Distributed Trust Management and Rogue AV Software

Angelos D. Keromytis
Columbia University

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Distributed Trust Management and Rogue AV Software	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
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

13. SUPPLEMENTARY NOTES
MURI Review, June 2010. U.S. Government or Federal Rights License

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**59**	

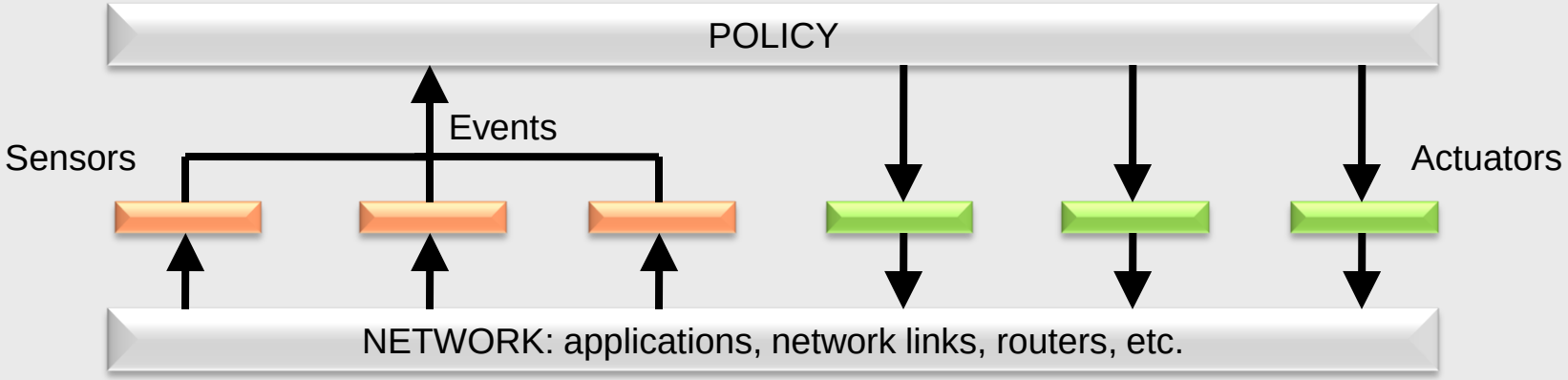
DTM – Motivation

- 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” Michael E. Locasto, Matthew Burnside, and Darrell Bethea. In Proceedings of the 23rd Large Installation System Administration (LISA) Conference. November 2009, Baltimore, MD.**
- 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



- 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
  - *"Arachne: Integrated Enterprise Security Management"*
    Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *8th Annual IEEE SMC Information Assurance Workshop (IAW),* pp. 214 - 220. June 2007, West Point, NY.
- Design DTM architecture
  - *"Asynchronous Policy Evaluation and Enforcement"*
    Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *2nd Computer Security Architecture Workshop (CSAW),* pp. 45 - 50. October 2008, Fairfax, VA.
- Collaborative/Distributed policy enforcement
  - *"F3ildCrypt: End-to-End Protection of Sensitive Information in Web Services"*
    Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *12th Information Security Conference (ISC),* pp. 491 - 506. September 2009, Pisa, Italy.
  - *"Path-based Access Control for Enterprise Networks"*
    Matthew Burnside and Angelos D. Keromytis. In Proceedings of the *11th Information Security Conference (ISC),* pp. 191 - 203. Taipei, Taiwan, September 2008.

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"

Marco Cova, Corrado Leita, Olivier Thonnard, Marc Dacier, and Angelos D. Keromytis. In Proceedings of the *5th European Conference on Computer Network Defense (EC2ND).* November 2009, Milan, Italy. *(Invited paper)*

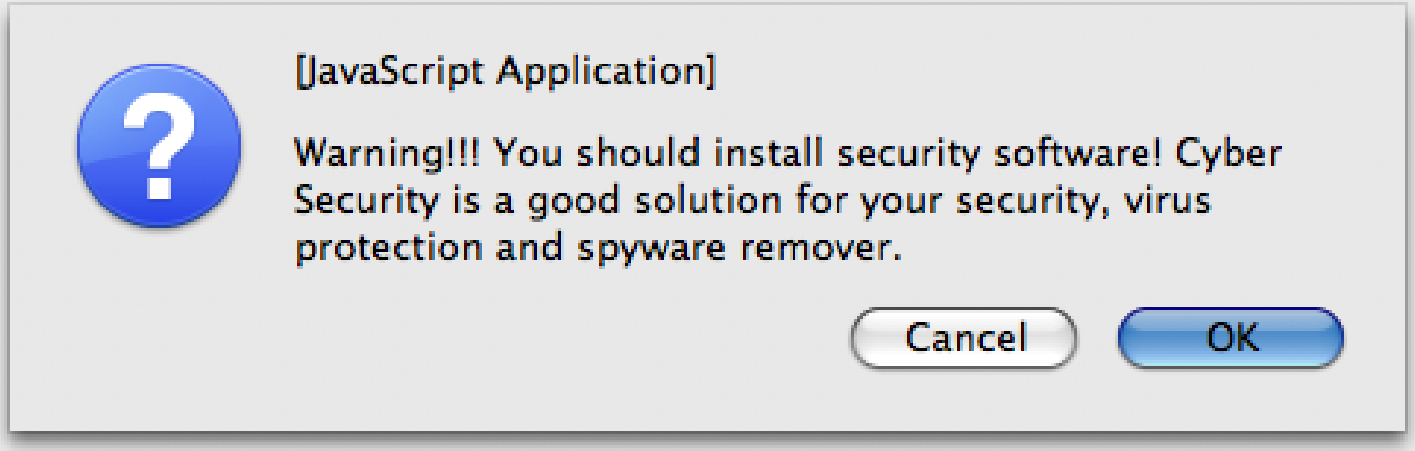
"An Analysis of Rogue AV Campaigns"

Marco Cova, Corrado Leita, Olivier Thonnard, Marc Dacier, and Angelos D. Keromytis. To appear in the Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID). September 2010, Ottawa, Canada.

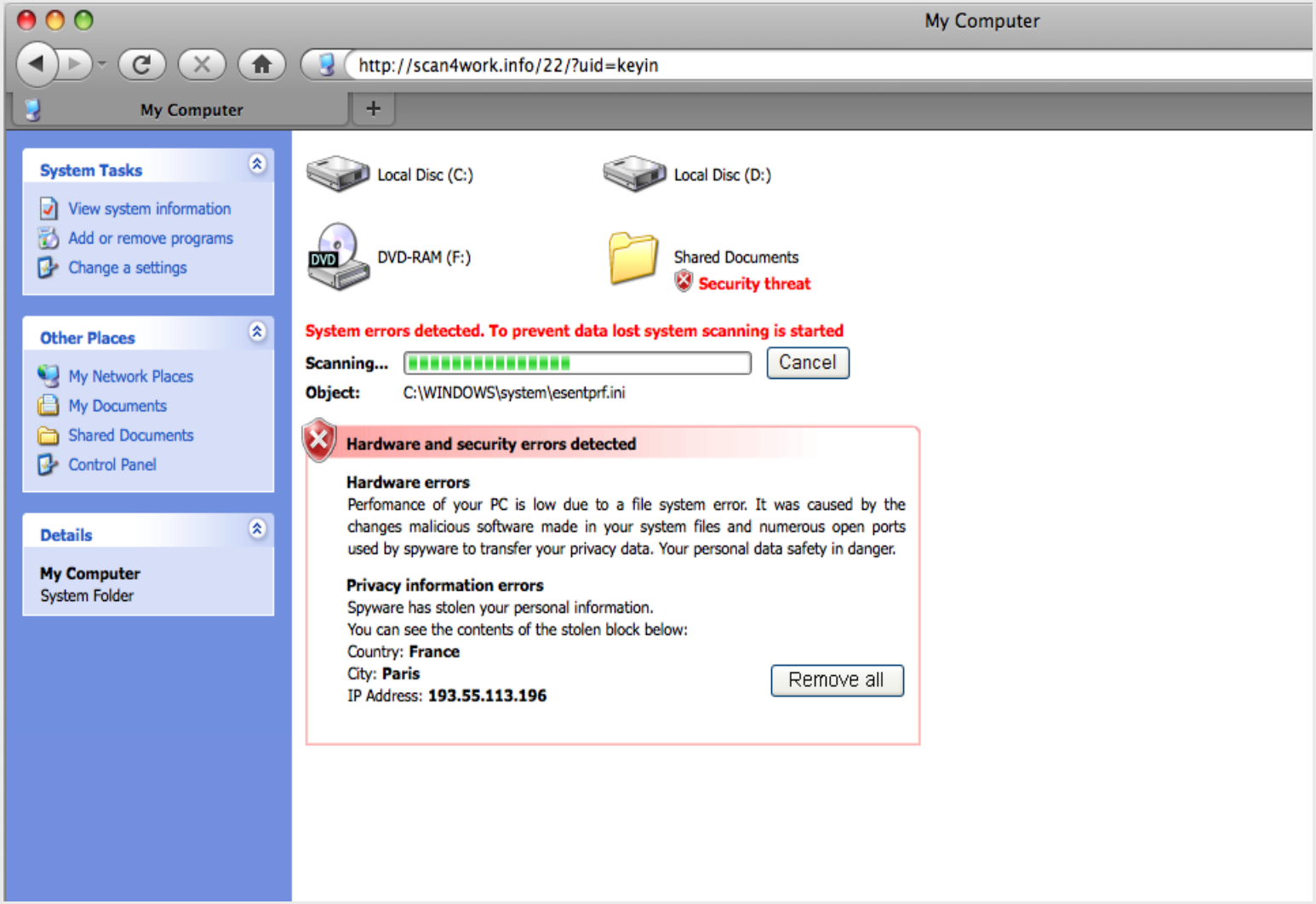
Bait


The New York Times – Breaking News, World News & Multimedia
http://www.nytimes.com/
Google
J.CREW
The New York Times
Thursday, November 5, 2009 Last Update: 1:40 PM ET
SHOP JCREW.COM
Search
THE DAMNED UNITED NOW PLAYING
Try Our EXTRA Home Page
Get Home Delivery | New York Mostly Cloudy 52°F
Switch to Global Edition
JOBS
REAL ESTATE
AUTOS
ALL CLASSIFIEDS
WORLD
U.S.
POLITICS
N.Y./REGION
BUSINESS
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
OPINION
ARTS
Books
Movies
Music
Television
Theater
STYLE
Dining & Wine
Fashion & Style
Home & Garden
Kerik Pleads 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 BERENSON 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.
NO SOCIALISTIC HEALTHCARE
Alex Brandon/Associated Press
PRESCRIPTIONS
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.
MAGAZINE PREVIEW
Making Health Care Better
By DAVID LEONHARDT
OPINION »
HOME FIRES
Oceans Apart
A mother and veteran on being away from family during war.
Collins: Hark! The Voters Speak! | Comments (197)
Kristof: Sick America
Editorial: The Off-Off-Year Elections
Op-Ed: Authentic G.O.P.
Schott: Non-Fire Night
THEATER »
REVIEWS
'Idiot Savant'
Willem Dafoe plays the title character in Richard Foreman's play.
'Nightingale'
Lynn Redgrave explores the life of her maternal grandmother.
THIS HOLIDAY SEASON REDISCOVER THE JOY OF FAMILY
ROBERT DE NIRO
EVERYBODY'S FINE
ROLLOVER FOR MORE
MARKETS »
At 1:42 PM ET
S.&P. 500 1,063.63 +17.13 +1.64%
Dow 9,982.08 +179.94 +1.84%
Nasdaq 2,101.16 +45.64 +2.22%
GET QUOTES
My Portfolios »
Stock, ETFs, Funds
Go
TONIGHT ONLY. AFTER 5PM.
HSBC PREMIER
LEARN

