Effective Malware Defense via Network-Centric Behavior-Based Learning

Roberto Perdisci

perdisci@cs.uga.edu

The New York Times

U.S.

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINI

POLITICS | EDUCATION | TEXAS

Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks

By ELISABETH BUMILLER
Published: January 27, 2013

WIRED.CO.UK

Search Wired.c

HOME | NEWS | REVIEWS | PHOTOS | VIDEOS | MAGAZINE | POD

Technology | Culture | Science | Business | Gaming | Ideas Bank

Home > News > Technology > Biggest cyber attack Spamhaus

TECHNOLOGY

'Largest cyber attack ever' is happening right now, threatens rest of web

By Ian Steadman | 27 March 13

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS

Stories

Home • News • Stories • 2011 • November • International Cyber Ring That Infected Millions of Computers Dismantled

Twitter | Facebook | Share

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

The New York Times Technology | Personal Tech | Business Day

Bits

JANUARY 4, 2013, 8:33 PM | 21 Comments

U.S. Banks Again Hit by Wave of Cyberattacks

By NICOLE PERLROTH

The New York Times

U.S.

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINI

POLITICS | EDUCATION | TEXAS

Pentagon Expanding Cybersecurity Force to Protect Networks Against Attacks

By ELISABETH BUMILLER
Published: January 27, 2013

WIRED.CO.UK

Search Wired.c

HOME | NEWS | REVIEWS | PHOTOS | VIDEOS | MAGAZINE | POD

Technology | Culture | Science | Business | Gaming | Ideas Bank

Home > News > Technology > Biggest cyber attack Spamhaus

TECHNOLOGY

'Largest cyber attack ever' is happening right now, threatens rest of web

By Ian Steadman | 27 March 13

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS

...nternational Cyber Ring That Infected Millions of Computers Dismantled

...are

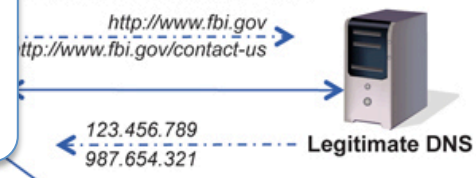
Impact of malicious software (**malware**)

- Identity Theft
- Online Bank Robberies
- Espionage
- DDoS attacks
- Phishing
- Spam
- ...

Your Computer Infected?

...an Internet service that converts user-friendly domain ...numerical addresses that allow computers to talk to each ...servers operated by Internet service providers, computer ... web sites, send e-mail, or connect to any Internet services.

... computers around the world with malware called ...o control DNS servers. As a result, the cyber thieves have ...dulent websites, interfered with their web browsing, and ...o other kinds of malicious software.



The New York Times Technology | Personal Tech | Business Day

Bits

JANUARY 4, 2013, 8:33 PM | 21 Comments

U.S. Banks Again Hit by Wave of Cyberattacks

By NICOLE PERLROTH

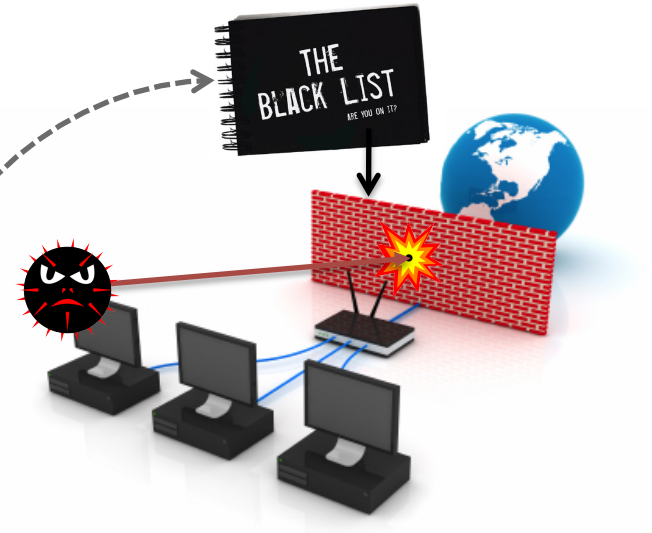
Current Defenses

Challenges:
- code obfuscation
- < 30% detection

file scan

Challenges:
- malware agility
- high TN rate

URL blacklisting



Challenges:
- anti-sandboxing
- scalability

sandboxing

focus mostly limited to characteristics of malware files

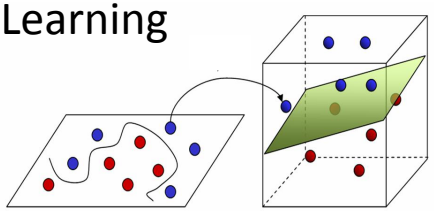
Research Statement

Radically improve the state-of-the-art of malware defense systems

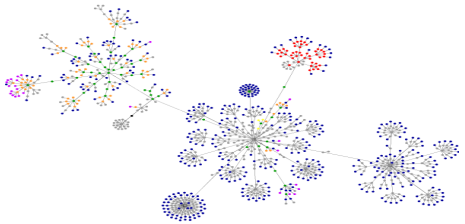
My Approach: Hybrid Behavior-Based Defenses

