Distributed Trust Management and Rogue AV Software

Angelos D. Keromytis
Columbia University
**Report Documentation Page**

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

| 1. REPORT DATE | JUN 2010 |
| 2. REPORT TYPE |  |
| 3. DATES COVERED | 00-00-2010 to 00-00-2010 |
| 4. TITLE AND SUBTITLE | Distributed Trust Management and Rogue AV Software |
| 5a. CONTRACT NUMBER | |
| 5b. GRANT NUMBER | |
| 5c. PROGRAM ELEMENT NUMBER | |
| 5d. PROJECT NUMBER | |
| 5e. TASK NUMBER | |
| 5f. WORK UNIT NUMBER | |
| 6. AUTHOR(S) | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | Columbia University, 2920 Broadway, New York City, NY, 10027 |
| 8. PERFORMING ORGANIZATION REPORT NUMBER | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | |
| 10. SPONSOR/MONITOR’S ACRONYM(S) | |
| 11. SPONSOR/MONITOR’S REPORT NUMBER(S) | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT | Approved for public release; distribution unlimited |
| 14. ABSTRACT | |
| 15. SUBJECT TERMS | |
| 16. SECURITY CLASSIFICATION OF: | |
| a. REPORT | unclassified |
| b. ABSTRACT | unclassified |
| c. THIS PAGE | unclassified |
| 17. LIMITATION OF ABSTRACT | Same as Report (SAR) |
| 18. NUMBER OF PAGES | 59 |
| 19a. NAME OF RESPONSIBLE PERSON | |

Standard Form 298 (Rev. 8-98) 
Prescribed by ANSI Std Z39-18
DTM – Motivation

• Distributed system defenses built as “islands”
  – Forced to make assumptions re: topology, other defenses …
    • Locally correct, globally incorrect security enforcement
  – Assumptions fail or are exploited by attackers!

• Our work is motivated by real security incidents experienced first hand
  – “Pushing Boulders Uphill: The Difficulty of Network Intrusion Recovery”

• DTM forces these assumptions in the open, allowing systems to verify them continuously
Overall Approach

• Define policies that take into consideration system-wide context
  – Extend security mechanisms to emit contextual information (continuous or event-based)
  – Distribute information to interested components
• Integrate IDS/ADS, access control, reaction
• Challenges:
  – Accuracy (extracting data from noise)
  – Complexity (defining policies)
  – Performance (scale with users, system, events)
ARACHNE is a system for the coordinated distribution and evaluation of a system-wide policy on different nodes
- Several prototype systems for enterprise-level security have been developed

GOAL: Integrate a variety of different, diverse security mechanisms and policy expression methods
- Achieve enhanced protection over any individual method
- Allow exchange of information between different mechanisms (Eliminate the possibility of “locally correct” but globally wrong decisions)
- Capture trade-offs between amount of global context, scalability, etc.
Specific Tasks (Years 1-3)

• Develop language for expressing DTM policies

• Design DTM architecture
  – ”Asynchronous Policy Evaluation and Enforcement”

• Collaborative/Distributed policy enforcement
  – ”F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services”
  – ”Path-based Access Control for Enterprise Networks”
Contributions

• Framework for integrating all types of defenses
• Proof of feasibility
  – Prototype, preliminary performance, security analysis
• Initial exploration of design options
• Education (GRA training, coursework integration)
• Outreach
  – Tech transition to the government (operations)
Future Directions

• Continue work on refining architecture and system
  – Explore performance/scalability, effectiveness, overhead tradeoffs

• Integrate with QTM
  – Particularly important in federated systems (e.g., dynamically composable SOAs)

• Investigate the use of reactive mechanisms
  – Global coordination of dynamic defenses
Expected Contributions in Years 4 & 5

• Proof of feasibility
  – *Experimentation in real environment*

• Exploration of design and implementation space

• Use of active defenses and deceit
  – *Can we challenge attackers’ (trust) assumptions?*
Outreach and Education

• Integrated material into COMS W4180 course
• 2 invited talks (beyond conference talks) and 1 panel
• Main Ph.D. GRA now working for NSA (R23)
Work on Rogue AV Campaigns

- Working with Symantec to determine modus operandi of rogue AV sites (and why users trust them)

"Gone Rogue: An Analysis of Rogue Security Software Campaigns"

“An Analysis of Rogue AV Campaigns”
Kerik Pledges Guilty, and Faces 27 to 33 Months in Jail
By SAM DOLNICK 38 minutes ago
Bernard B. Kerik, the former New York police commissioner, will be sentenced in February for tax fraud and making false statements.

Insider Trading Charges for 14, Some Tied to Galleon
By ALEX BERENS 28 minutes ago
Federal prosecutors charged 14 hedge fund employees, lawyers and other investors in criminal complaints that all appear to be connected to charges already filed against Raj Rajaratnam.