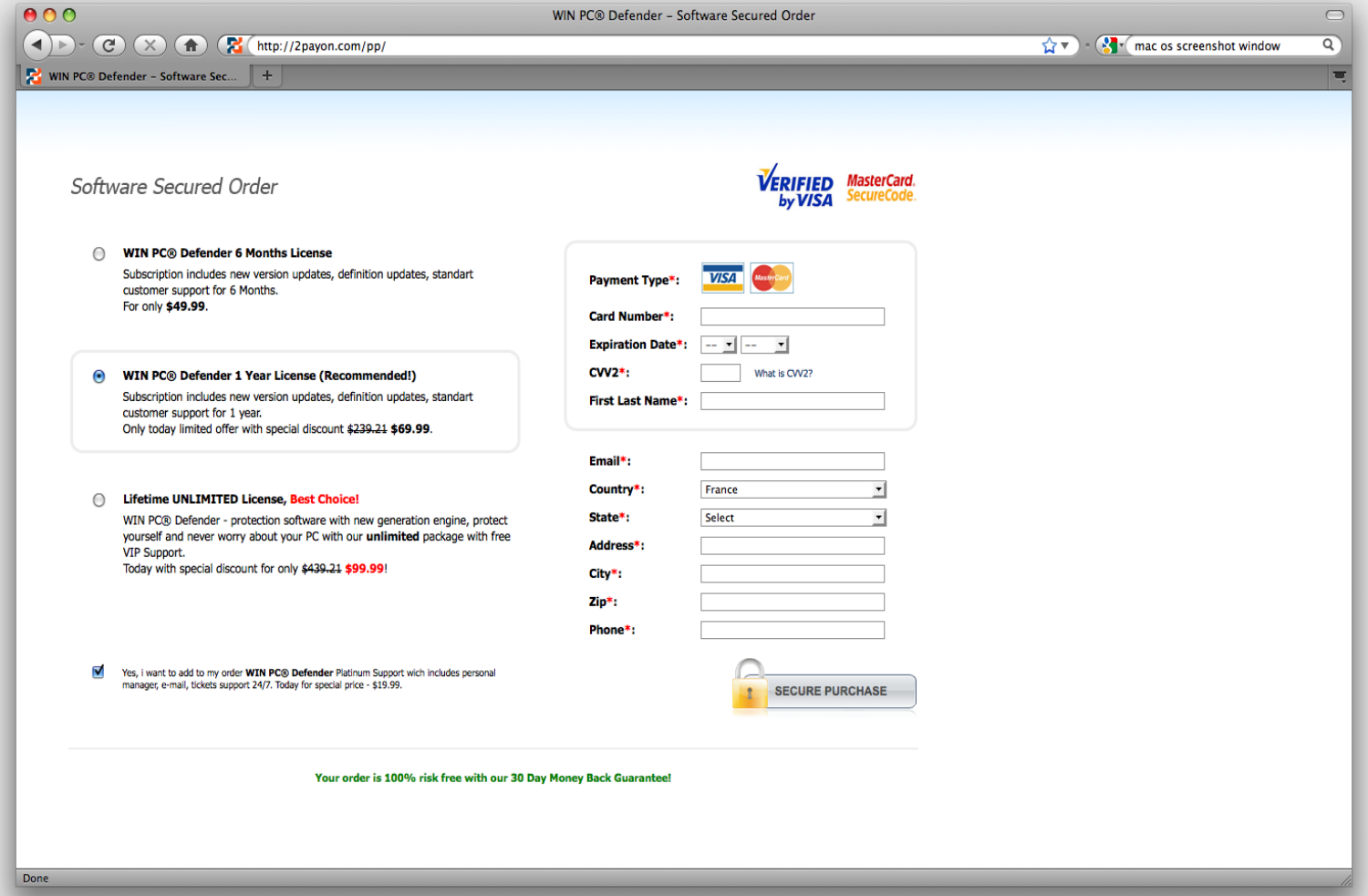
Hijack


[JavaScript Application]
Warning!!! You should install security software! Cyber Security is a good solution for your security, virus protection and spyware remover.
Cancel
OK

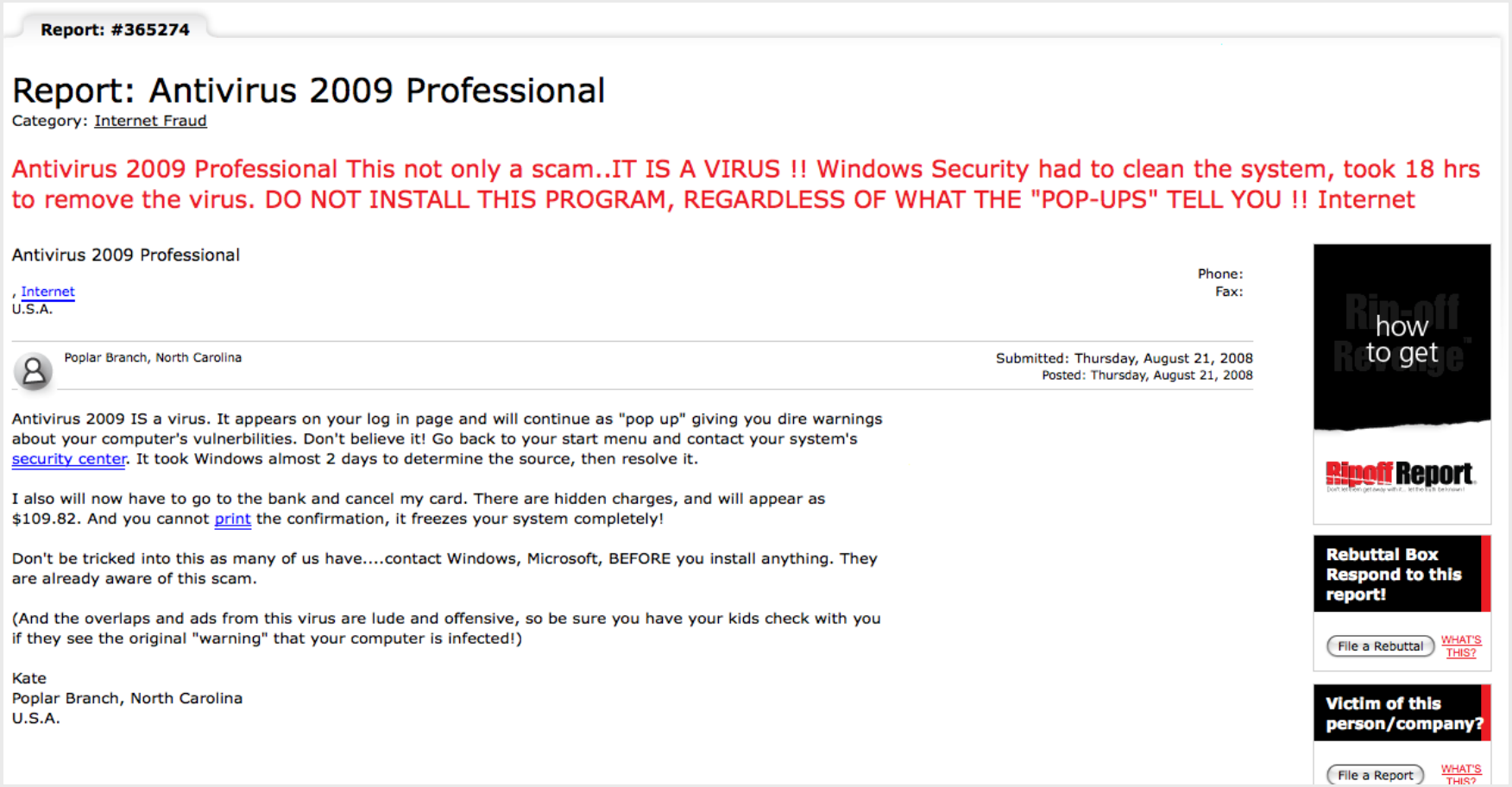
Scare Tactics



Payment


WIN PC® Defender – Software Secured Order
http://2payon.com/pp/
mac os screenshot window
WIN PC® Defender – Software Sec...
Software Secured Order
VERIFIED by VISA
MasterCard SecureCode.
WIN PC® Defender 6 Months License
Subscription includes new version updates, definition updates, standart customer support for 6 Months.
For only $49.99.
WIN PC® Defender 1 Year License (Recommended!)
Subscription includes new version updates, definition updates, standart customer support for 1 year.
Only today limited offer with special discount $239.21 $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 $439.21 $99.99!
Yes, I want to add to my order WIN PC® Defender Platinum Support wich includes personal manager, e-mail, tickets support 24/7. Today for special price - $19.99.
Payment Type*:
Card Number*:
Expiration Date*:
CVV2*:
What is CVV2?
First Last Name*:
Email*:
Country*:
France
State*:
Select
Address*:
City*:
Zip*:
Phone*:
SECURE PURCHASE
Your order is 100% risk free with our 30 Day Money Back Guarantee!
Done

Aftermath



Report: #365274

Report: Antivirus 2009 Professional

Category: Internet Fraud

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

, Internet
U.S.A.

Phone:
Fax:

Poplar Branch, North Carolina

Submitted: Thursday, August 21, 2008
Posted: Thursday, August 21, 2008

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 vulnerbilities. 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?