Network Security

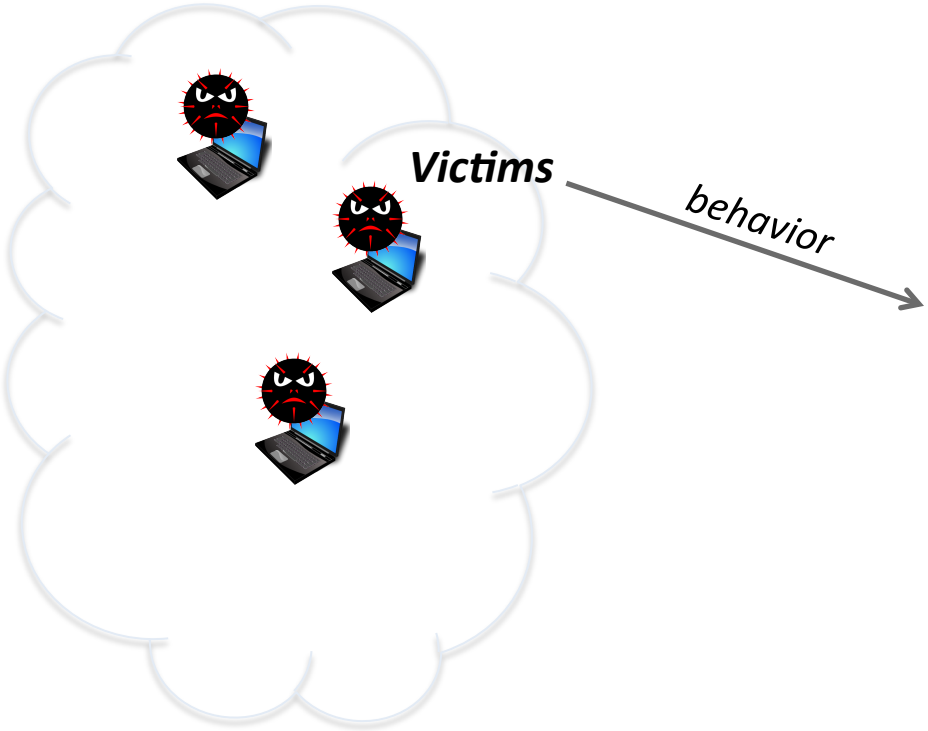
Machine Learning



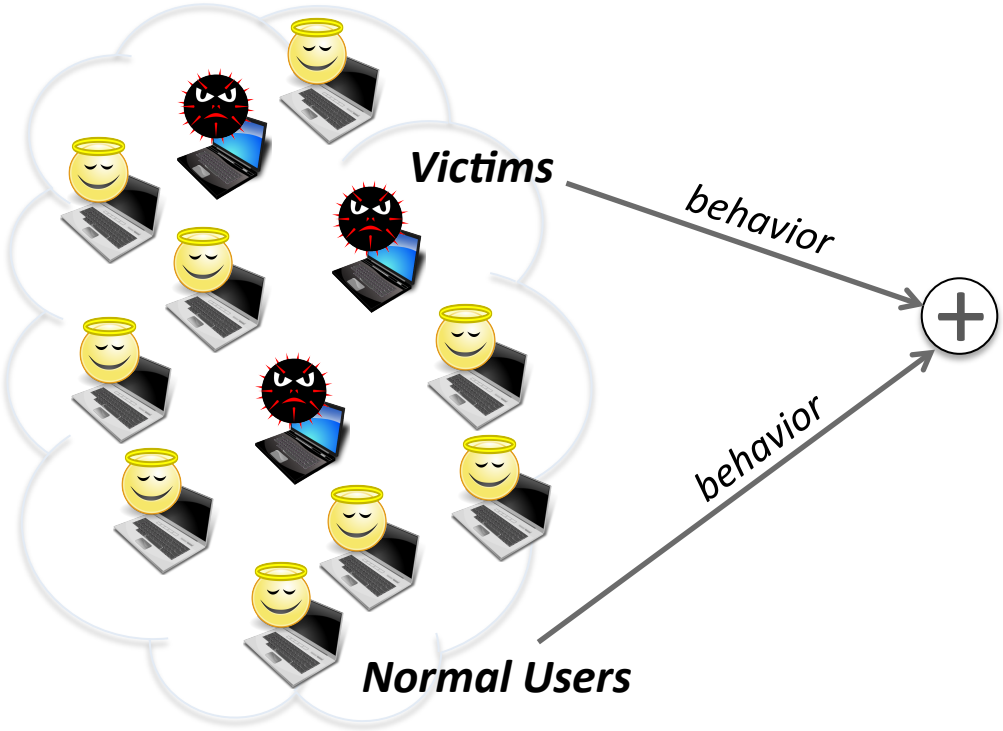
Big Data Mining



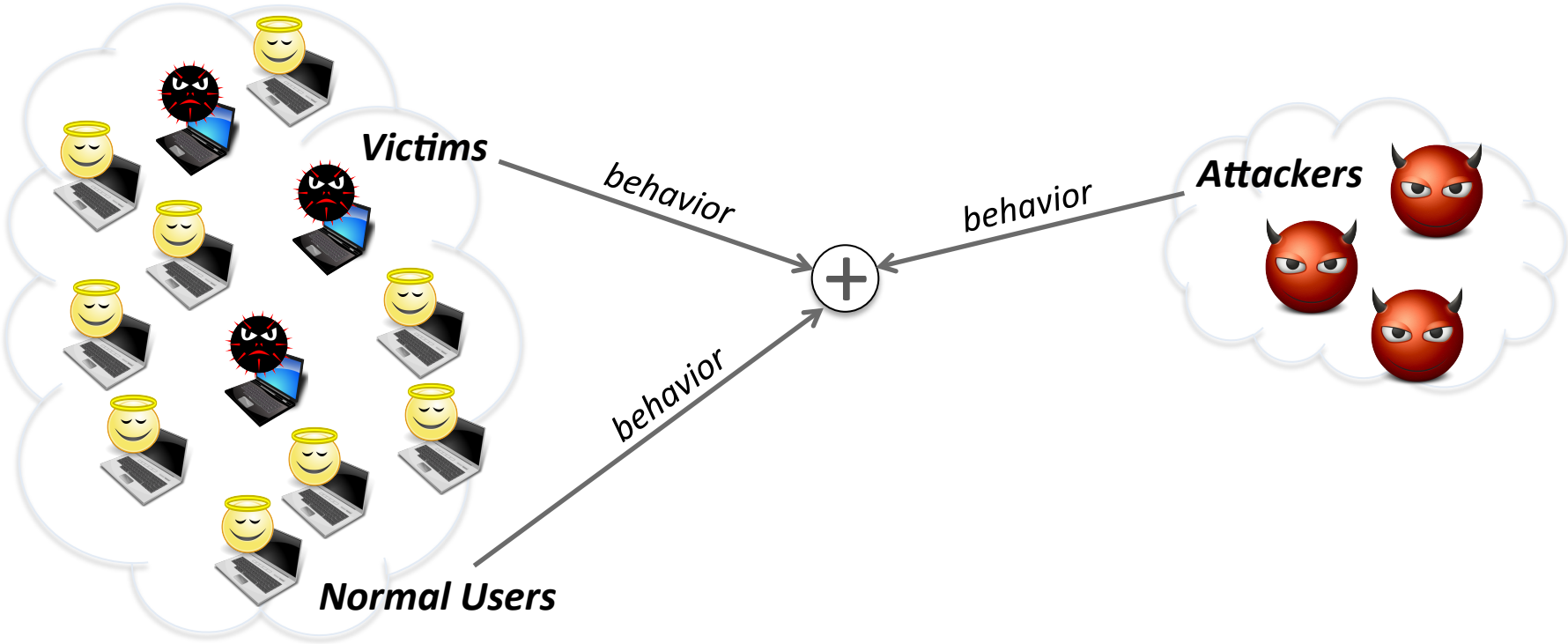
Hybrid Behavior-Based Defense



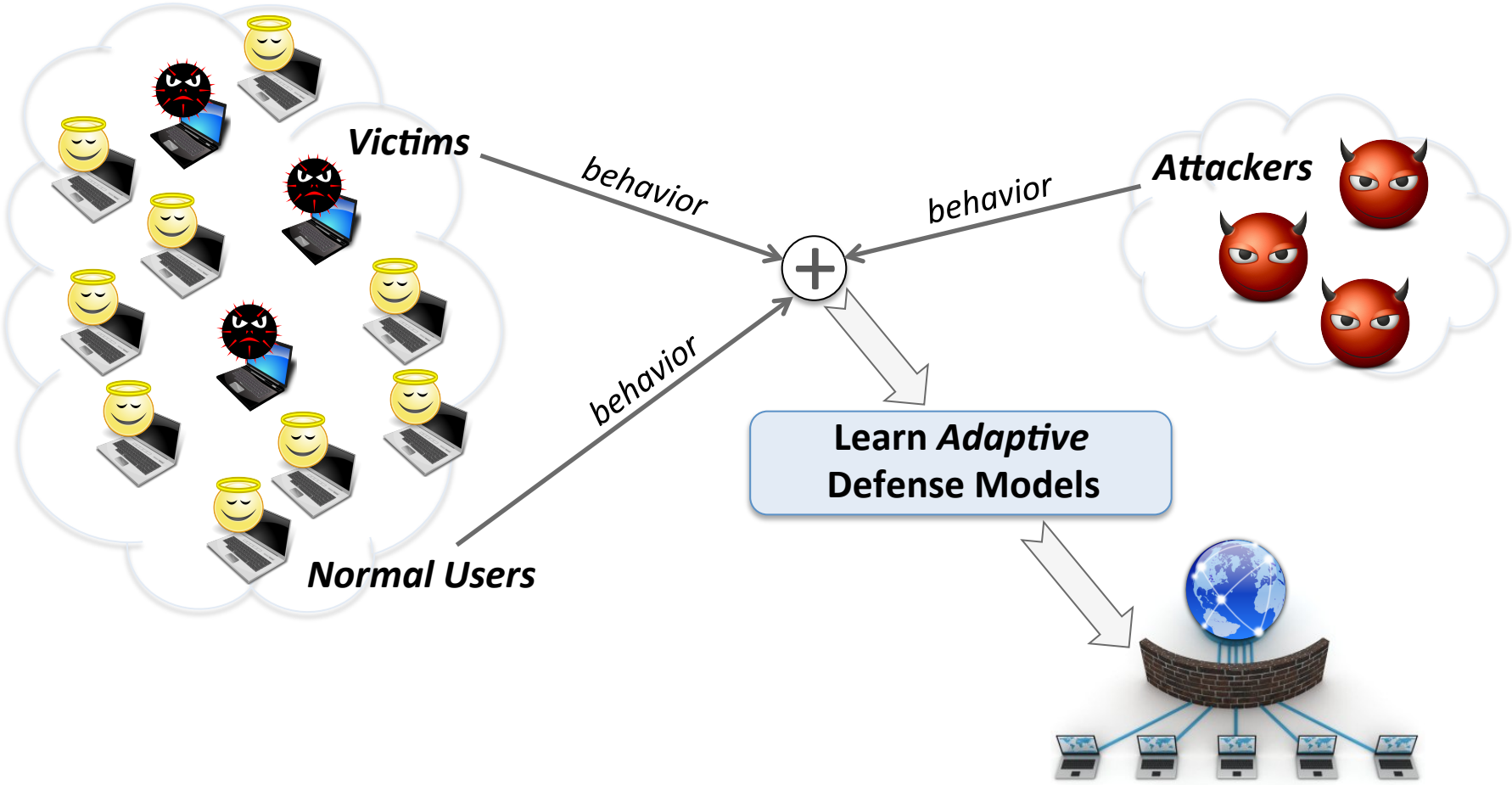
Hybrid Behavior-Based Defense



Hybrid Behavior-Based Defense

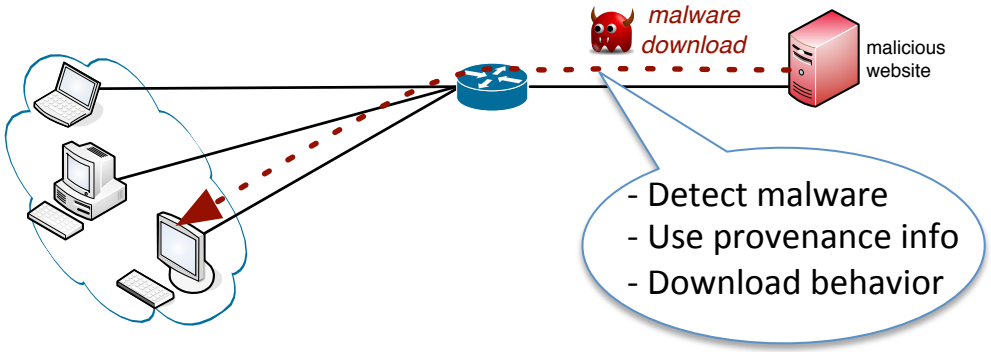


Hybrid Behavior-Based Defense



Measuring and Detecting Malware Downloads in Live Network Traffic

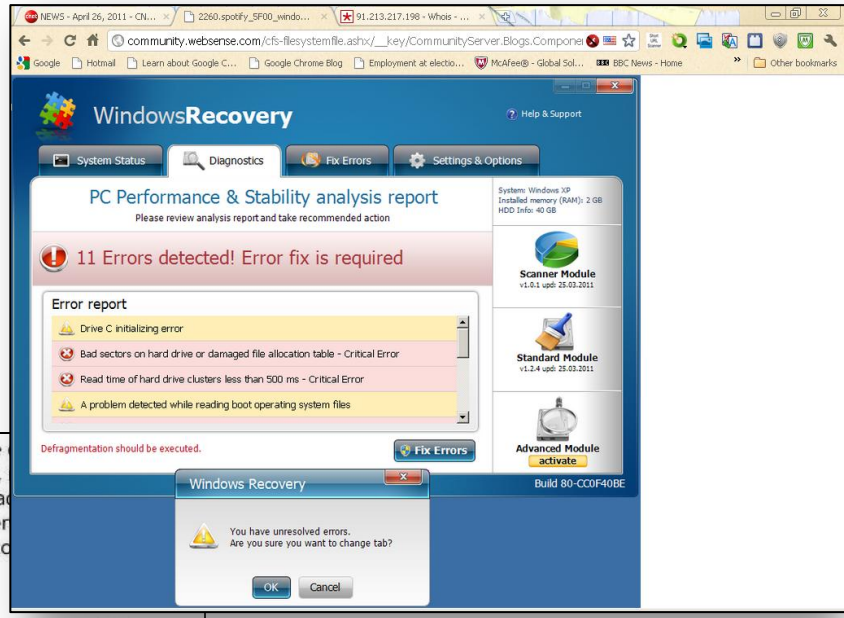
Phani Vadrevu[1], Babak Rahbarinia[1],
Roberto Perdisci[1,2], Kang Li[1], Manos Antanokakis[3]
[1]University of Georgia, [2]Georgia Tech, [3]Damballa Labs

