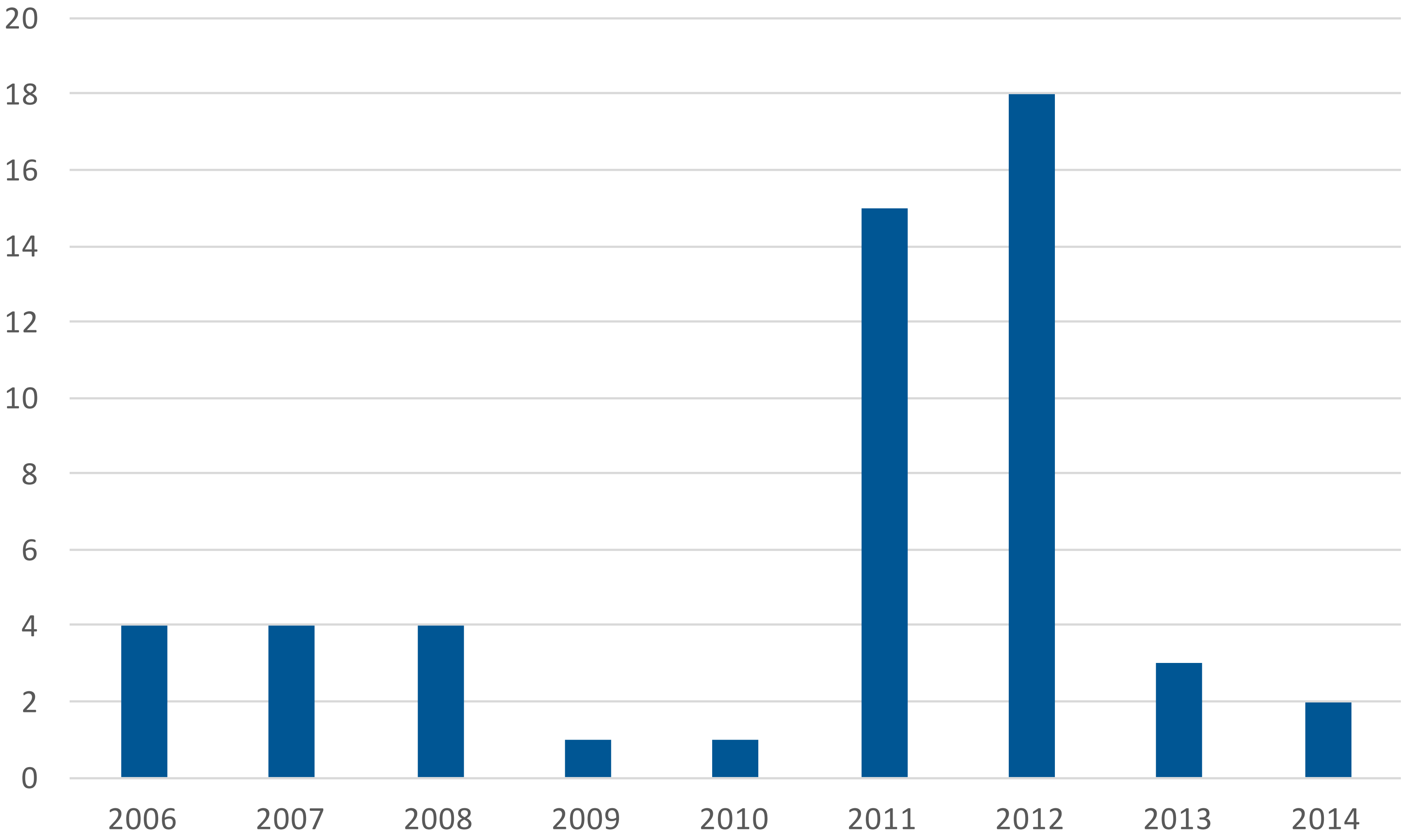
- If OSINT was correct that Briba, C0d0so0, and Derusbi were the same, then this would provide a larger starting point analysis
- Fn2yara Results – Compared 244 Briba files, 25 Codoso files, and 183 Derusbi files
- Derusbi and Codoso shared 2 functions.
  - 1 function was found in 4 of the 183 Derusbi files and the another function was found in 11 of the 183 Derusbi files.
- Derusbi and Briba shared 7 functions.
  - 5 functions were only found in 1 file each of the Derusbi files.
  - 2 functions were only found in 2 files each of the Derusbi files.