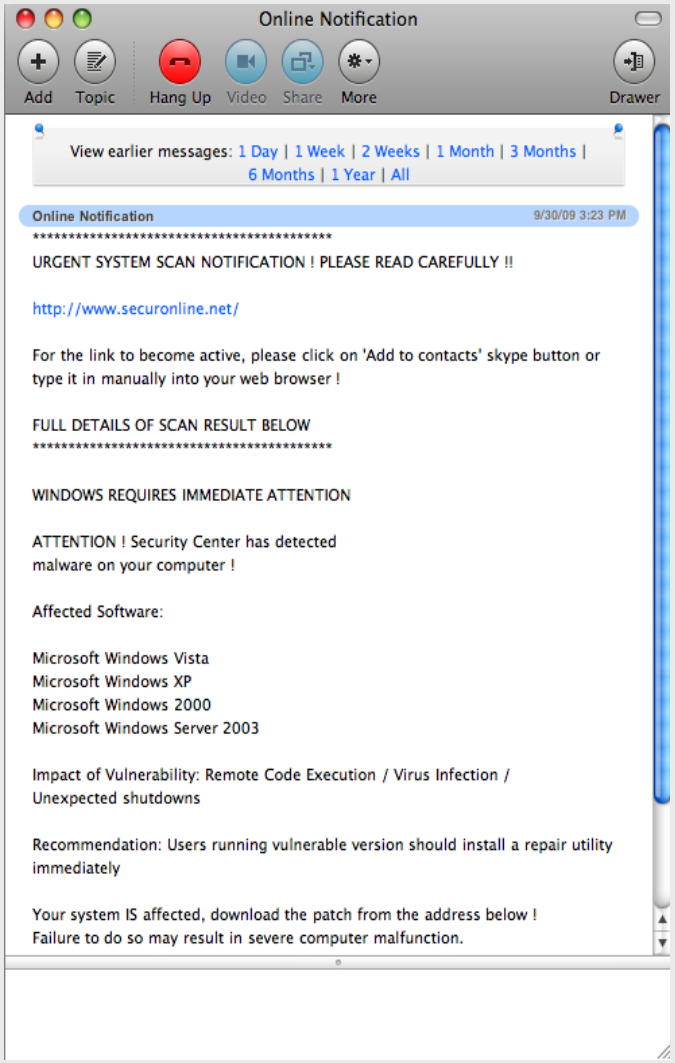
- False alerts only
  - Tens of alerts on freshly installed machine
- “Selective” alerts
  - IE Defender spreads via Zlob malware
  - After installation, it correctly detects Zlob
- “1980-style” alerts
  - Filename, registry path checks
- Sometimes come with EULA…

Distribution: Website Downloads

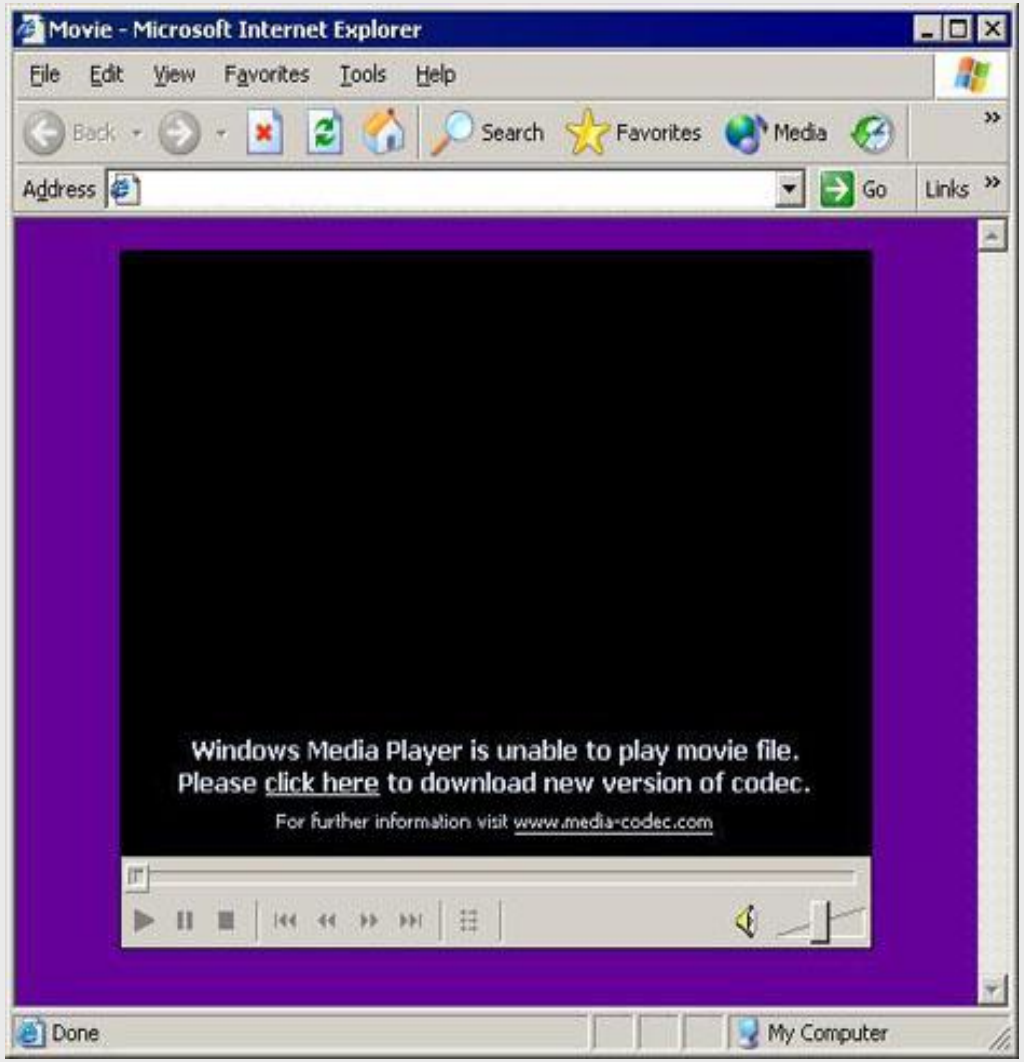
Distribution: Spam

(Courtesy of www.m86security.com)

Distribution: Skype



Distribution: Fake Codec



(Courtesy of threatinfo.trendmicro.com

Distribution: Malvertisement

eWeek Web Site Leads Users to Rogue Anti-Virus (AV) Application

Date:02.24.2009

April 15th, 2009

Scareware pops-up at FoxNews

Posted by Dancho Danchev @ 6:41 am

USAToday.com Ads Redirect to Rogue AV

Posted by Paul Royal on Thu, May 07, 2009

Home > News > New York Times serves up rogue ads to readers

New York Times serves up rogue ads to readers

Angela Moscaritolo September 14, 2009

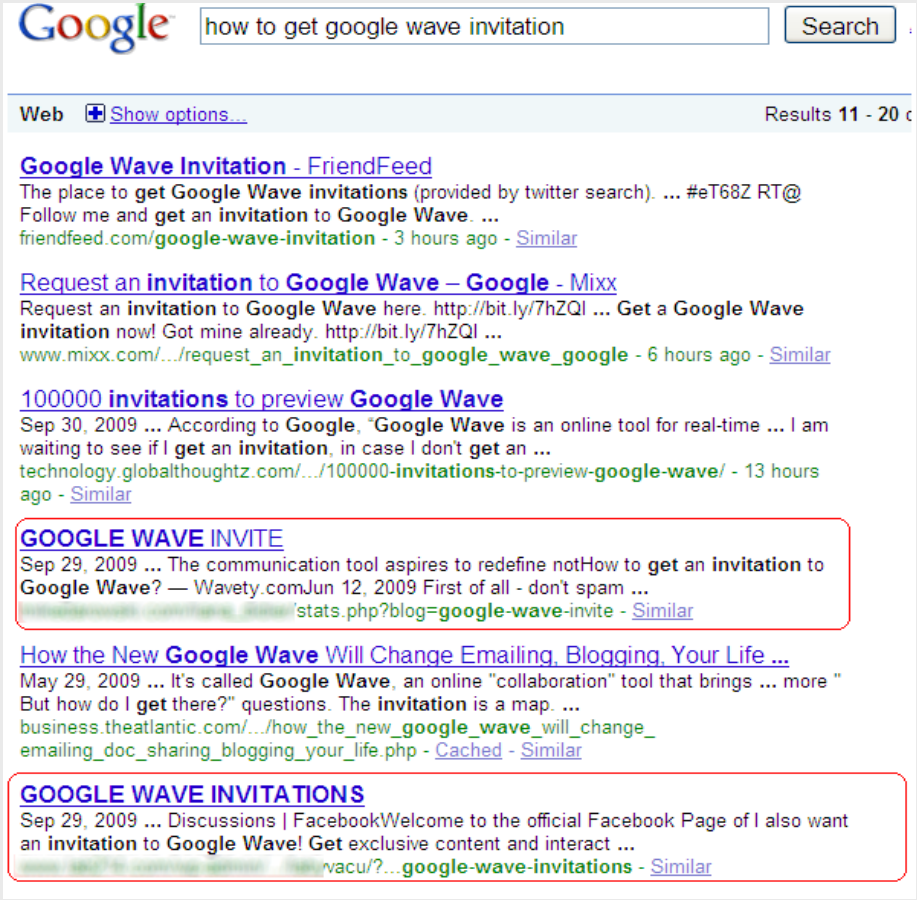
Gizmodo victimized by malicious advertising scam

by Steve Ragan – Oct 28 2009, 16:00

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

Distribution: SEO



(Courtesy of securitylabs.websense.com)