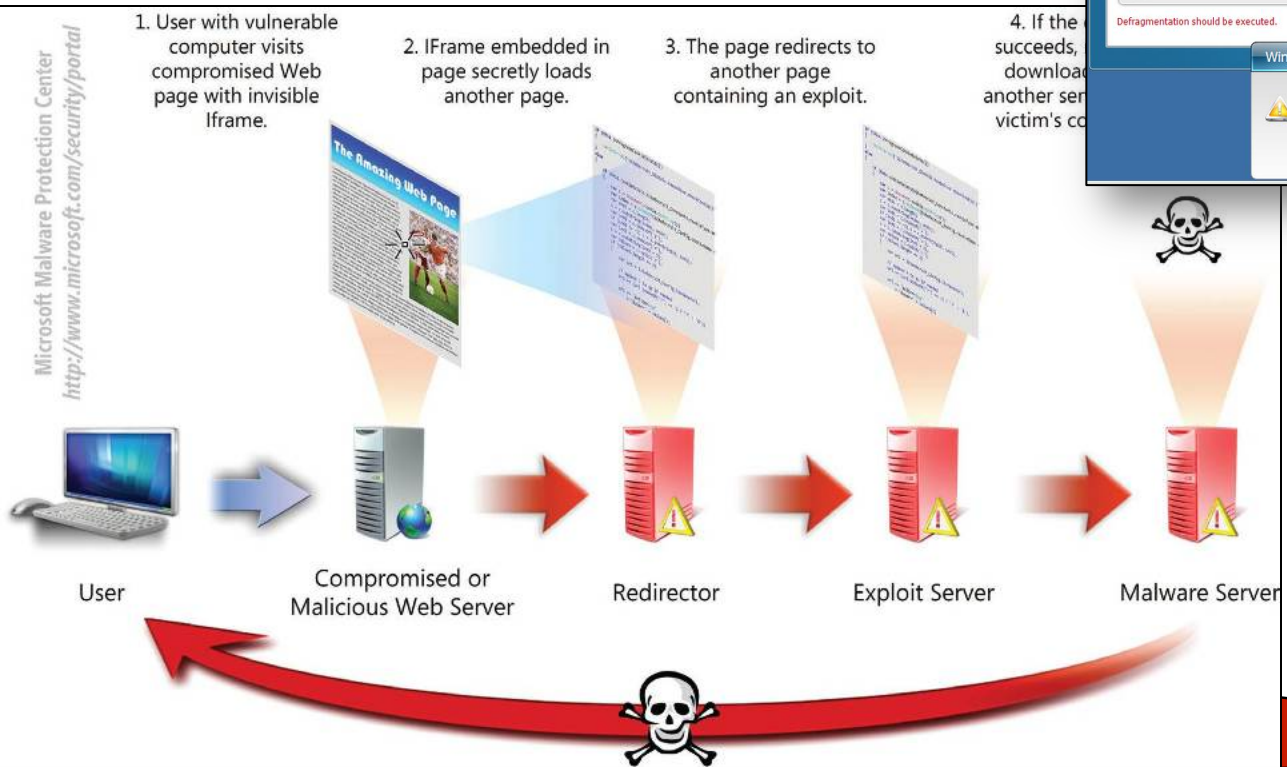


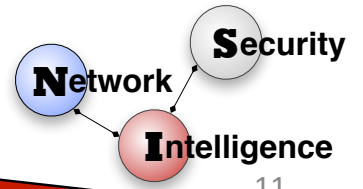
http://amico.googlecode.com

Malware Downloads

- Social Engineering Attacks
- Drive-by downloads







Existing Solutions

AV Signatures

- Code obfuscation / Polymorphism, lots of FNs

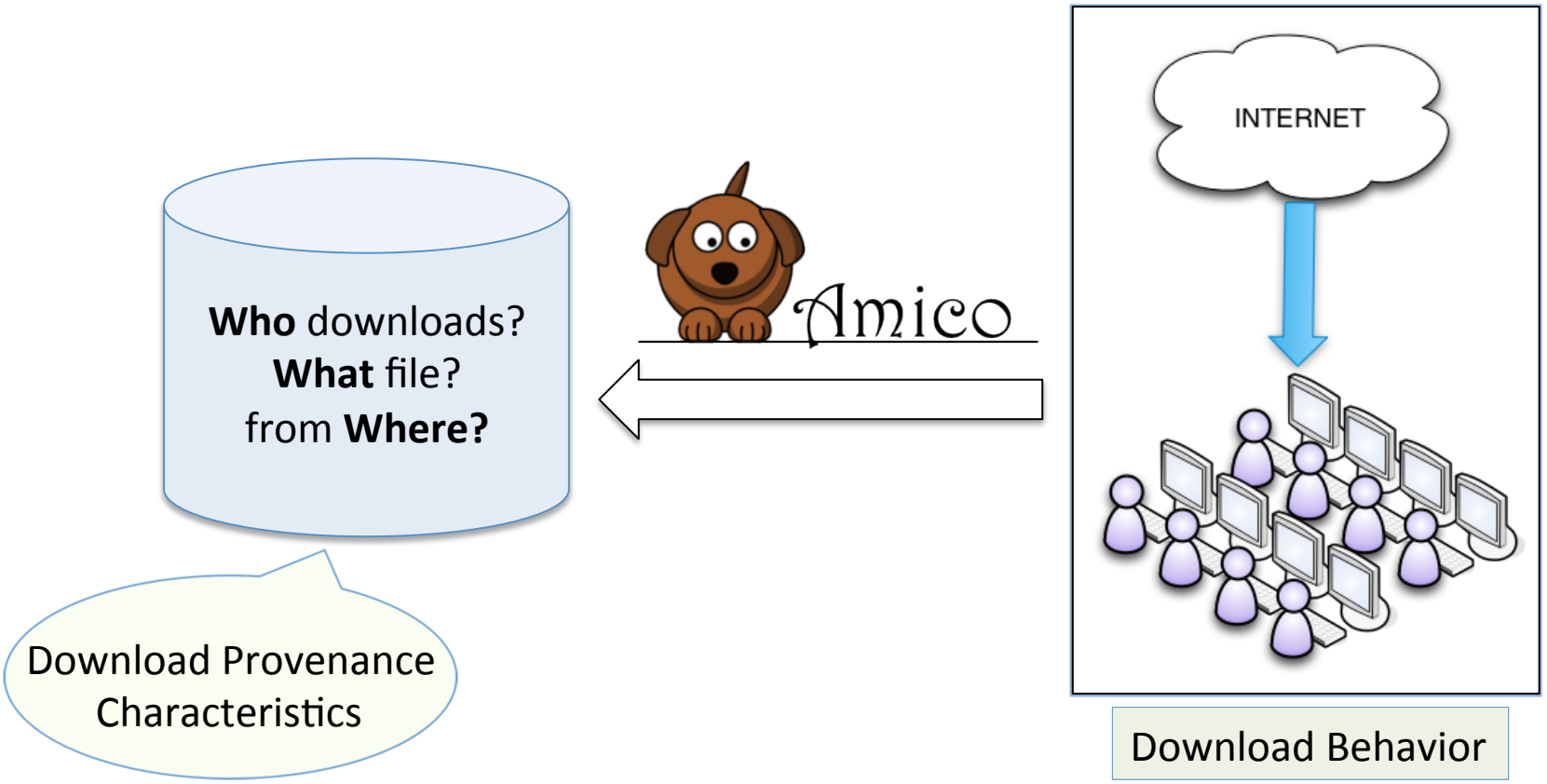
URL Blacklists

- Mainly static, lots of FNs

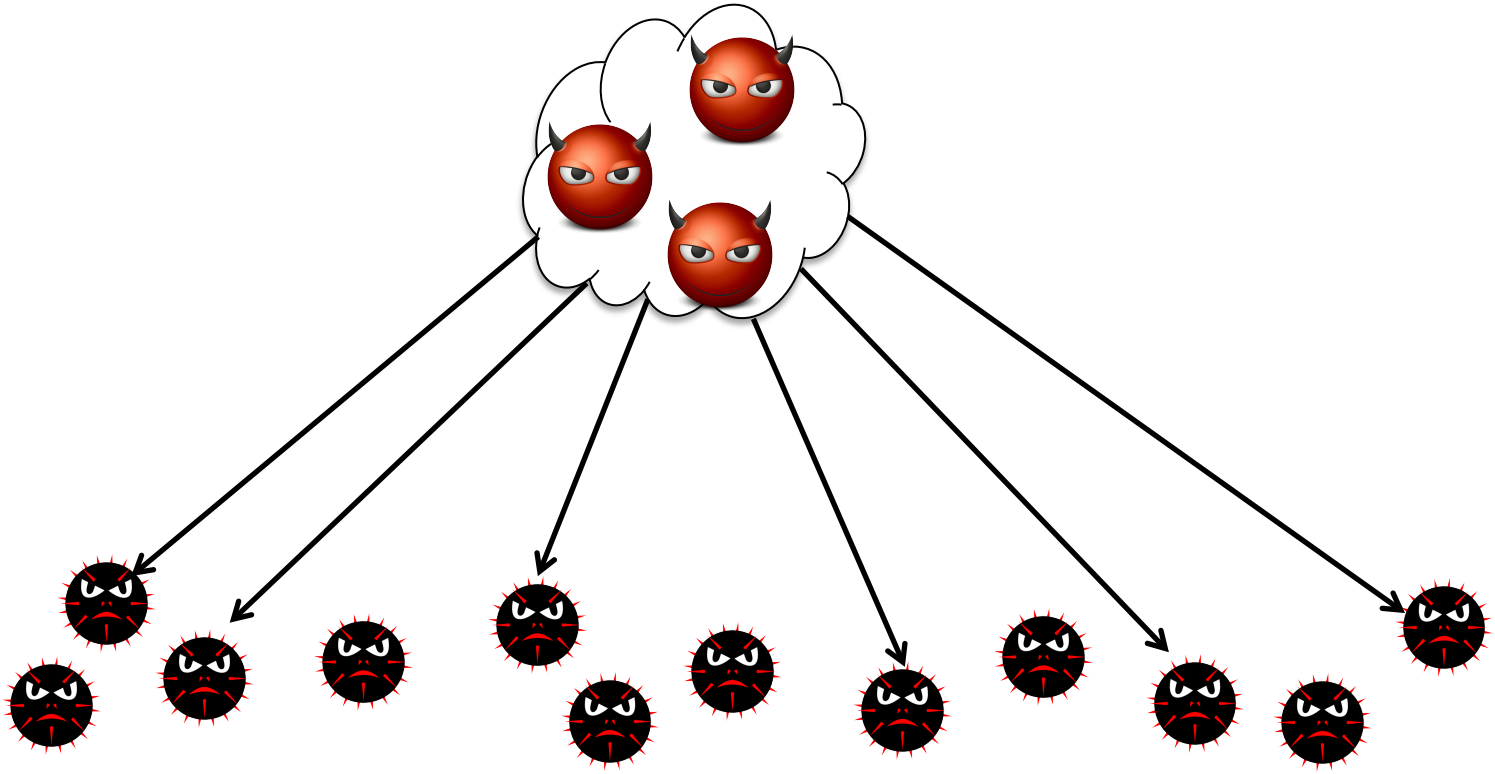
DNS/IP Reputation Systems

- Dynamic, but lots of FPs

Accurate Malware Identification via Classification of live network traffic Observations

