Cooperation Suggestion for Detecting Malwares in Websites in AP Region

Sang-yong Choi
Senior Researcher

Korea Advanced Institute of Science and Technology (KAIST)
Cyber Security Research Center (CSRC)
Introduction to
KAIST Cyber Security Research Center
Introduction

- KAIST Cyber Security Research Center (CSRC)
  - Founded in 2011
  - Research and developing core security technologies
  - Produce top-level human resources
    - Graduate School of Information Security (GSIS)
    - S+ Convergence AMP

- Research area
  - Real-time malware analysis system
  - Malware collection/analysis technology
  - Mobile platform security
Vision

• **Make Korea a strong nation in cyber security** by developing core technologies and establishing the anticipatory strategy for cyber attacks

• **Take a key role in national cyber defense** by producing world-class security experts
History

- Feb. 2011: CSRC / GSIS was founded
- Feb. 2013: SIMon was launched
  - Monitoring 420k+ domains
  - Distribute weekly security trend report to 120+ organizations in Korea
- June. 2013: SIMon Software registration
- Aug. 2013: SIMon Patent application

- Produced 290+ talented students through S+ Convergence AMP and Graduate program
- Signed MOU with 6 national agencies, 2 industrial companies
## The Roles

### National Security Control Tower

<table>
<thead>
<tr>
<th><strong>Cheong Wa Dae</strong></th>
<th><em>(The Presidential Office)</em></th>
</tr>
</thead>
</table>

### Research & Development

- National security strategy and policy
- Detect and block a malware distribution
- Analysis and presumption of incident and vulnerabilities by collecting data
- Protect the national critical information infrastructures
- Risk Management Framework

### Awareness, Education & Training

- Graduate School of Information Security
- S+ *(Smart technology, Security, Strategy)* Convergence Advanced Management Program
- Advanced information security technology

### Services & Monitoring

- CERT/CC of Educational and Research organizations

---

**Private, Public and Governments for secure Cyber Korea**
SIMan: Suspicious Information Monitoring System for Websites & Malware Distribution Trends
Virtualized Agent Cluster

• Web crawling
• Multi-level emulator
• Highly scalable

Manager / Database server

• Agent management
• Website scheduling
• Task history management

Web User Interface

• Statistics visualization

Architectural Diagram

 KAIST Cyber Security Research Center

- 8/19 -
Key features

• **Scalable detection range**
  • Traversing 420k+ websites (currently)
  • Fitting in with any size of business

• **Intensive webpage analysis**
  • Multi-level emulation
  • Signature- / Behavior-based analysis

• **Manageable agent pool**
  • Running VM-based agents on high-performance servers
Achievements

• **Patent application (Korean):**
  • **Title:** Apparatus and Method for Monitoring Suspicious Information in Web Page
  • August, 2013.

• **Software registration (Korean):**
  • **Title:** SIMon: Suspicious Information Monitoring system in Website
  • June, 2013.
Malware Trends

• Drive-by Download Attack using vulnerable website

Monitoring

The first half year (2013)
### Malware Detection

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Watering hole</th>
<th>Normal Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single vulnerability</td>
<td>Exploit code injected into a webpage</td>
<td>Multi vulnerability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Watering hole</th>
<th>Normal Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive-by Download</td>
<td>Stop free anti-virus S/W service(V3 Lite, Alyac)</td>
<td>Stop commercial anti-virus S/W service(V3 365)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attack</th>
<th>Watering hole</th>
<th>Normal Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop periodically download malware</td>
<td>Stop real-time communication</td>
<td></td>
</tr>
</tbody>
</table>

- **2013.2**: Detecting and alerting “Watering hole attack”
Malware Detection

- 2013.6 : Detecting and alerting “Phishing Attack for Banking Site”
Malware Analysis

- 2013.3 : Analysis of malware used “3.20 Cyber Terror” & reporting
• Weekly security issues, Malware distribution trends & analysis
Cooperation Suggestion
for Detecting Malwares in Websites in AP Region
Toward Secure Web in AP Region

• Web-based malware becomes a top security threat
  • Especially, drive-by download attack

• Whole AP region already has been the target of various attacks

• SIMon can be extended to monitor/analyze wider region
  • Customized SIMon for your interests
  • Publish security trend report for AP Region

• Collaborative effort can effectively build the secure web environment
  • We are always welcome any requests and suggestion!
Thank you

Any suggestions or requests are welcome!

csrc@kaist.ac.kr