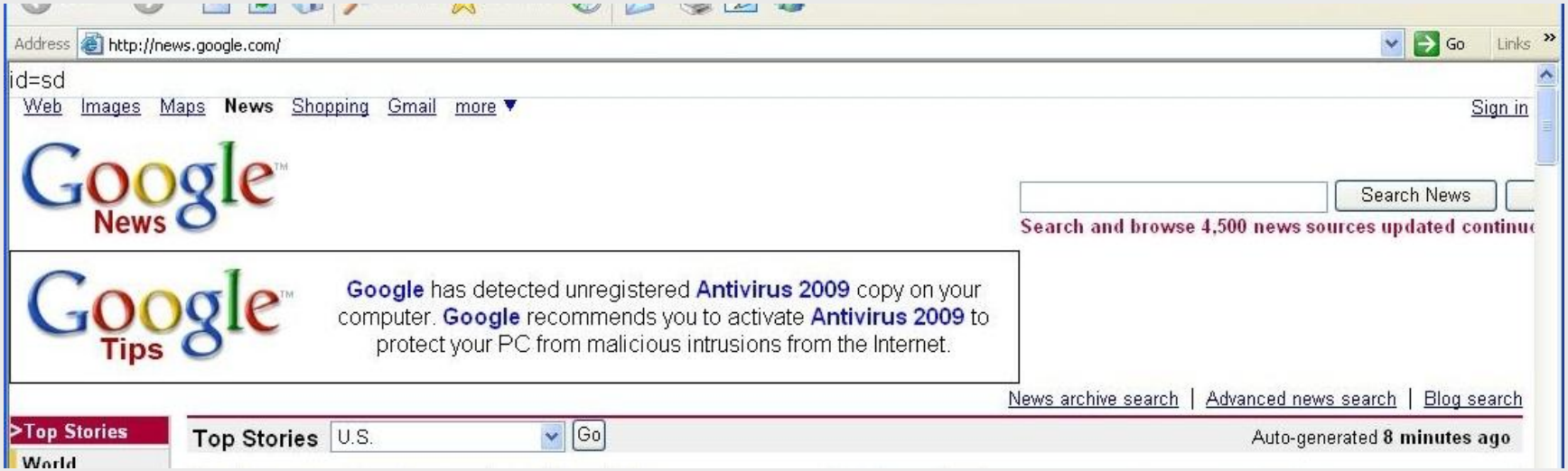
Other searches:

- 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”

Distribution: Piggyback BHO



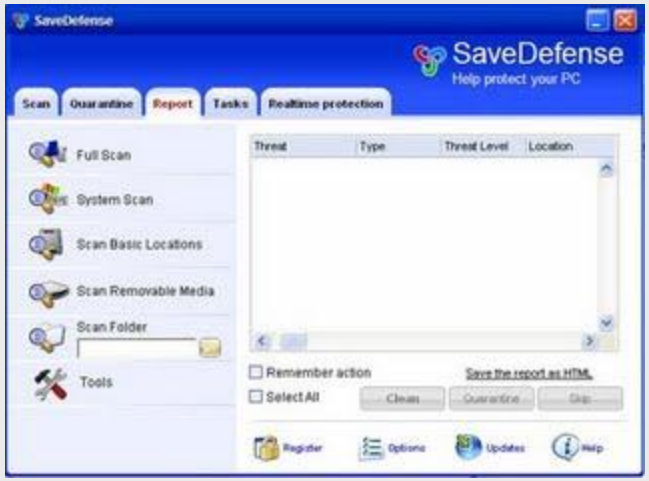
"Google recommends you to activate Antivirus 2009
to protect your PC
from malicious intrusions from the Internet"

Products

Rank	Product
1	Spyware Guard 2008
2	AntiVirus 2008
3	AntiVirus 2009
4	Spyware Secure
5	XPAntivirus
6	WinFixer
7	SafeStrip
8	ErrorRepair
9	Internet Antivirus
10	DriveCleaner

Over 250 rogue AV programs, according to Symantec.

Spot the Difference



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

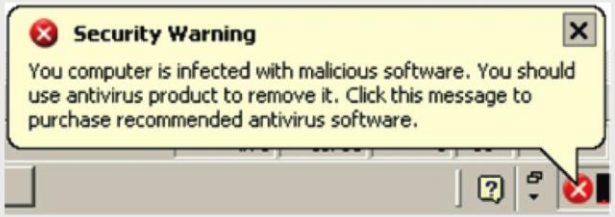
Rebranding

- 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

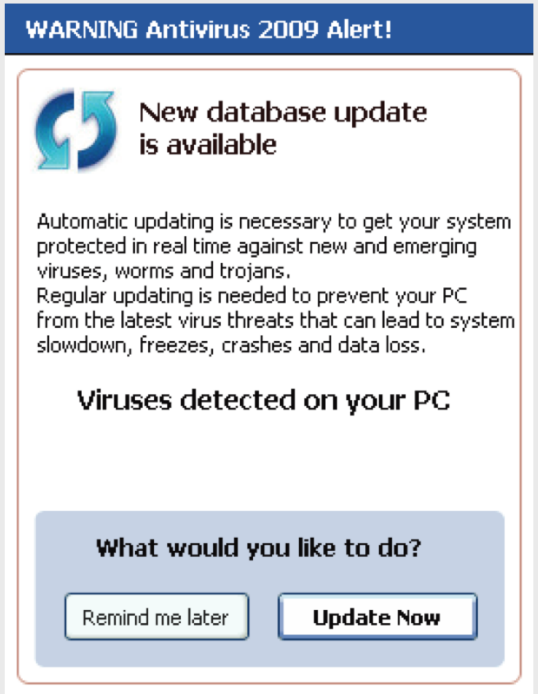
Basic Business Model

- 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

TrafficConverter.biz

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

Country	Price
United States	$0.55
United Kingdom	$0.52
Canada	$0.52
Australia	$0.50
Spain	$0.16
Ireland	$0.16
France	$0.16
Italy	$0.16
Germany	$0.12
Belgium	$0.12

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

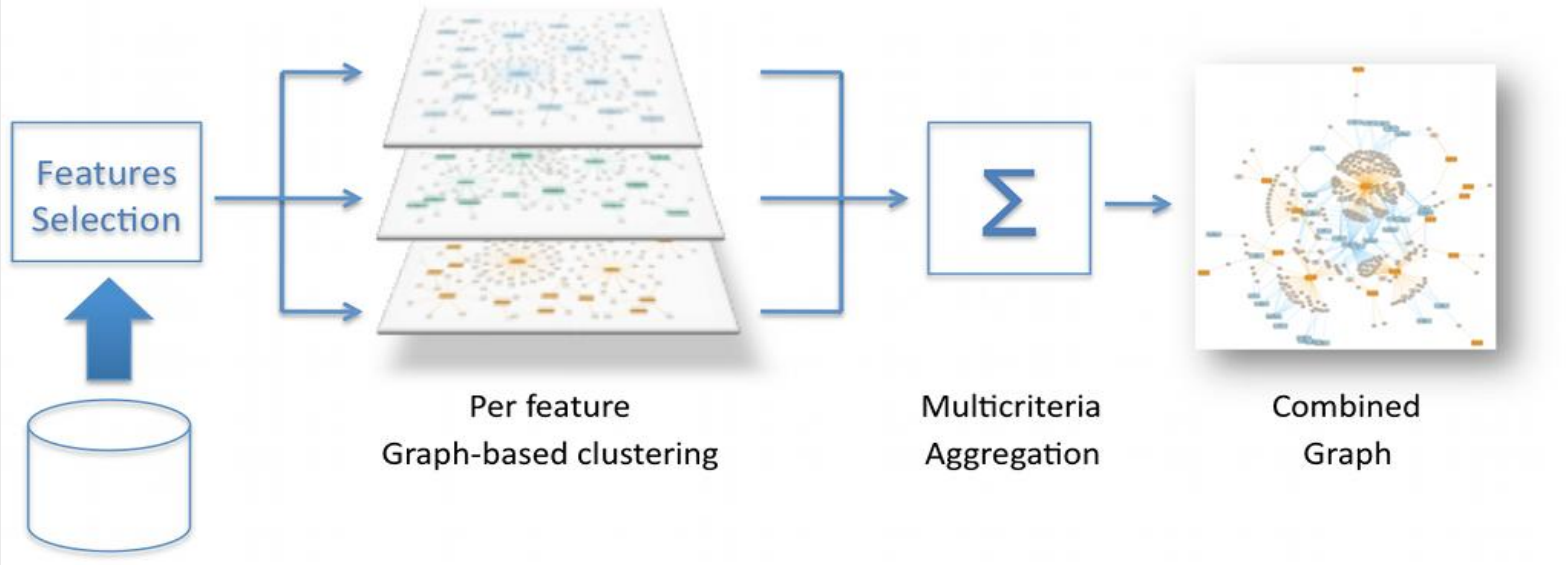
- Assumption: campaign is managed by a group of people, who are likely to reuse, at various stages of the campaign, the same techniques, strategies, and tools
- Approach: look for emerging patterns in infrastructure components (web sites)

Features

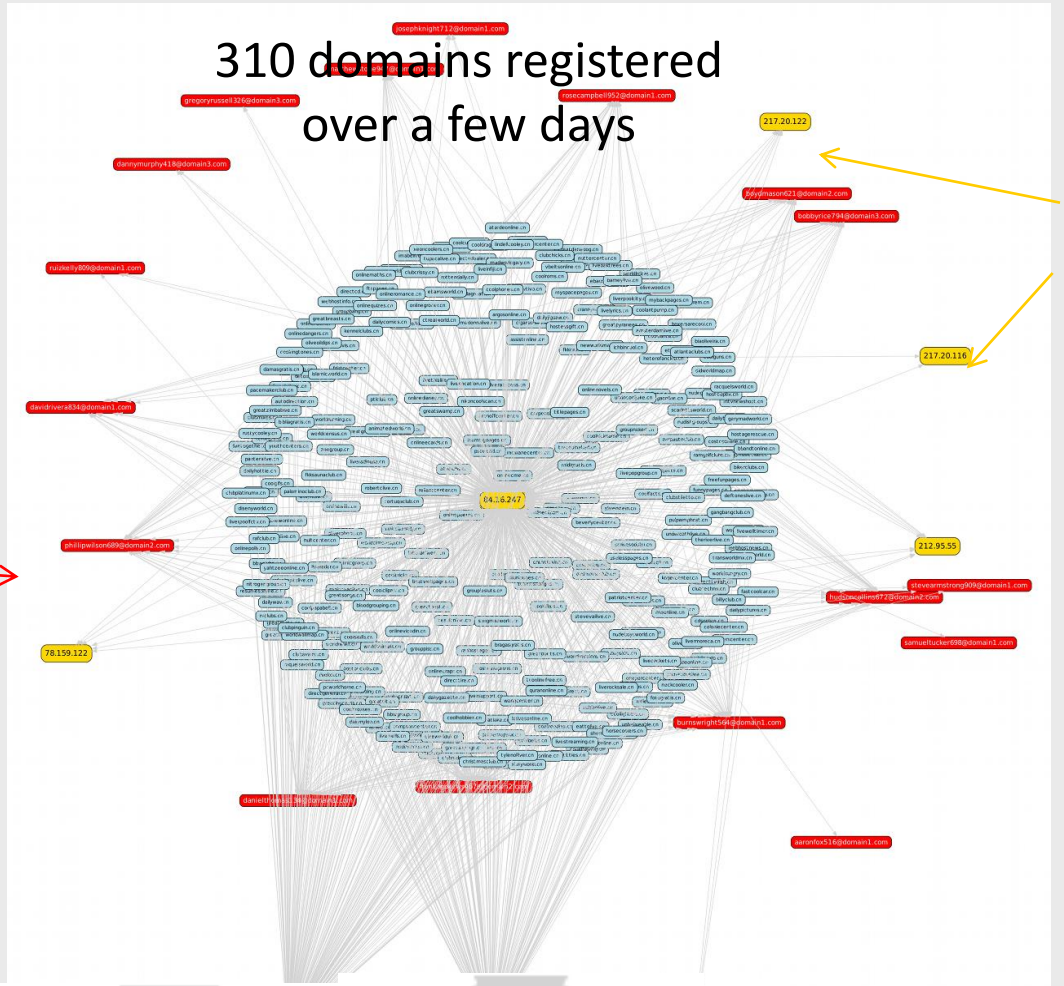
- IP address
- DNS domain names
- Geolocation
- Server identification name and version
- ISP
- ASN
- DNS registrar
- DNS registrant
- Uptime