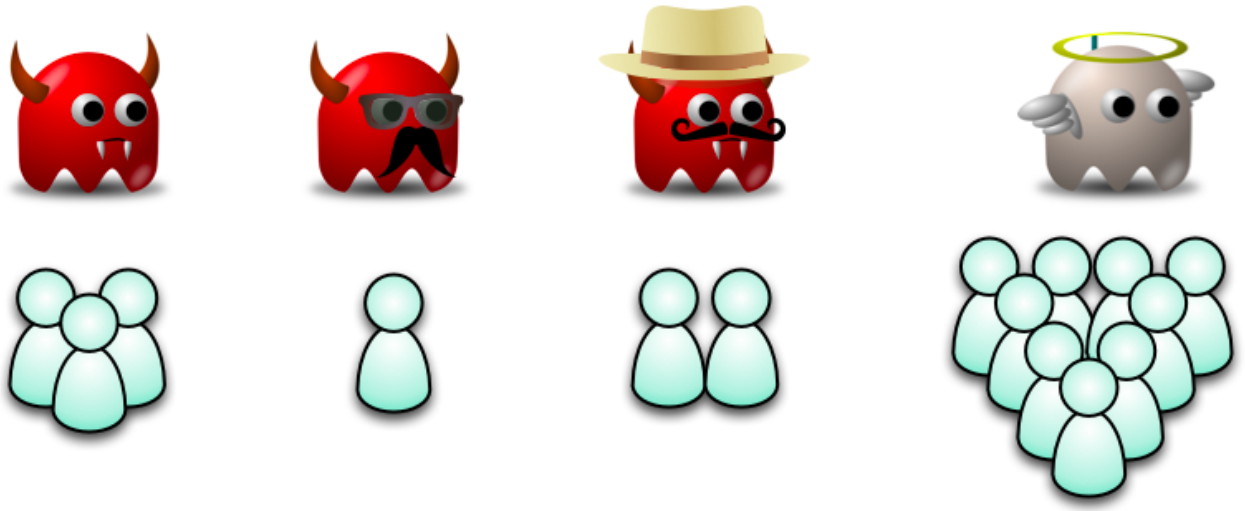


How is Malware Distributed?



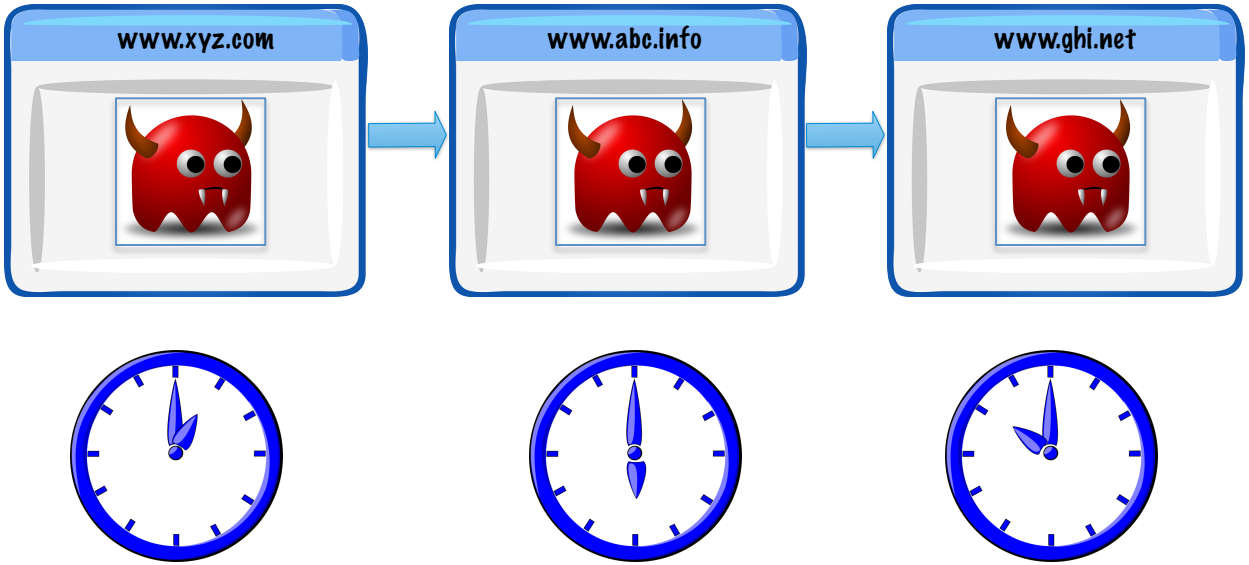
Malware Distribution Operations are “Agile”

	Malware	Benign EXEs
File content	changes frequently	is very stable



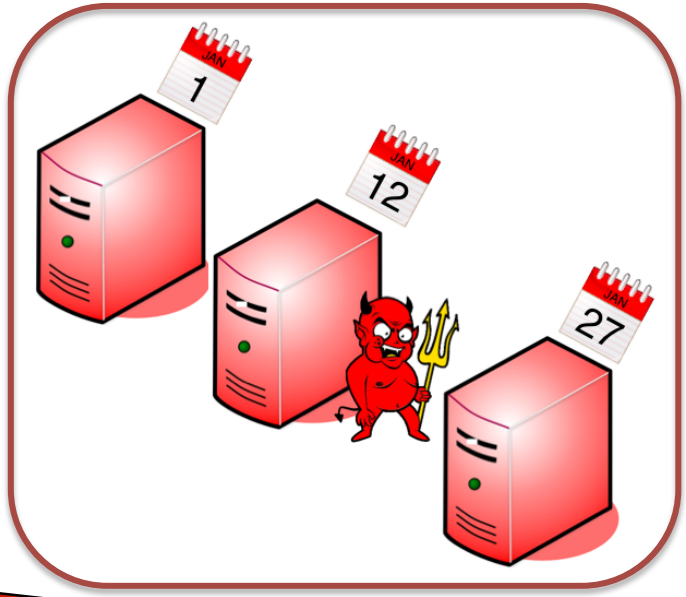
Malware Distribution Operations are "Agile"

	Malware	Benign EXEs
File content	changes frequently	is very stable
Domain names	**change frequently**	**are very stable**



Malware Distribution Operations are "Agile"

	Malware	Benign EXEs
File content	changes frequently	is very stable
Domain names	change frequently	are very stable
IPs	**change somewhat frequently**	**are relatively stable**