Malware Findings

- 112 files as of 1 January 2016 analysis
- 58 unique domain names used for command and control (C2)
- 5 IP addresses
- Ports 53, 80, 443, 1426, 2515, 8080, and 8090
- Notable strings and executables: cia.exe, wininint.exe, lsw.exe, mgame, routeprint, tom.jpg

Derusbi

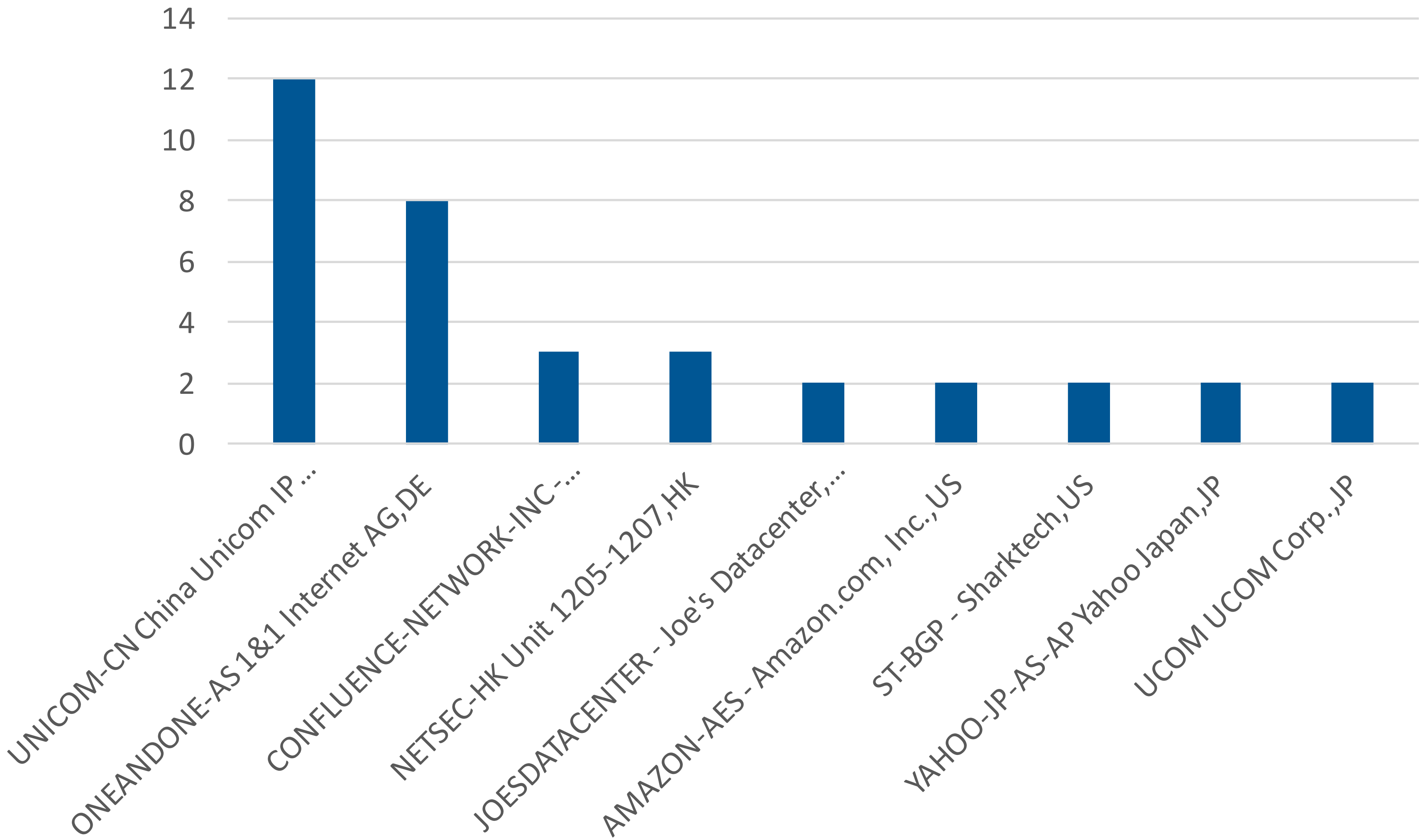
Compile times



Network Data

- 60 unique domain names after indicator expansion
- 50 IP addresses after indicator expansion
- 12 Name Servers
- No data in SOA records
- MX records were variants of yahoo[.]jp

Organizational Analysis



Incident Data

- In 2014, RSA compiled a report detailing the operations of Shell_Crew, also known as Deep Panda, WebMasters, Kung-fu Kittens, and PinkPanther (RSA, 2014).
- The group was active well into late 2015, and was responsible for the Office of Personnel Management (OPM) breach (Hesseldahl, 2015).
- Shell_Crew uses a RAT, a post exploitation tool, and complex kernel level tool as part of its attack platform. The kernel level tool has been tied to Derusbi
- In 2014, Crowdstrike tracked attacks against the Defense Industrial base, healthcare, government, and technology sectors (Dahl, 2016). It was identified that these campaigns were using Derusbi and Sakula families, and were eventually linked to Deep Panda (Dahl, 2016).
- Malware was used alongside Sakula, but there is no indication they are similar.

Vulnerabilities and Exploits

Vulnerability

- Multiple sides to the story
  - Reports show that groups that used Derusbi targeted CVE-2014-9163, CVE-2010-2861, and CVE-2014-6271
    - CVE-2014-9163 – Adobe Flash Player
    - CVE-2010-2861 – Adobe Coldfusion
    - CVE-2014-6271 – Shellshock

Exploit

- Time helps with exploit discovery