Multicriteria Clustering

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



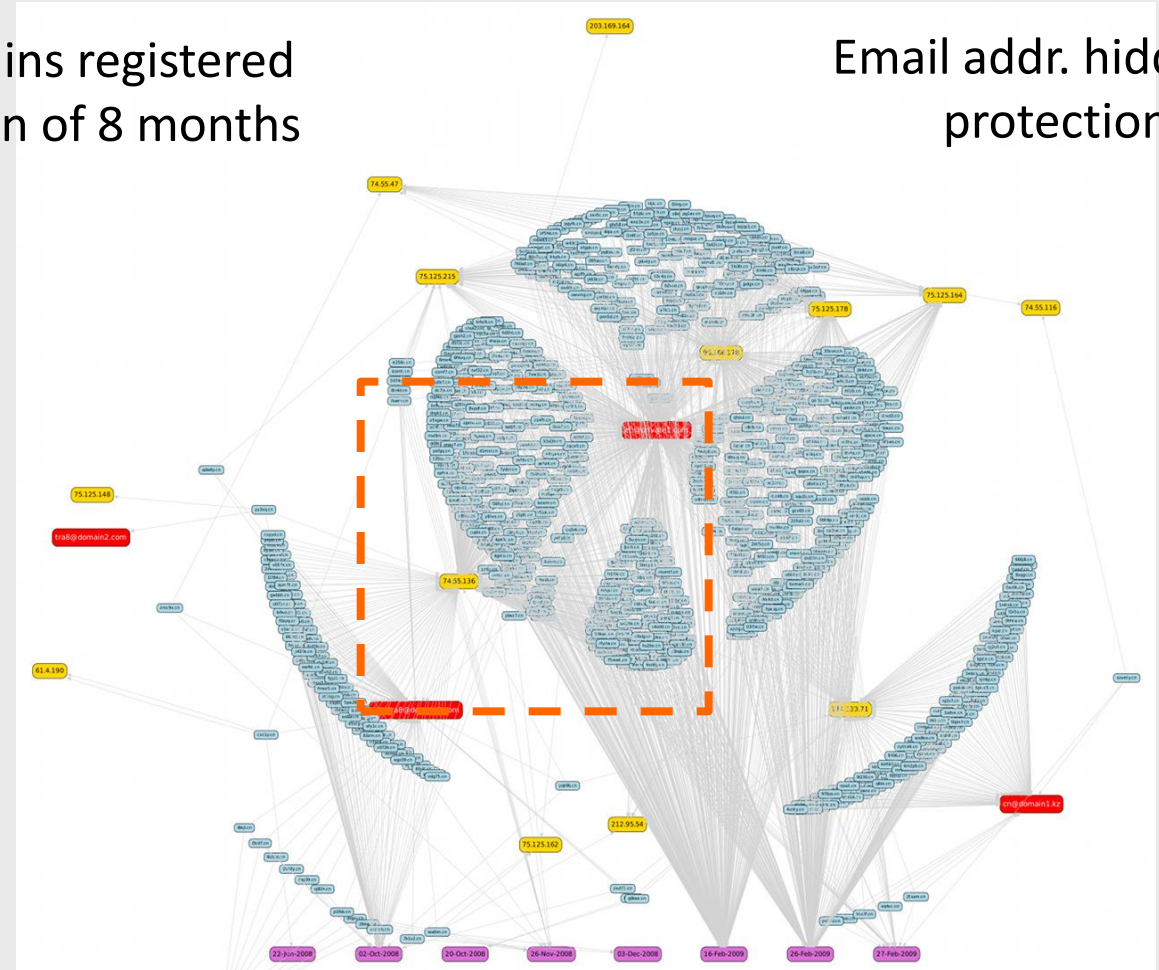
TRIAGE: a “simple” example



A slightly more complex example

750 domains registered over a span of 8 months

Email addr. hidden by privacy protection services

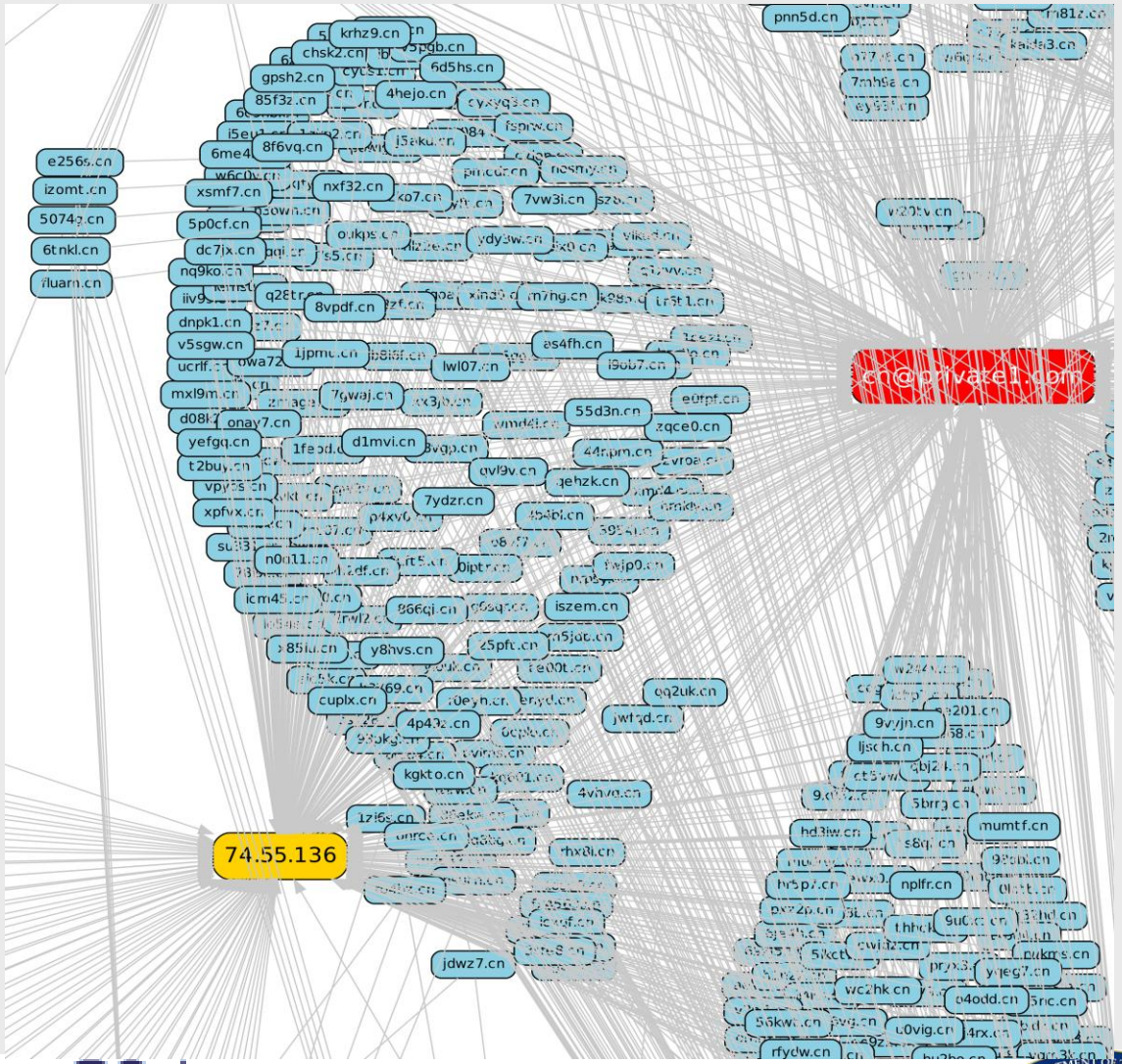