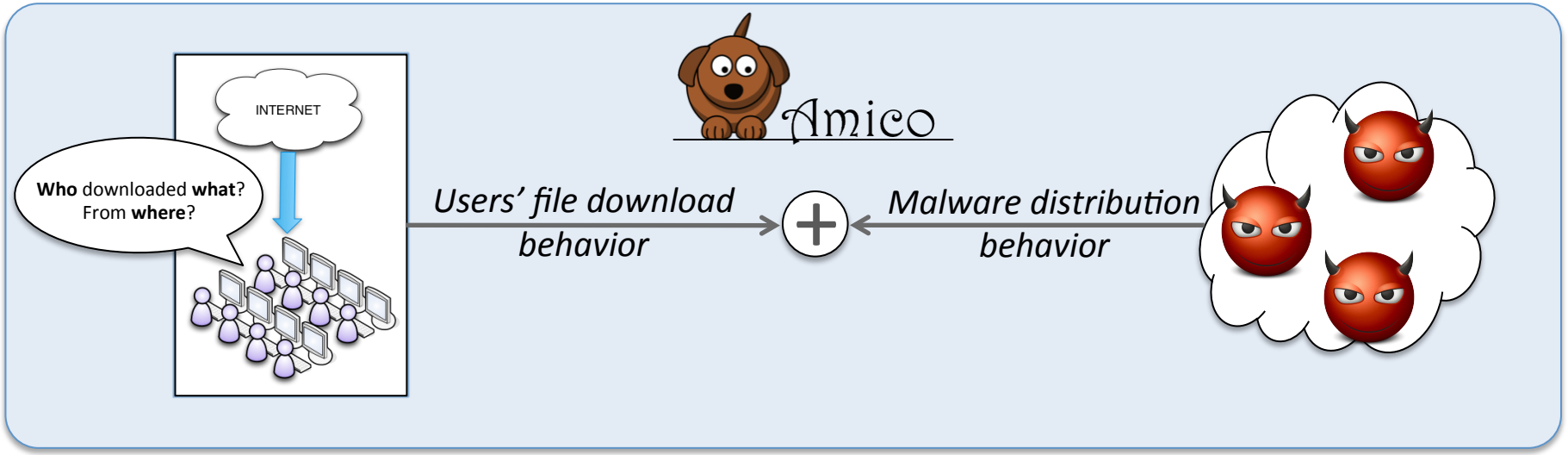


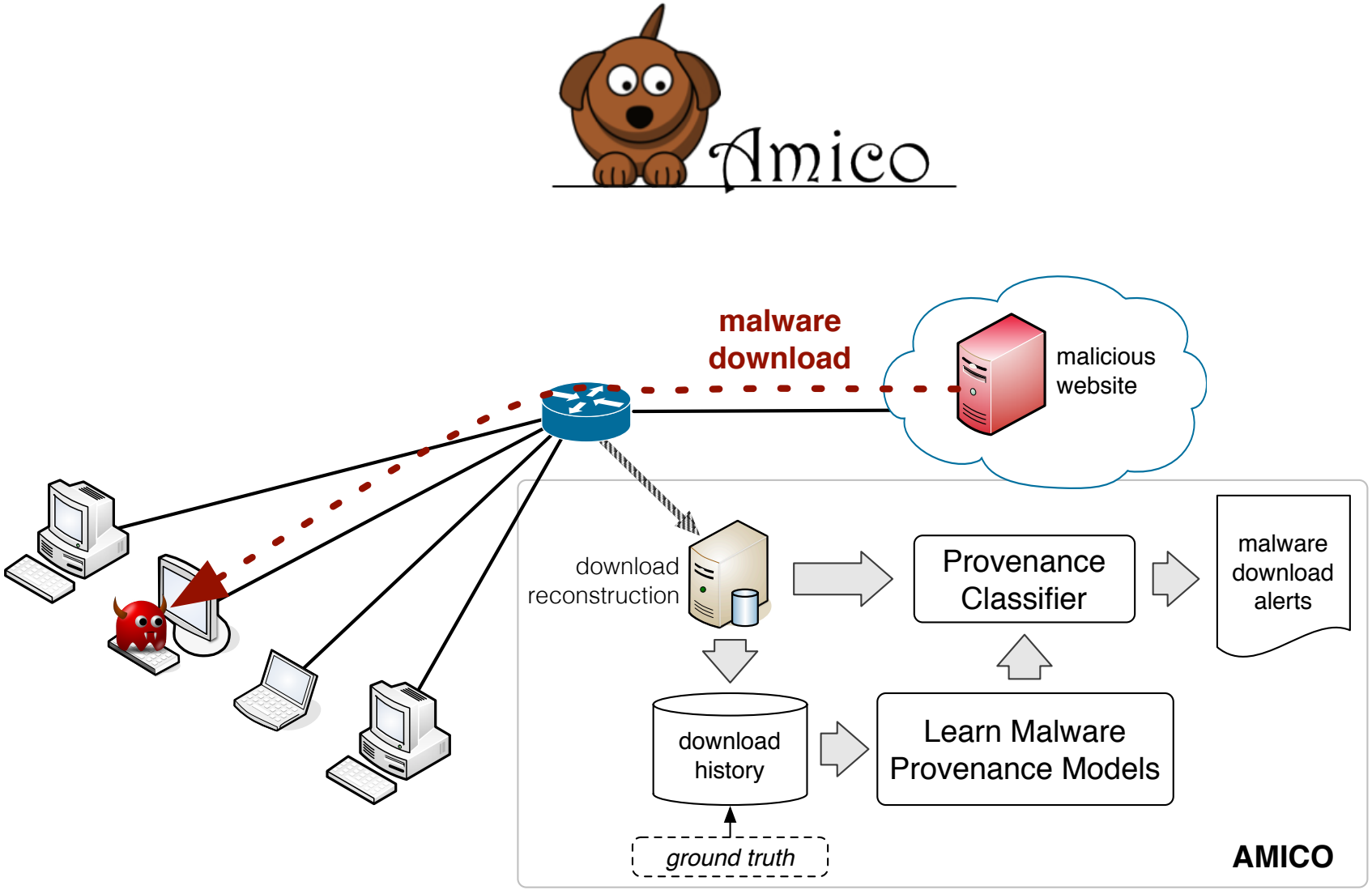
date	md5	host	server	avs
2013-09-09	26b69ac7f022efc52ffd244cca379d1d	com.servehttp.qbkgwrwrxt	78.138.103.226	
2013-09-09	40144bbcc43fd13bb6747739f0883dea	com.servehttp.vewsqnxip	78.138.103.226	
2013-09-08	6aa24a2c3cce53d00c1825c0aaa03594	com.servehttp.npvfndow	78.138.103.226	
2013-09-08	a84f22ff4ca0ea62a18fe286cf0121ef	com.servehttp.npvfndow	78.138.103.226	
2013-08-22	831d898e75aa6fa57edb0f495c1a7989	com.servehttp.efrrerrms	212.7.195.124	
2013-08-22	ab2aadc3f11b79a4672ed4330492c7a0	com.servehttp.efrrerrms	212.7.195.124	
2013-08-22	d3131fac1e4857951a592e0ed4ee4db5	com.servehttp.wryvisox	212.7.195.124	
2013-08-21	fd8ef9d08125e45fff182f190ba38b96	com.myvnc.sqekewrsrt	212.7.195.124	
2013-08-12	00b3f13c8b1f9c5fd159099ec7bae68d	com.myvnc.ioggijxems	212.7.195.122	
2013-07-29	2fb418ae2fb0d539d78270505d3bb468	com.myvnc.lvpgzfylxd	212.7.195.120	
2013-07-10	7bf95ca51ab3ae36a55c34ec86dda1bd	biz.myftp.atzlmxf	212.7.195.111	
2013-06-21	0482b01ac3bf6dc777690ef4d83d1b14	com.servehttp.vtsqisngb	212.7.199.29	
2013-06-21	1b757b9221a6c2ef1c44326f3f264a57	com.servehttp.xsbgefk	212.7.199.29	
2013-06-21	2218d338236d70fdfaf2a9f14d816399	com.servehttp.nlpsumav	212.7.199.29	
2013-06-21	2abdca63a4f5ed282c6c0f35486c4b0d	com.servehttp.olqdezzd	212.7.199.29	
2013-06-21	2d09812679ad6273156987adbf4c74d3	com.servehttp.xsbgefk	212.7.199.29	
2013-06-21	2f069234985c95a3ad1f4307b6a92e4e	com.servehttp.xvyrscdire	212.7.199.29	
2013-06-21	72ec9d51735765d08b7747b7efb9c945	com.servehttp.vtsqisngb	212.7.199.29	
2013-06-21	da670e94ce9079a659b819370dac0e06	com.servehttp.pgxsbyw	212.7.199.29	
2013-06-21	f23c104b52d712f700d4e98d58fb752c	com.servehttp.ejkukehex	212.7.199.29	
2013-06-20	0792d91194c07306555ec8cd5d58ff12	com.servehttp.kwbhidcsjq	212.7.199.29	
2013-06-20	10ecf6c608125c69e2242746f8b3ac72	com.servehttp.batslbdii	212.7.199.28	
2013-06-20	b5251b085ef708348f8ea6fd782aa143	com.servehttp.jsjdvxosvq	212.7.199.28	
2013-06-20	b5251b085ef708348f8ea6fd782aa143	com.servehttp.xbnaiaqt	212.7.199.28	
2013-06-20	bc3cc9dd1756277353535345267777e200	com.servehttp.vkcercgrbq	212.7.199.28	1
2013-06-20	d298e8a52e889d77ed30b45878275b3b	com.servehttp.kwbhidcsjq	212.7.199.29	
2013-06-20	f8c2da632f2ef89b55fd97315c05eef4	com.servehttp.batslbdii	212.7.199.28	
2013-06-19	056c00a8dabe23c452b8b45e449d336b	com.servehttp.odjeiup	212.7.199.28	1
2013-06-19	7b81cbe11e2219d38543343c91135ebe	com.servehttp.ebzmuzlag	212.7.199.28	1
2013-06-19	7b81cbe11e2219d38543343c91135ebe	com.servehttp.qmcbidam	212.7.199.28	1
2013-06-19	7b81cbe11e2219d38543343c91135ebe	com.servehttp.vyubcjpkjo	212.7.199.28	1
2013-06-19	930fe87f86398f2f7111ae123425535b	com.servehttp.aldrrhmqyt	212.7.199.28	1
2013-06-19	ffe70a8aa9afc617ab705f0df4b1e531	com.servehttp.ebzmuzlag	212.7.199.28	
2013-06-18	6b06886f9dfce2ad64efbde86fadd5ed	net.sytes.cjfiocen	212.7.199.27	
2013-06-18	6b06886f9dfce2ad64efbde86fadd5ed	net.sytes.wlhxlcadj	212.7.199.27	
2013-06-18	80fe9e7645800f5baac9eaf3990d9a70	net.sytes.syzoxzfwh	212.7.199.27	
2013-06-18	b1b84738f4ae7ab7db21e55e9ed5767b	net.sytes.raidaicmhd	212.7.199.27	
2013-06-17	4a5dda470319eb3ba2ec0ca1bbeae5dc	net.sytes.bssbmazn	212.7.199.27	

(38 rows)