- 3 exploit files for CVE-2014-9163
- PoCs for CVE-2010-2861 and CVE-2014-6271 on Exploit-DB
- 14 exploit files for CVE-2014-6271

TL;DR

- Derusbi is associated with APT actors. It is not C0d0s0 or Briba
- Actors used a small network to compromise victim machines including those associated with education networks.
- All infrastructure tied to 12 name servers
- In at least 2 cases, the group exploited zero-day vulnerabilities in Adobe products such as ColdFusion and Flash Player.
- We found at least 3 exploits related to CVE-2014-9163 and 14 related to CVE-2014-6271
- We believe those using the malware will continue compromising products with wide-spread use for the purposes of intelligence gathering.

Future Work

Future Work

- This is only one methodology

- Create additional methodologies to identify the strengths and weaknesses of starting or ending with particular points

- Community gap area is in exploits
  - We are currently developing an ’Exploit Catalog’
  - We are happy to discuss it further offline

Conclusion

Takeaways for you

- Outside-in approach allows you to see more than just 1 aspect of an intrusion
  - Deploy better defenses
  - Create an adversary profile

- What was our goal?
  - Begin with the tools used by adversaries rather than with network or incident data alone.
  - Use the data you have in house to help decision makers

Q & A

Contact Information

Presenter

Deana Shick

Member of the Technical Staff

Telephone: +1 412.268.2279

Email: dshick@cert.org

Twitter: @deanashick

Presenter

Kyle O'Meara

Sr. Member of the Technical Staff

Telephone: +1 412.268.2537

Email: komeara@cert.org

Twitter: @cool_breeze26

Paper

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=453938