22-Jun-2008

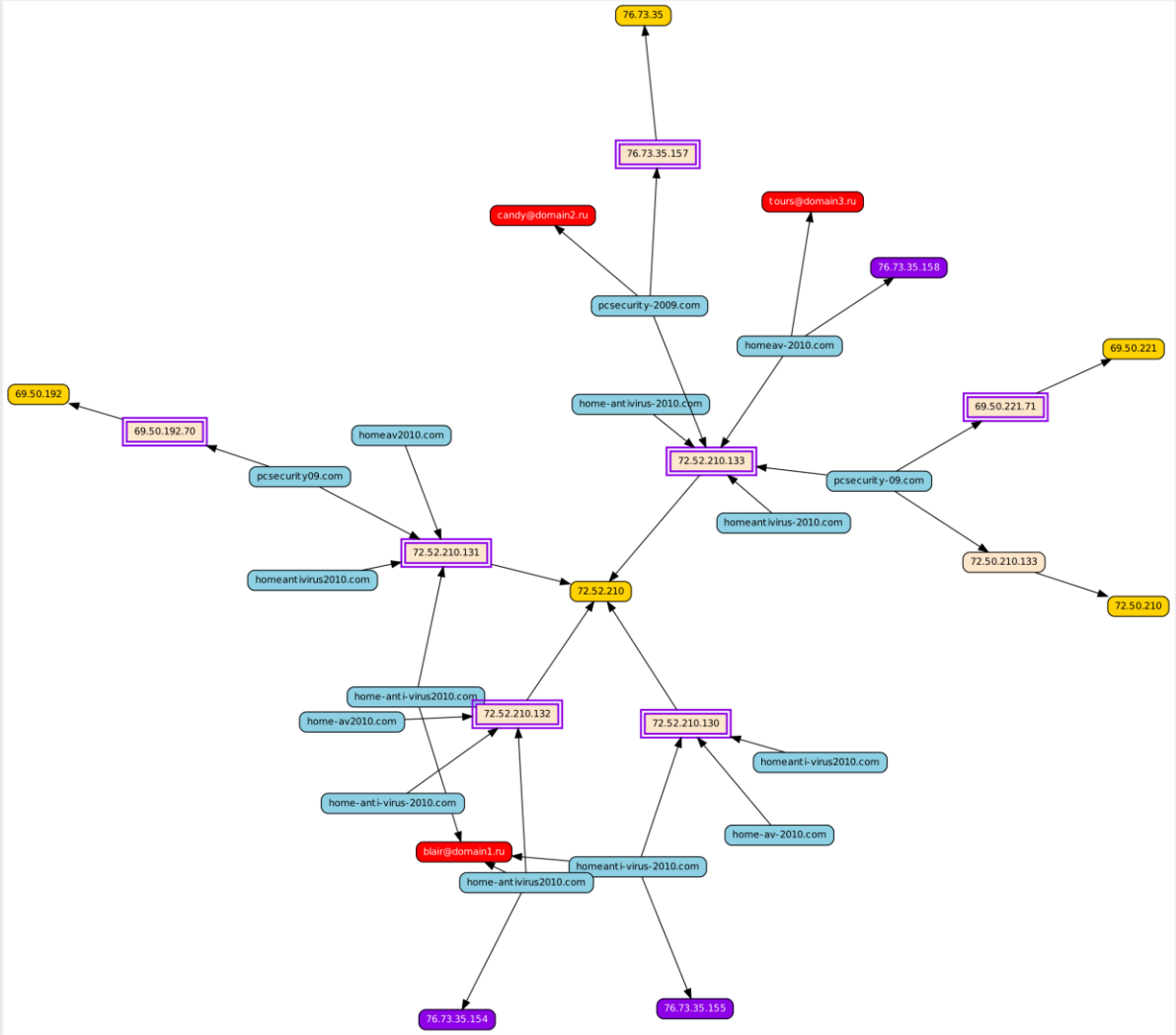
27-Feb-2009

Time

A slightly more complex example

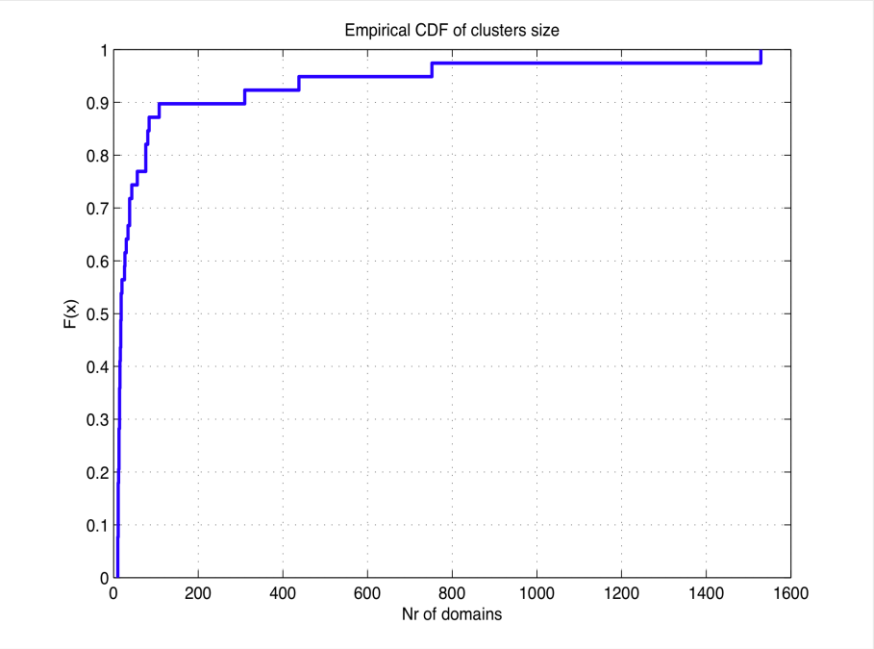


AntiVirus2010

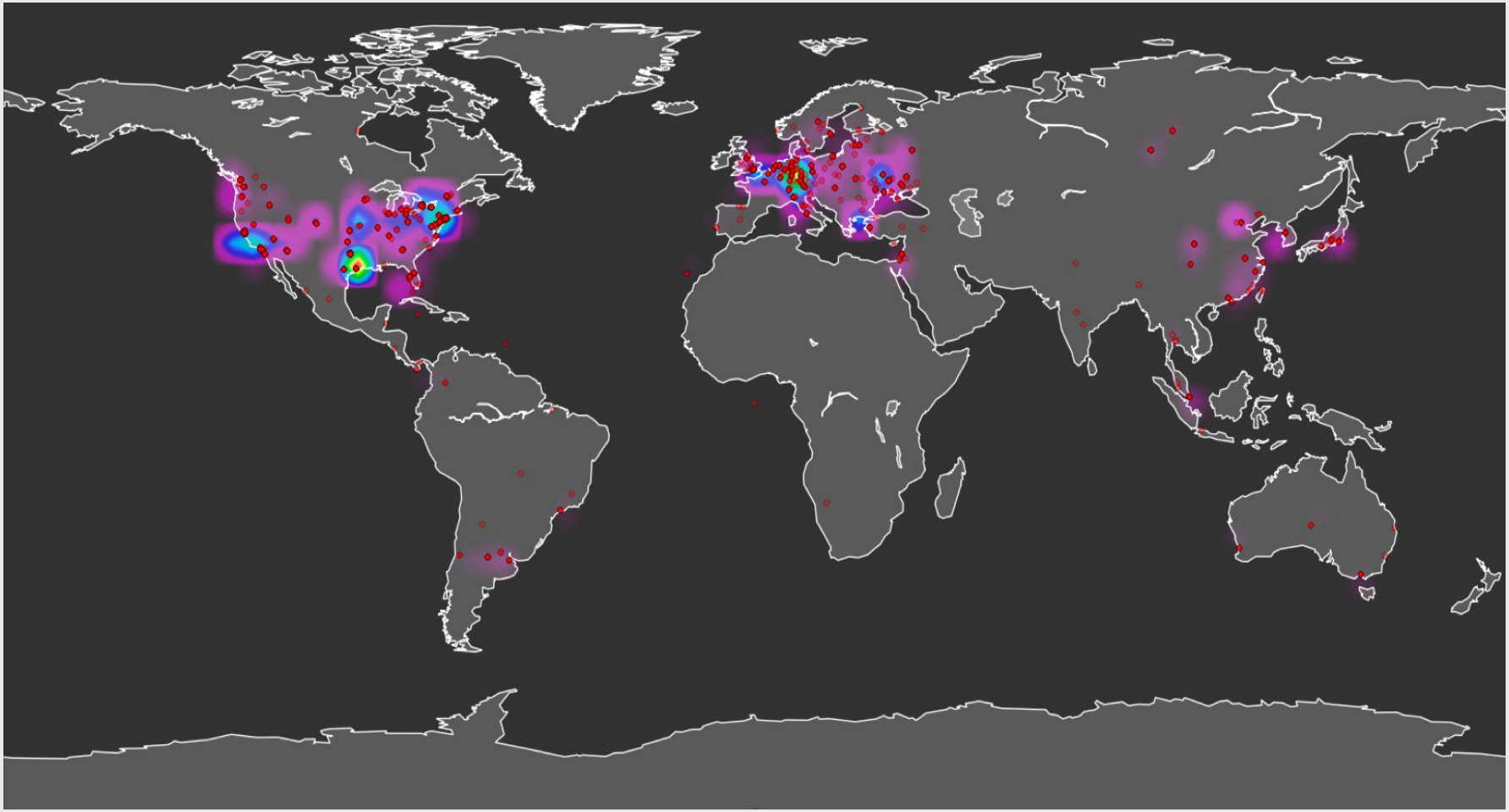


Cluster Results

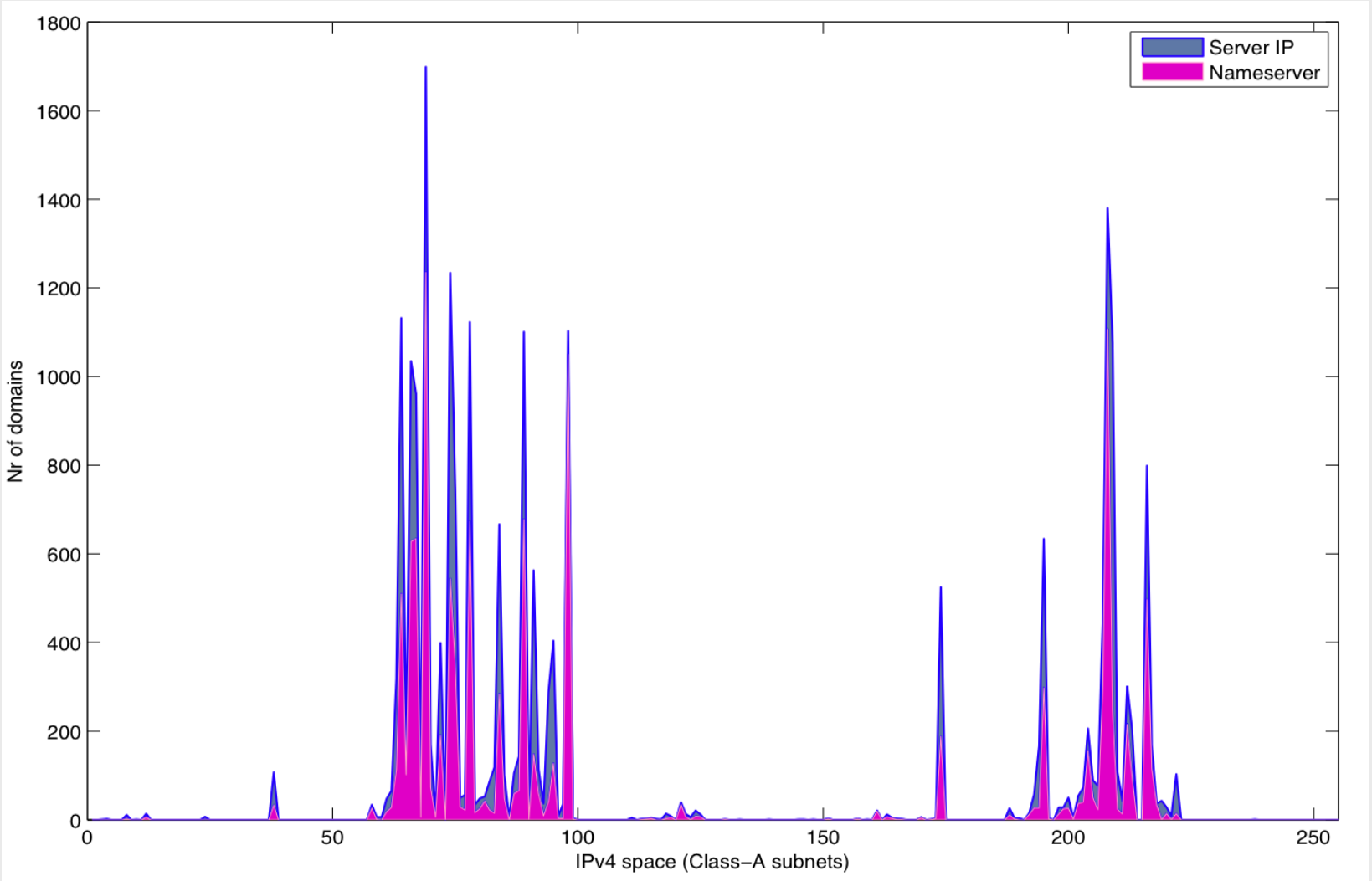
- 39 clusters with at least 10 domains
- They account for ~70% dataset