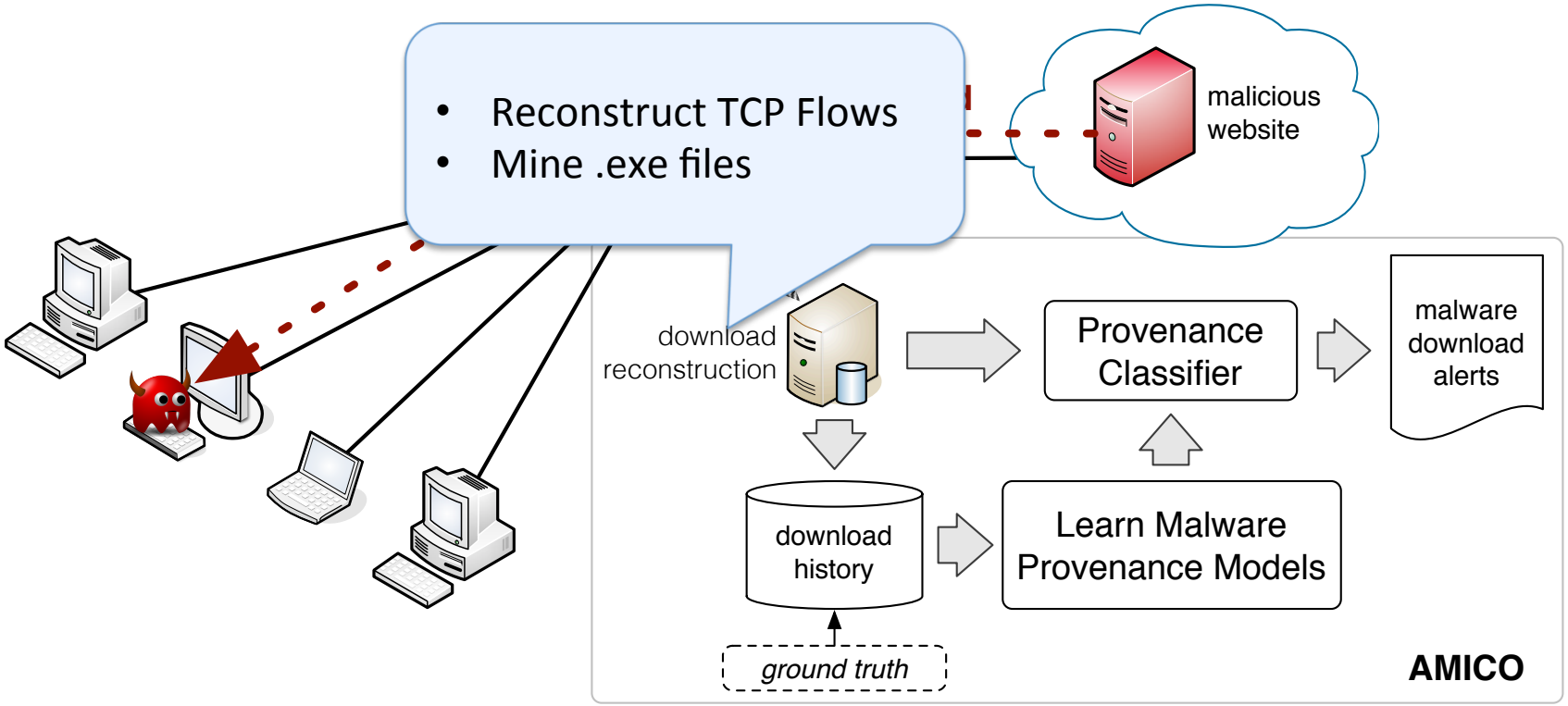
date	host	server	substring
2013-09-09	com.servehttp.qbkgwrwrxt	78.138.103.226	/index.php?c=RaEQL35QhmE7hpsF36yBUnT13rfyVW/Ug8Sn2nZXeo/Ynfh
2013-09-09	com.servehttp.vewsqnxip	78.138.103.226	/index.php?c=RaEQL35QhmE7hpsF36yBU3X127PgW2GSiNy+2HVZf8nAluV
2013-09-08	com.servehttp.npvfndow	78.138.103.226	/index.php?c=RaEQL35QhmE7hpsF36yBUHv13rHyVW/Ug8Sn2nZXeo/Ynfh
2013-08-22	com.servehttp.wryvisox	212.7.195.124	/index.php?c=RaEQL35QhmE7hpsF36yBU3z13rHyVW/Ug8Sn2nZXeo/Ynfh
2013-08-22	com.servehttp.efrrerrms	212.7.195.124	/index.php?c=RaEQL35QhmE7hpsF36yBVHriwbfwVW/Ug8Sn2nZXeo/Ynfh
2013-08-21	com.myvnc.sqekewrsrt	212.7.195.124	/index.php?c=RaEQL35QhmE7hpsF36yBUHv13rLzVW/Ug8Sn2nZXeo/Ynfh
2013-08-12	com.myvnc.ioggijxems	212.7.195.122	/index.php?c=RaEQL35QhmE7hpsF36yBUn/13rD0VW/Ug8Sn2nZXeo/Ynfh
2013-07-29	com.myvnc.lvpgzfylxd	212.7.195.120	/index.php?c=RaEQL35QhmE7hpsF36yBU3j117DgW2GSiNy+2HVZf8nAluV
2013-07-10	biz.myftp.atzlmxf	212.7.195.111	/index.php?c=RaEQL35QhmE7hpsF36yBU3z13rDzVW/Ug8Sn2nZXeo/Ynfh
2013-06-21	com.servehttp.nlpsumav	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBXXj13bD7VW/Ug8Sn2nZXeo/Ynfh
2013-06-21	com.servehttp.xsbgefk	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBVHnrwbz6VW/Ug8Sn2nZXeo/Ynfh
2013-06-21	com.servehttp.vtsqisngb	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBU3z13rPgW2GSiNy+2HVZf8nAluV
2013-06-21	com.servehttp.ejkukehex	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBVH/uwbXzRWHaxc+/w3RUdIqehfN
2013-06-21	com.servehttp.olqdezzd	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBVHXvwbz6VW/Ug8Sn2nZXeo/Ynfh
2013-06-21	com.servehttp.xvyrscdire	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBU3j13bbzVW/Ug8Sn2nZXeo/Ynfh
2013-06-21	com.servehttp.pgxsbyw	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBVH3pwbb7VW/Ug8Sn2nZXeo/Ynfh
2013-06-20	com.servehttp.vkcercgrbq	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBUnX13L3gW2GSiNy+2HVZf8nAluV
2013-06-20	com.servehttp.xbnaiaqt	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBVHziwbHlVW/Ug8Sn2nZXeo/Ynfh
2013-06-20	com.servehttp.kwbhidcsjq	212.7.199.29	/index.php?c=RaEQL35QhmE7hpsF36yBUnT13rPzVW/Ug8Sn2nZXeo/Ynfh
2013-06-20	com.servehttp.jsjdvxosvq	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBU3X13rHgW2GSiNy+2HVZf8nAluV
2013-06-20	com.servehttp.batslbdii	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBU3z13rPgW2GSiNy+2HVZf8nAluV
2013-06-19	com.servehttp.ebzmuzlag	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBUHv13rzlVW/Ug8Sn2nZXeo/Ynfh
2013-06-19	com.servehttp.qmcbidam	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBVHrowb3wVW/Ug8Sn2nZXeo/Ynfh
2013-06-19	com.servehttp.odjeiup	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBV3z13r33VW/Ug8Sn2nZXeo/Ynfh
2013-06-19	com.servehttp.vyubcjpkjo	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBVH7uwbX6T2Haxc+/w3RUdIqehfN
2013-06-19	com.servehttp.aldrrhmqyt	212.7.199.28	/index.php?c=RaEQL35QhmE7hpsF36yBVHzswb3yVW/Ug8Sn2nZXeo/Ynfh
2013-06-18	net.sytes.syzoxzfwh	212.7.199.27	/index.php?c=RaEQL35QhmE7hpsF36yBXHX12bbgW2GSiNy+2HVZf8nAluV
2013-06-18	net.sytes.cjfiocen	212.7.199.27	/index.php?c=RaEQL35QhmE7hpsF36yBUGLo3abuVSeZkMW823tcOdHLi+s
2013-06-18	net.sytes.wlhxlcadj	212.7.199.27	/index.php?c=RaEQL35QhmE7hpsF36yBUn713bbgW2GSiNy+2HVZf8nAluV
2013-06-18	net.sytes.raidaicmhd	212.7.199.27	/index.php?c=RaEQL35QhmE7hpsF36yBU3z13bX2VW/Ug8Sn2nZXeo/Ynfh
2013-06-17	net.sytes.bssbmazn	212.7.199.27	/index.php?c=RaEQL35QhmE7hpsF36yBUHX13bf0VW/Ug8Sn2nZXeo/Ynfh

Attackers' Behavior + Users' Behavior

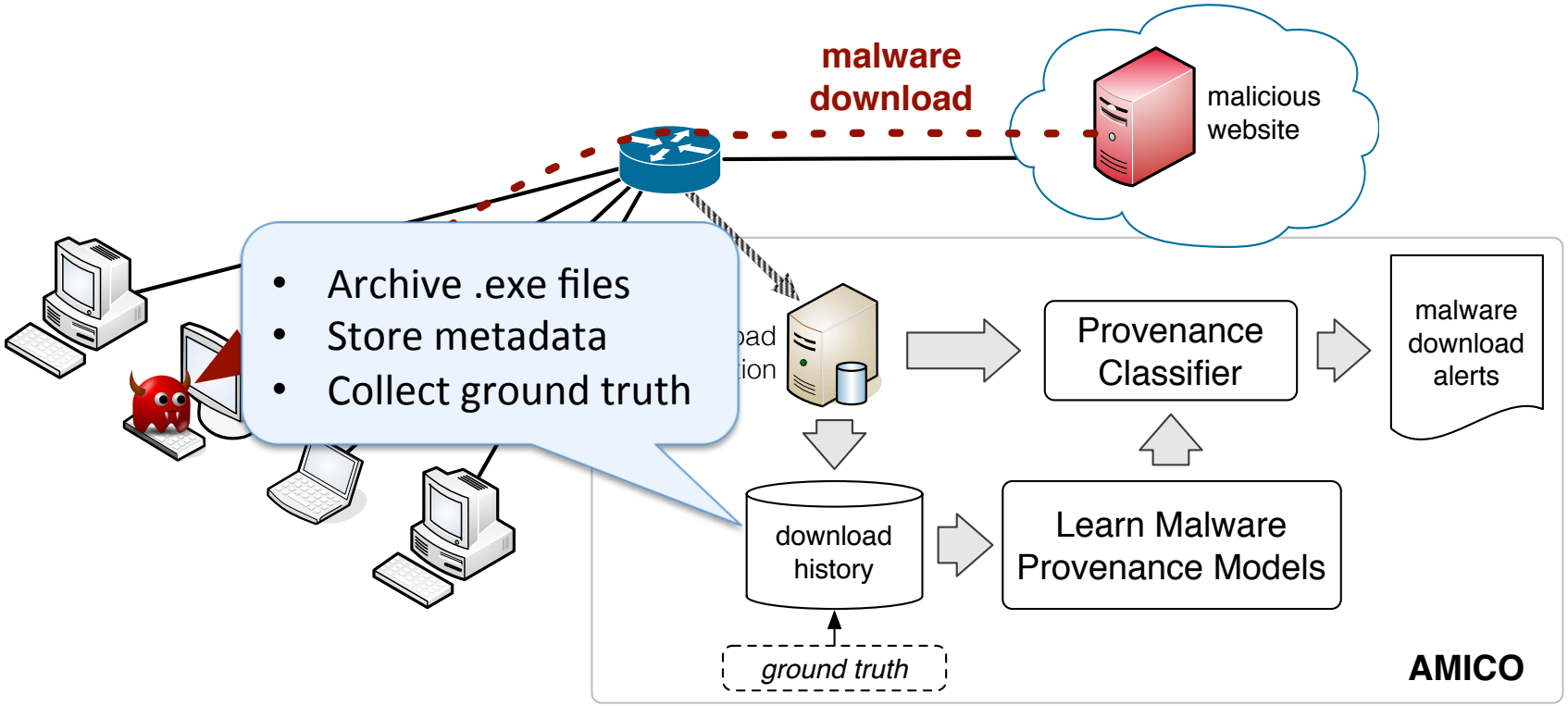



Amico
malware
download
malicious
website
download
reconstruction
Provenance
Classifier
malware
download
alerts
download
history
Learn Malware
Provenance Models
ground truth
AMICO