On the Hill, Protesters Chant ‘Kill the Bill’
By DAVID HERSZENHORN 23 minutes ago
Thousands of demonstrators surfaced on Capitol Hill in opposition to the Democrats’ health care legislation.

Making Health Care Better
By DAVID LEONHARDT
The evidence-based medicine practiced at Intermountain

1,063.53 9,828.08 2,101.16
+17.13 +17.94 +45.64
+1.64% +1.84% +2.22%
[JavaScript Application]

Warning!!! You should install security software! Cyber Security is a good solution for your security, virus protection and spyware remover.

OK
Cancel
System errors detected. To prevent data lost system scanning is started

Scanning...

Object: C:\WINDOWS\system\esentprf.ini

Hardware and security errors detected

Hardware errors
Performance of your PC is low due to a file system error. It was caused by the changes malicious software made in your system files and numerous open ports used by spyware to transfer your privacy data. Your personal data safety in danger.

Privacy information errors
Spyware has stolen your personal information.
You can see the contents of the stolen block below:
Country: France
City: Paris
IP Address: 193.55.113.196
Software Secured Order

- **WIN PC® Defender 6 Months License**
  - Subscription includes new version updates, definition updates, standard customer support for 6 Months.
  - For only $49.99.

- **WIN PC® Defender 1 Year License (Recommended)**
  - Subscription includes new version updates, definition updates, standard customer support for 1 year.
  - Only today limited offer with special discount $63.21 $69.99.

- **Lifetime UNLIMITED License, Best Choice!**
  - WIN PC® Defender - protection software with new generation engine, protect yourself and never worry about your PC with our unlimited package with free VIP Support.
  - Today with special discount for only $438.21 $99.99!

Your order is 100% risk free with our 30 Day Money Back Guarantee!
Antivirus 2009 Professional This not only a scam..IT IS A VIRUS !! Windows Security had to clean the system, took 18 hrs to remove the virus. DO NOT INSTALL THIS PROGRAM, REGARDLESS OF WHAT THE "POP-UPS" TELL YOU !! Internet Antivirus 2009 Professional

Antivirus 2009 IS a virus. It appears on your log in page and will continue as "pop up" giving you dire warnings about your computer's vulnerabilities. Don't believe it! Go back to your start menu and contact your system's security center. It took Windows almost 2 days to determine the source, then resolve it.

I also will now have to go to the bank and cancel my card. There are hidden charges, and will appear as $109.82. And you cannot print the confirmation, it freezes your system completely!

Don't be tricked into this as many of us have....contact Windows, Microsoft, BEFORE you install anything. They are already aware of this scam.

(And the overlaps and ads from this virus are lude and offensive, so be sure you have your kids check with you if they see the original "warning" that your computer is infected!)

Kate
Poplar Branch, North Carolina
U.S.A.

(Courtesy of http://www.ripoffreport.com/)
Rogue AV

- Misleading application
- Pretends to be legitimate security software, such as an anti-virus scanner
- Offers little or no protection
- Often facilitates installation of same malware it pretends to protect from
How “little” is too little?

• False alerts only
  – Tens of alerts on freshly installed machine
• “Selective” alerts
  – IE Defender spreads via Zlob malware
  – After installation, it correctly detects Zlob
• “1980-style” alerts
  – Filename, registry path checks
• Sometimes come with EULA…
Have no idea about Spyware?

Spyware, like a virus, is a malicious software planted on your PC by a third party in order to secretly monitor what you do online.

Once your browsing habits are analyzed, you are flooded with endless commercials, popups and spam from inside your PC!

Spyware also dramatically slows down your computer and Internet connection speeds.

Spyware collects your private information and steals your identity, passwords, credit card details and other.

If the answer is “Yes”, then you are probably infected.

1. Your computer has slowed down?
2. Your Internet connection speed has decreased?
3. You get popups and annoying ads when you’re online or even offline?

100% remove of malicious software, viruses, spyware, malware etc.

Protect personal information from phishing.

Environment care program:
$2 dollars from every sale will be sent on saving green forests in Amazonia.

Have more questions?
You can contact us easy via Online Support.

Environmental Story

Fighting viruses, spyware, malware is not only a question of security. Spyware actually abuses your computer, overuses CPU speed, network bandwidth, makes your PC run slow. As a result you start consuming more power, working longer, think of replacing your PC with a new one which brings more recyclable waste (many computers’ parts contain toxic wastes).

So to show how much we care we decided to send $2 from each product sale on saving green forests in Amazonia.