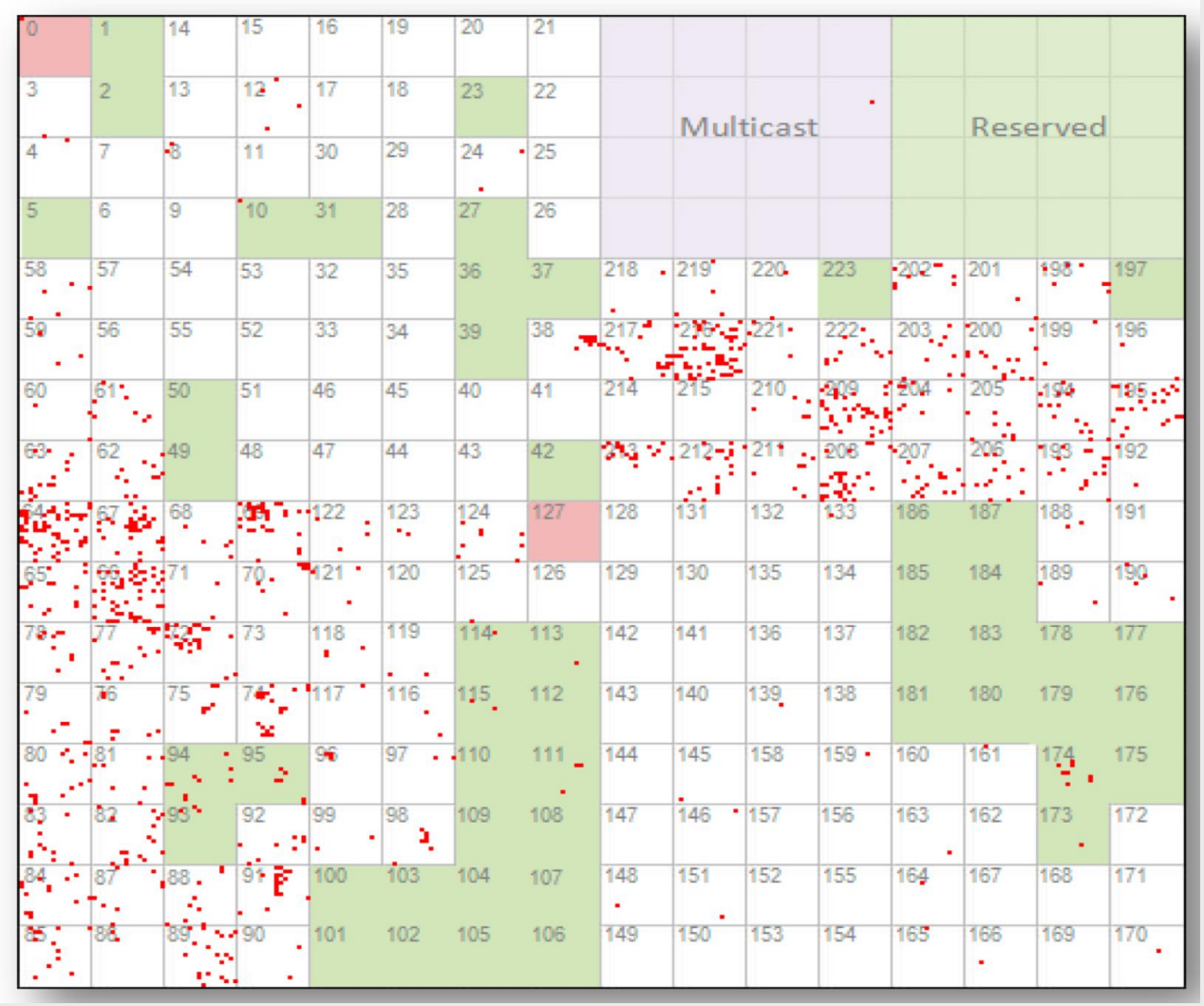
Server Geolocation



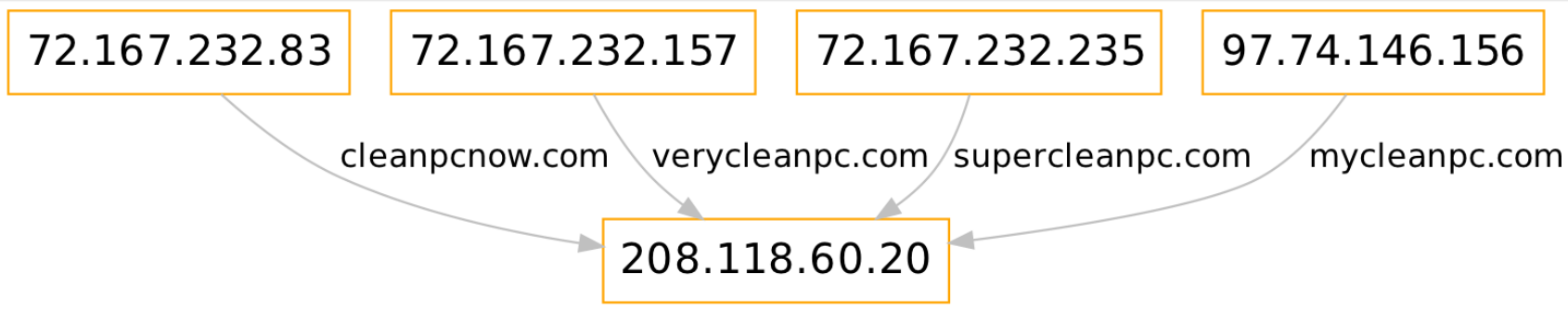
Server IPs


Server IP
Nameserver
Nr of domains
IPv4 space (Class–A subnets)
0
200
400
600
800
1000
1200
1400
1600
1800
0
50
100
150
200
250

Rogue-friendly Networks?



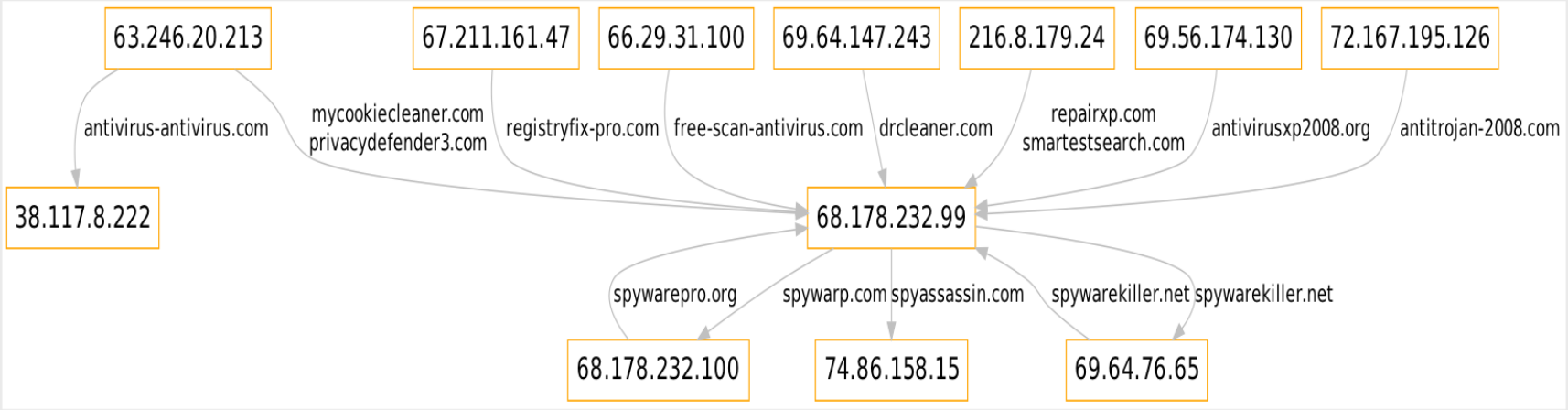
Activating Sites



In one-day interval:

- Moved 3 sites from GoDaddy's parking servers to active servers
- Consolidated 4th site

Deactivating Sites



Rogue AV Registrants

Registrant's email domain	# Sites
gmail.com	1,238 (30%)
id-private.com	574 (14%)
whoisprivacyprotect.com	533 (13%)
privacyprotect.org	125 (3%)
mas2009.com	101 (2%)