Read full story
Free Video Nude
Anjelina Jolie

About this mailing:
You are receiving this e-mail because you subscribed to MSN Featured Offers. Microsoft respects your privacy. If you do not wish to receive this MSN Featured Offers e-mail, please click the "Unsubscribe" link below. This will not unsubscribe you from e-mail communications from third-party advertisers that may appear in MSN Feature Offers. This shall not constitute an offer by MSN. MSN shall not be responsible or liable for the advertisers' content nor any of the goods or service advertised. Prices and item availability subject to change without notice.

©2008 Microsoft | Unsubscribe | More Newsletters | Privacy

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

(Courtesy of www.m86security.com)
URGENT SYSTEM SCAN NOTIFICATION! PLEASE READ CAREFULLY!!

http://www.securonline.net/

For the link to become active, please click on 'Add to contacts' skype button or type it in manually into your web browser!

FULL DETAILS OF SCAN RESULT BELOW

WINDOWS REQUIRES IMMEDIATE ATTENTION

ATTENTION! Security Center has detected malware on your computer!

Affected Software:
- Microsoft Windows Vista
- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows Server 2003

Impact of Vulnerability: Remote Code Execution / Virus infection / Unexpected shutdowns

Recommendation: Users running vulnerable version should install a repair utility immediately

Your system IS affected, download the patch from the address below!
Failure to do so may result in severe computer malfunction.
Distribution: Fake Codec

(Courtesy of threatinfo.trendmicro.com)
Distribution: Drive-by Downloads

• Victim visits a legitimate web site, which has been compromised (say, via SQL injection)
• Hidden iframe redirects victim to malicious site
• Malicious site launches a number of browser and plugin exploits
• If successful, exploits download and run rogue AV on the victim’s machine
Other searches:

- Sport events ("March madness")
- Natural disasters ("Samoa earthquake")
- Legit anti-virus ("F-Secure")
- ...
Distribution: Piggyback Trojan

- 9 April, 2009, Confiker awakens, and
- Downloads a Waledac malware,
- Which installs SpywareProtect2009,
- Which asks for $49.95 to remove “threats”
“Google recommends you to activate Antivirus 2009 to protect your PC from malicious intrusions from the Internet”
## Products

<table>
<thead>
<tr>
<th>Rank</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Spyware Guard 2008</td>
</tr>
<tr>
<td>2</td>
<td>AntiVirus 2008</td>
</tr>
<tr>
<td>3</td>
<td>AntiVirus 2009</td>
</tr>
<tr>
<td>4</td>
<td>Spyware Secure</td>
</tr>
<tr>
<td>5</td>
<td>XPAntivirus</td>
</tr>
<tr>
<td>6</td>
<td>WinFixer</td>
</tr>
<tr>
<td>7</td>
<td>SafeStrip</td>
</tr>
<tr>
<td>8</td>
<td>ErrorRepair</td>
</tr>
<tr>
<td>9</td>
<td>Internet Antivirus</td>
</tr>
<tr>
<td>10</td>
<td>DriveCleaner</td>
</tr>
</tbody>
</table>

Over 250 rogue AV programs, according to Symantec.
Spot the Difference

(Courtesy of http://rogueantispyware.blogspot.com/)
Rebranding

- Changes in the name, logos, pictures of a rogue AV
- Helps evade detection if original version of the rogue AV has been discovered
- Minimizes the impact of credit card chargebacks and payment reversals
Basic Business Model

- Rogue AV basic: $0
- Rogue AV full: $30-$100
- Multi-year licensing: ~$20 more
- Bundling other applications: ~$20 more
- Fraudulent credit card transactions: $$$
From Basic to Full

“Click this message to purchase recommended antivirus software”

“Regular updating is needed”
Affiliate-based Business Model

- Affiliates are given a range of links and JavaScript snippets
- Links and scripts embedded in shady or compromised sites
- Victim visits affiliate-controlled web site and pays for full version of rogue AV
- Affiliate responsible for generating installation is paid 60% of installation revenue
- In economic lingo: “Affiliate-based, pay-per-sale model”
TrafficConverter.biz

• Web site used to manage affiliate
  – Provides support (files, links, etc.)
  – Tracks installation and sales

• Bonus programs
  – VIP points
  – Contests for top-selling affiliates (win a Mercedes)

• Database snatched by security researchers before its shutdown in November 2008
Affiliate earnings

- 500 active affiliates
- Per-sale price: $30
- Top affiliate purportedly earning $332K in one month (!)
- Top-10 affiliates purportedly earning $23K/week