Registrants seem to value their privacy…

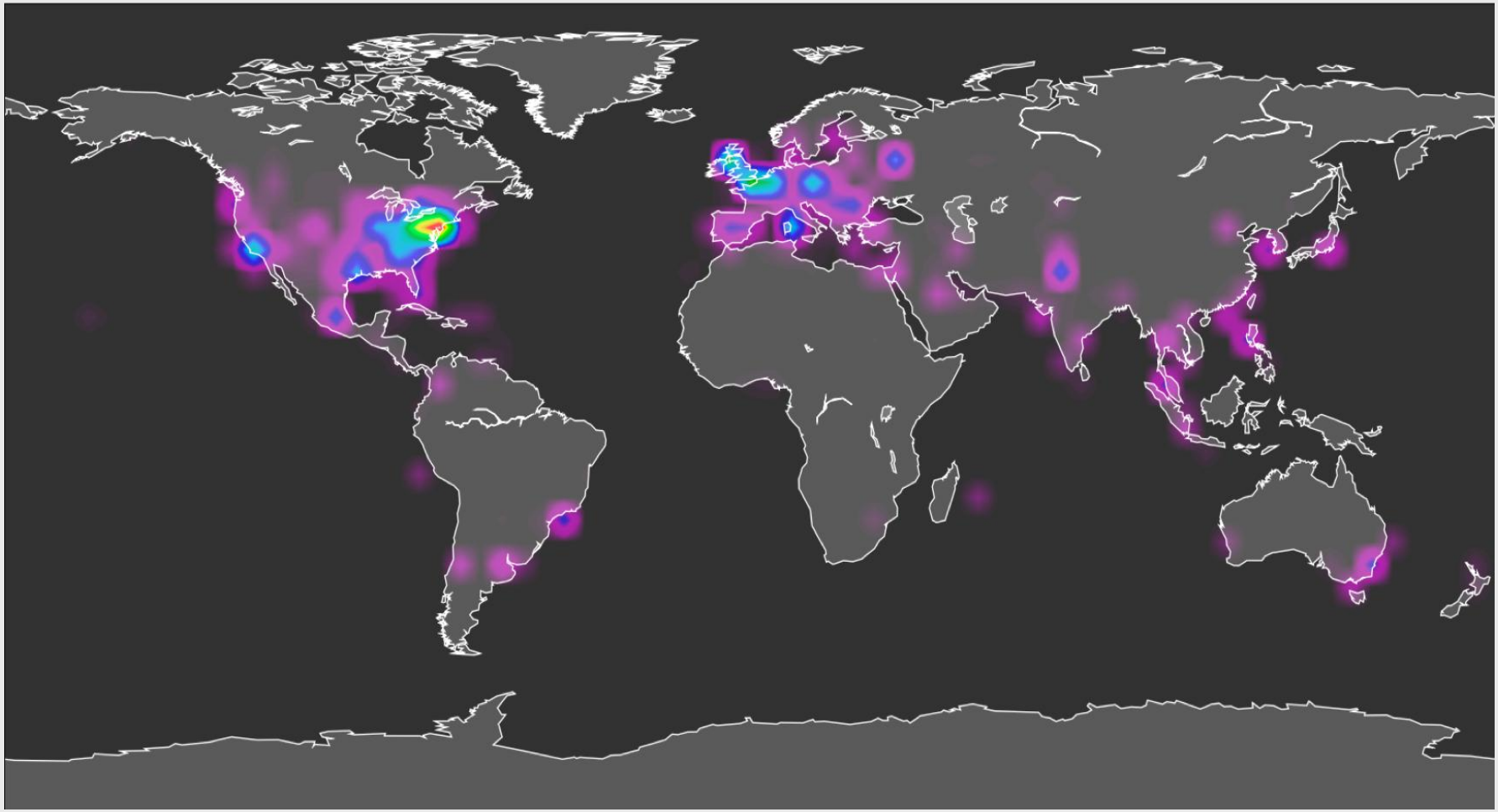
Beyond the Graphs

- 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

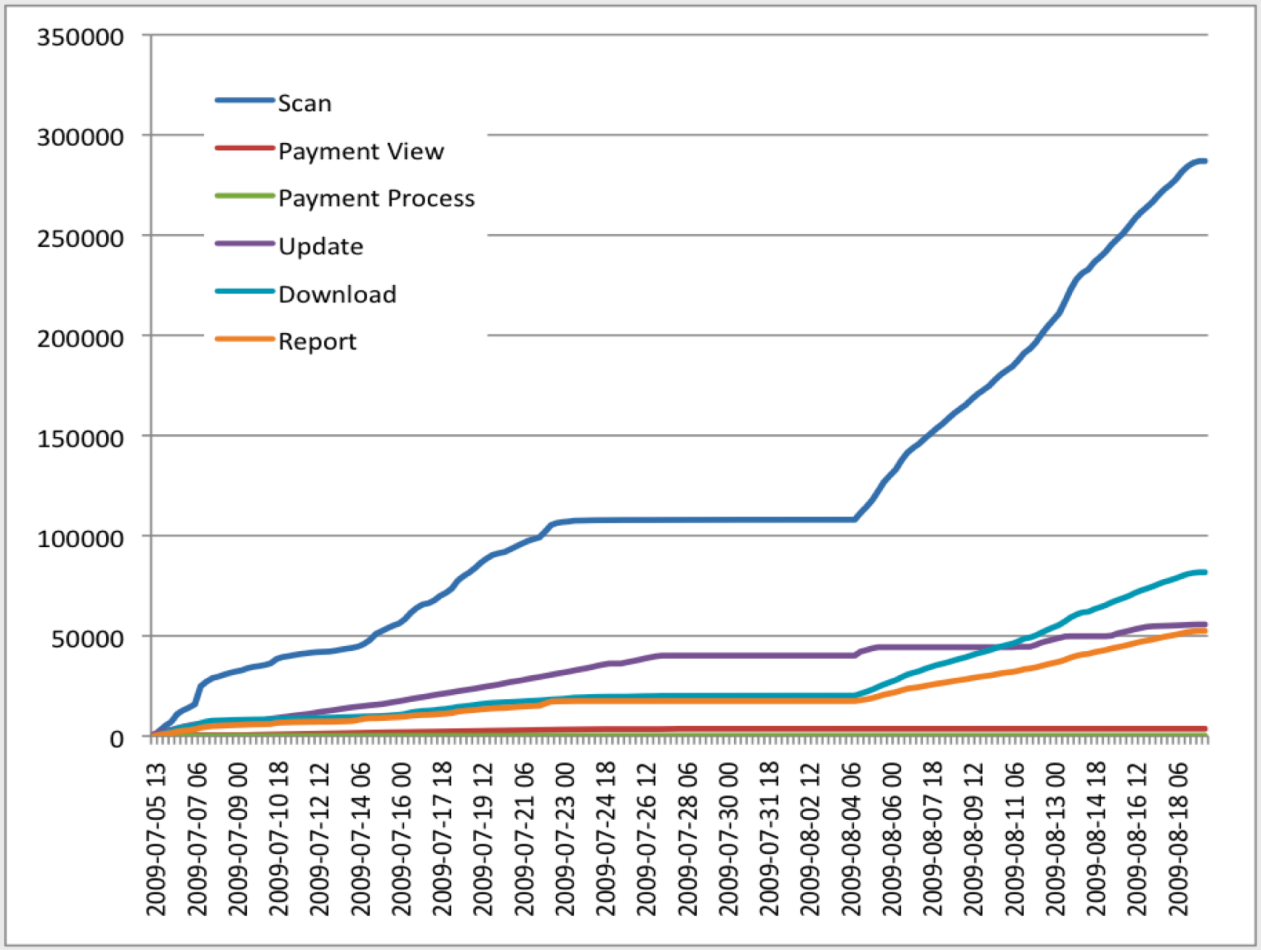
(Potential) Victim Geolocation



Request Types

- Scan
- Download
- Update
- Payment form
- Payment confirmation
- Report

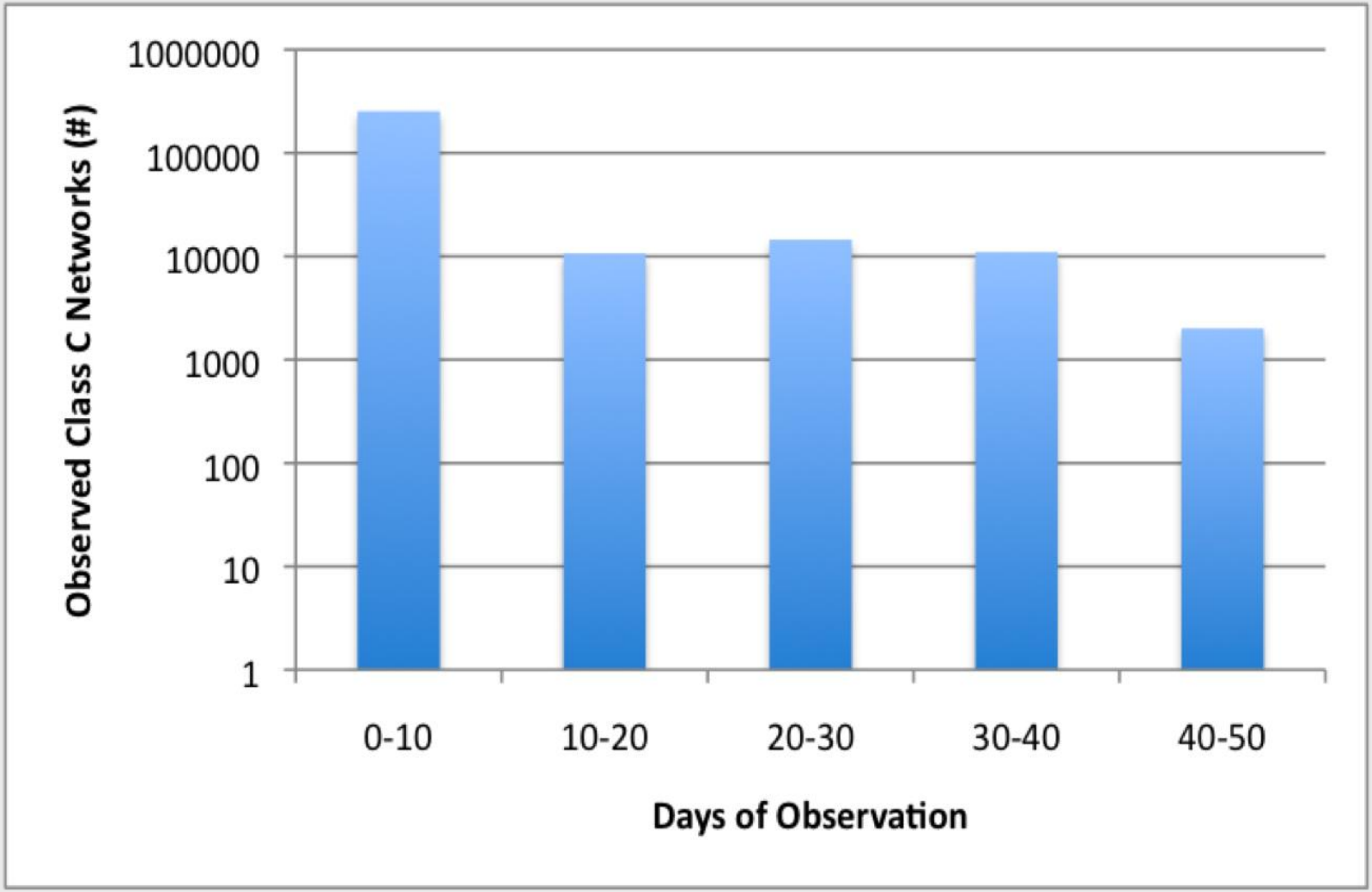
Rogue AV Effectiveness



On sites we monitored:

- 1.26% of users visit payment page
- 0.03% attempt to complete purchase

Interaction Duration



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