Per-installation price

<table>
<thead>
<tr>
<th>Country</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>$0.55</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>$0.52</td>
</tr>
<tr>
<td>Canada</td>
<td>$0.52</td>
</tr>
<tr>
<td>Australia</td>
<td>$0.50</td>
</tr>
<tr>
<td>Spain</td>
<td>$0.16</td>
</tr>
<tr>
<td>Ireland</td>
<td>$0.16</td>
</tr>
<tr>
<td>France</td>
<td>$0.16</td>
</tr>
<tr>
<td>Italy</td>
<td>$0.16</td>
</tr>
<tr>
<td>Germany</td>
<td>$0.12</td>
</tr>
<tr>
<td>Belgium</td>
<td>$0.12</td>
</tr>
</tbody>
</table>
Rogue AV Campaigns

- Coordinated effort by cyber-criminals to distribute and profit from a rogue AV
- Components:
  - Malware code
  - Infrastructure used to distribute it
  - Victims that fall for it
Campaign Analysis

Data:
• 2 months in summer 2009
• 4,305 rogue AV-hosting servers (IP addresses)
• 6,500 domains

Goals:
• Infrastructure
  – How created and managed
  – Identify related sites
• How it affects clients
Whac-a-mole?
Identifying Campaigns

• Assumption: campaign is managed by a group of people, who are likely to reuse, at various stages of the campaign, the same techniques, strategies, and tools

• Approach: look for emerging patterns in infrastructure components (web sites)
Features

- IP address
- DNS domain names
- Geolocation
- Server identification name and version
- ISP
- ASN
- DNS registrar
- DNS registrant
- Uptime
Multicriteria Clustering

- TRIAGE
  - = atTRIbution of Attack phenomena using Graph-based Event clustering

- Multicriteria clustering method
TRIAGE: a “simple” example

310 domains registered over a few days

registrants

IP networks

06/10/2010

MURI Review Meeting

17-Oct-2008

18-Oct-2008
A slightly more complex example

750 domains registered over a span of 8 months

Email addr. hidden by privacy protection services

06/10/2010

MURI Review Meeting
A slightly more complex example
Cluster Results

- 39 clusters with at least 10 domains
- They account for ~70% dataset
Server Geolocation
Server IPs

![Graph showing distribution of server IPs and nameservers across IPv4 space (Class-A subnets).]
Rogue-friendly Networks?
Activating Sites

In one-day interval:
• Moved 3 sites from GoDaddy’s parking servers to active servers
• Consolidated 4th site

06/10/2010
MURI Review Meeting
Deactivating Sites
Rogue AV Registrants

<table>
<thead>
<tr>
<th>Registrant’s email domain</th>
<th># Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmail.com</td>
<td>1,238 (30%)</td>
</tr>
<tr>
<td>id-private.com</td>
<td>574 (14%)</td>
</tr>
<tr>
<td>whoisprivacyprotect.com</td>
<td>533 (13%)</td>
</tr>
<tr>
<td>privacyprotect.org</td>
<td>125 (3%)</td>
</tr>
<tr>
<td>mas2009.com</td>
<td>101 (2%)</td>
</tr>
</tbody>
</table>

Registrants seem to value their privacy...

06/10/2010 MURI Review Meeting
Beyond the Graphs

• Automate the identification of campaigns
• Insights into how cyber criminals operate
  – Registration strategy (time)
  – Name schemes
• Attack attribution/understanding
• Future work: early warning system
Clients

• 6 of the rogue AV-hosting servers leaked information about their clients
  – Site name
  – Client IP
  – Client Request
• No access to content of communication
• 45-day monitoring
• 372,096 distinct client IP addresses
(Potential) Victim Geolocation
Request Types

- Scan
- Download
- Update
- Payment form
- Payment confirmation
- Report
Rogue AV Effectiveness

On sites we monitored:
• 1.26% of users visit payment page
• 0.03% attempt to complete purchase
Interaction Duration

![Bar Chart]

- **Observed Class C Networks (#)**
  - 0-10: 10,000,000
  - 10-20: 100,000
  - 20-30: 10,000
  - 30-40: 1,000
  - 40-50: 100

- **Days of Observation**
  - 0-10
  - 10-20
  - 20-30
  - 30-40
  - 40-50

06/10/2010

MURI Review Meeting
Conclusions

• Rogue AV significant threat
  – “Products”
  – Distribution mechanisms
  – Developed economy

• Our contributions
  – Understanding infrastructure
  – Identifying related sites
  – Insights into modus operandi criminals
  – Inside look at victims (potential and actual)
Some Legal Victories

• Washington State’s Attorney General obtained a $1 million settlement from Secure Computer LLC, of White Plains, NY (December 2006), distributor of Spyware Cleaner

• Microsoft and Washington State’s Attorney General filed lawsuits against Branch Software, distributor of Registry Cleaner XP

• FTC obtained $1.9 million settlement from distributors of WinFixer, WinAntivirus, DriveCleaner, ErrorSafe, and XP Antivirus