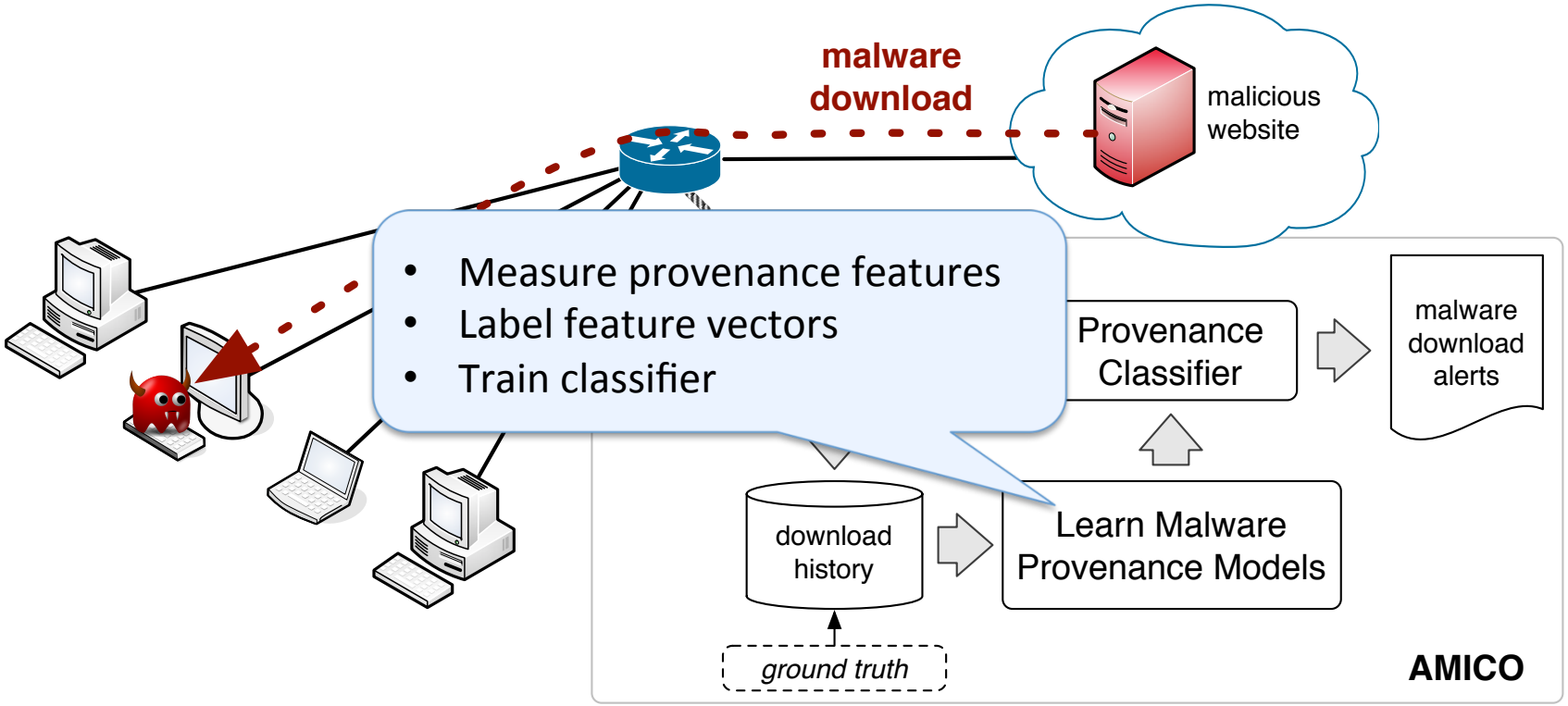
File Reconstruction



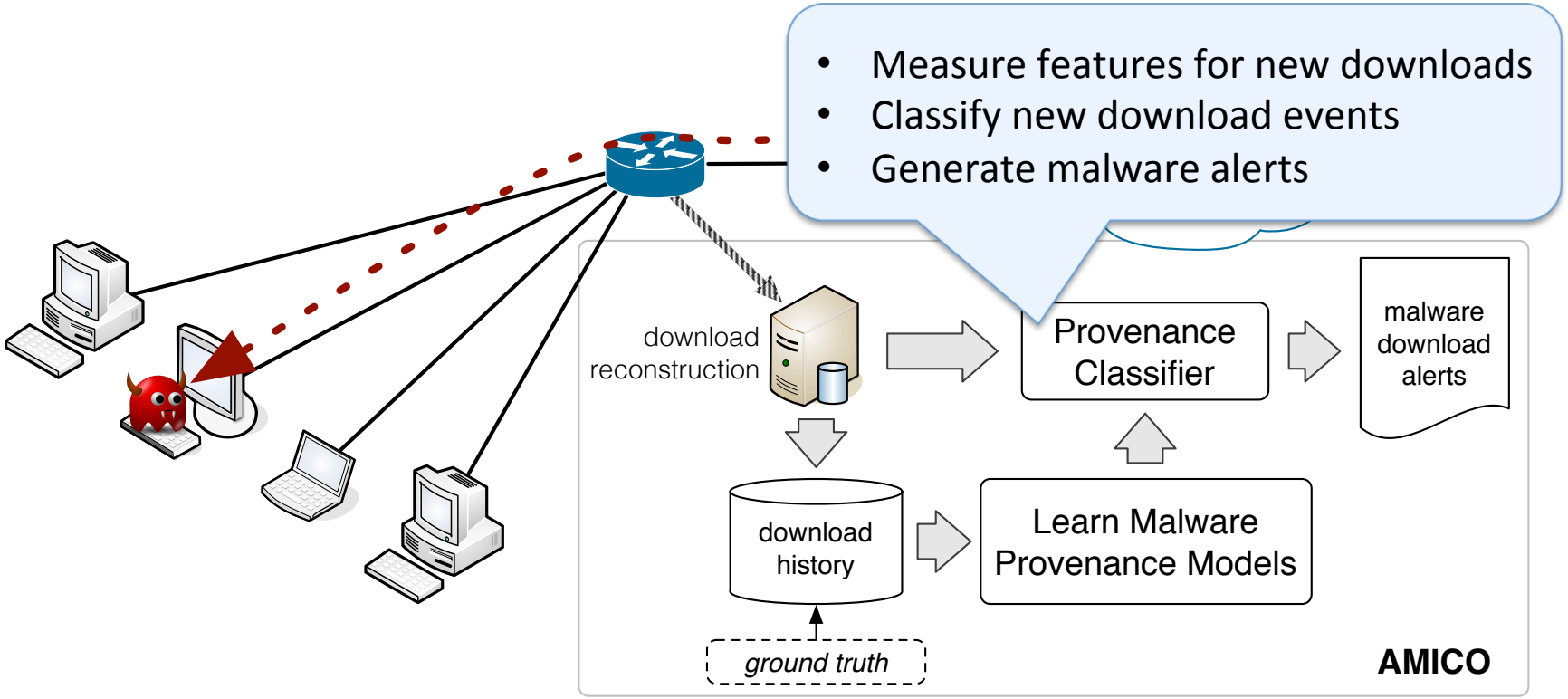
Download History DB



Classifier Training



Provenance Classifier

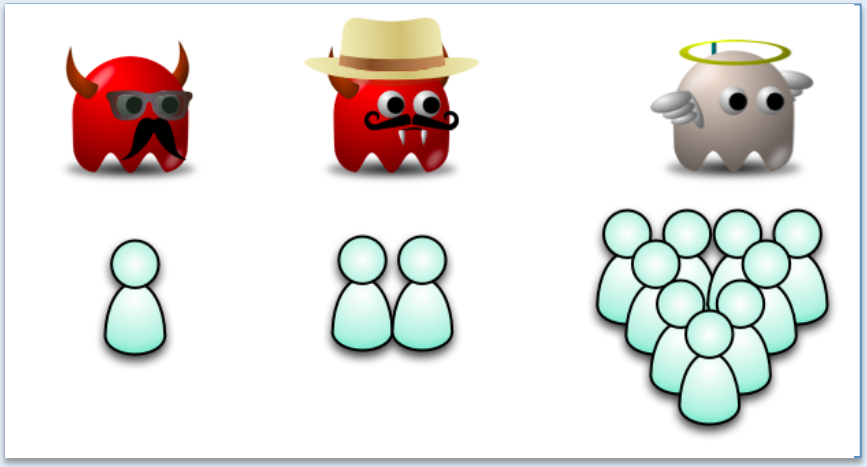


Feature Extraction

- **Past file downloads**
- Domain features
- Server IP features
- URL features
- Download request features

✧ The hash of the downloaded file

1. How many times?
2. How many clients?
3. When was it first seen?

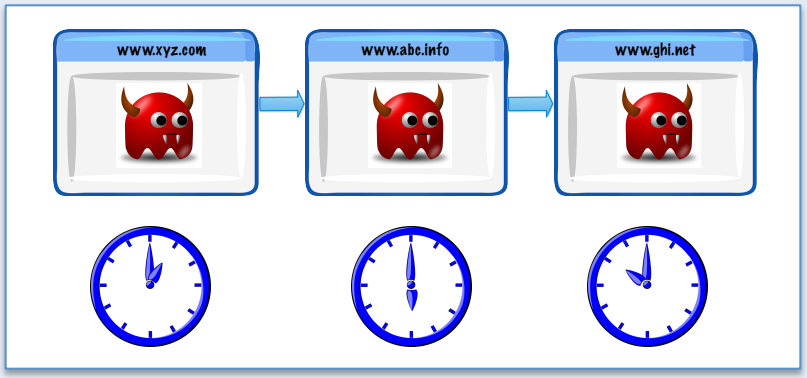


Feature Extraction

- Past file downloads
- **Domain features**
- Server IP features
- URL features
- Download request features

✧ The domain and its 2LD
✧ E.g.: downloads.bbc.co.uk & bbc.co.uk

✧ For both domain & 2LD:
1. # total downloads
2. # benign/malicious downloads
3. Avg. # AV labels



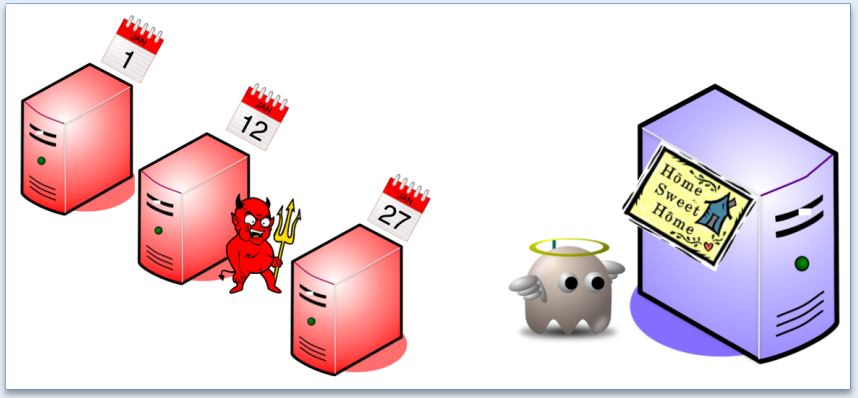
Feature Extraction

- Past file downloads
- Domain features
- **Server IP features**
- URL features
- Download request features

✧ The server IP and its BGP Prefix

✧ For both IP & BGP prefix:

1. # total downloads
2. # benign/malicious downloads
3. Avg. # AV labels



Feature Extraction

- Past file downloads
- Domain features
- Server IP features
- **URL features**
- Download request features

- ✧ The URL & URL structure (regex)
- ✧ Example:
  - ✧ /attach/u?ui=2&ik=69&th=1
  - ✧ /*/*?*=*&*=*&*=*

- ✧ For both URL & URL structure:

1. # total downloads
2. # malware downloads
3. # distinct files downloaded

substring
/index.php?c=RaEQL35QhmE7hpsF36yBUnT13rfyVW/Ug8Sn2nZXeo/Ynfh
/index.php?c=RaEQL35QhmE7hpsF36yBU3X127PgW2GSiNy+2HVZf8nAluV
/index.php?c=RaEQL35QhmE7hpsF36yBUHv13rHyVW/Ug8Sn2nZXeo/Ynfh
/index.php?c=RaEQL35QhmE7hpsF36yBU3z13rHyVW/Ug8Sn2nZXeo/Ynfh
/index.php?c=RaEQL35QhmE7hpsF36yBVHriwbfwVW/Ug8Sn2nZXeo/Ynfh
/index.php?c=RaEQL35QhmE7hpsF36yBUHv13rLzVW/Ug8Sn2nZXeo/Ynfh
/index.php?c=RaEQL35QhmE7hpsF36yBUn/13rD0VW/Ug8Sn2nZXeo/Ynfh
/index.php?c=RaEQL35QhmE7hpsF36yBU3j117DgW2GSiNy+2HVZf8nAluV
/index.php?c=RaEQL35QhmE7hpsF36yBU3z13rDzVW/Ug8Sn2nZXeo/Ynfh

Feature Extraction

- Past file downloads
- Domain features
- Server IP features
- URL features
- **Download request features**

✧ Anomalies in the HTTP request

1. Does **Host** have a valid domain name?
2. Is **Referer** present?
3. Length & depth of the URL
4. Extension of the downloaded file

```
sha1 | 28178e6fd7cdd935baa833906c5cadb20f80128f
host | com.shamoa.up
url  | /uploads/images/shamoa-ced100a656.gif
```

Detection ratio: 37/46

```
sha1 | deee2f46cb5a518f5a0d09a5466fd0ce724c1992
host | 220.73.162.3
url  | /Download/MicroProCon.exe
```

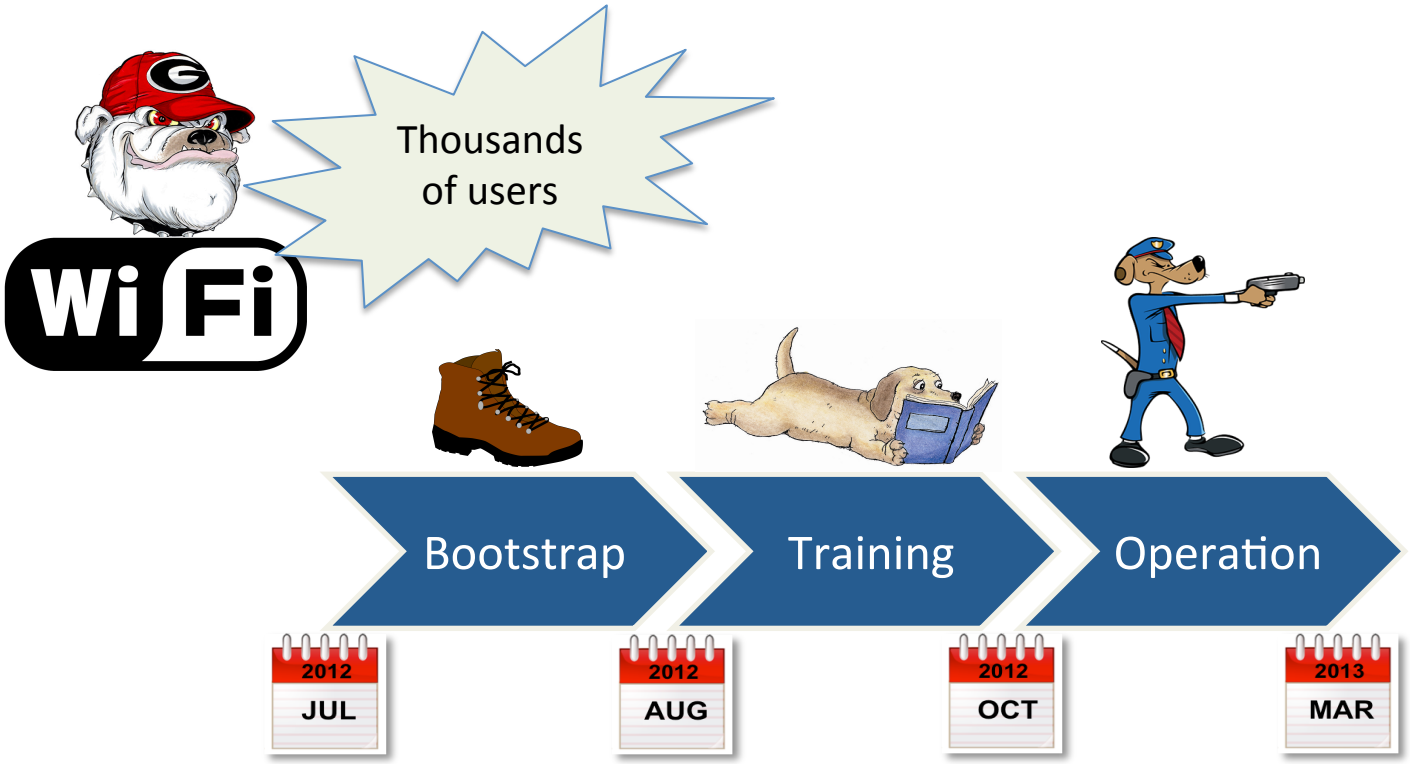
Detection ratio: 31/46

Ground Truth

- Partial ground truth on past download examples
  - For labeling training data
  - For feature generation purposes

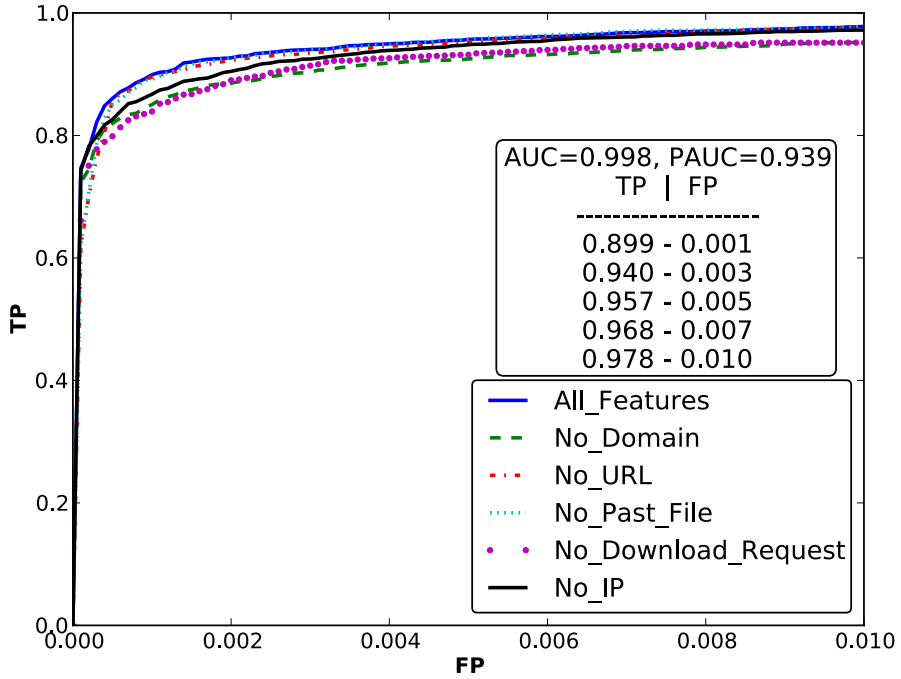
1. Compute hash of the file
2. Send the hash to VirusTotal (VT)
3. Label the file using these rules:
   a. If hash is not present in VT: ***unknown***
   b. If flagged by 2 or more trusted AVs: ***malware***
   c. If 0 AVs flagged the file: ***benign***

Training & Deployment

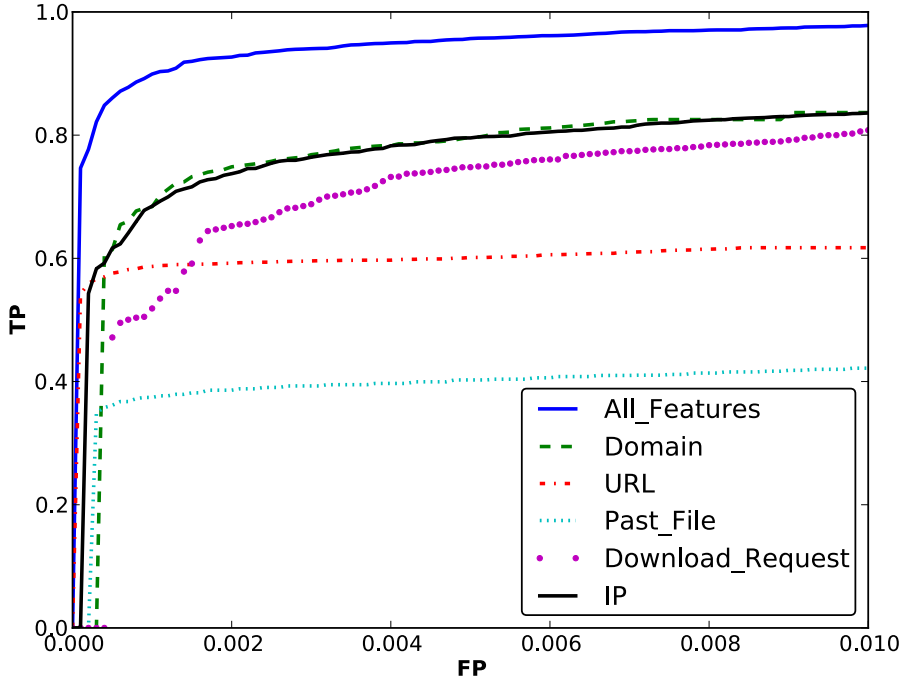


Note: our release of AMICO ships with an "default" trained classifier

Feature Analysis
(cross-validation)

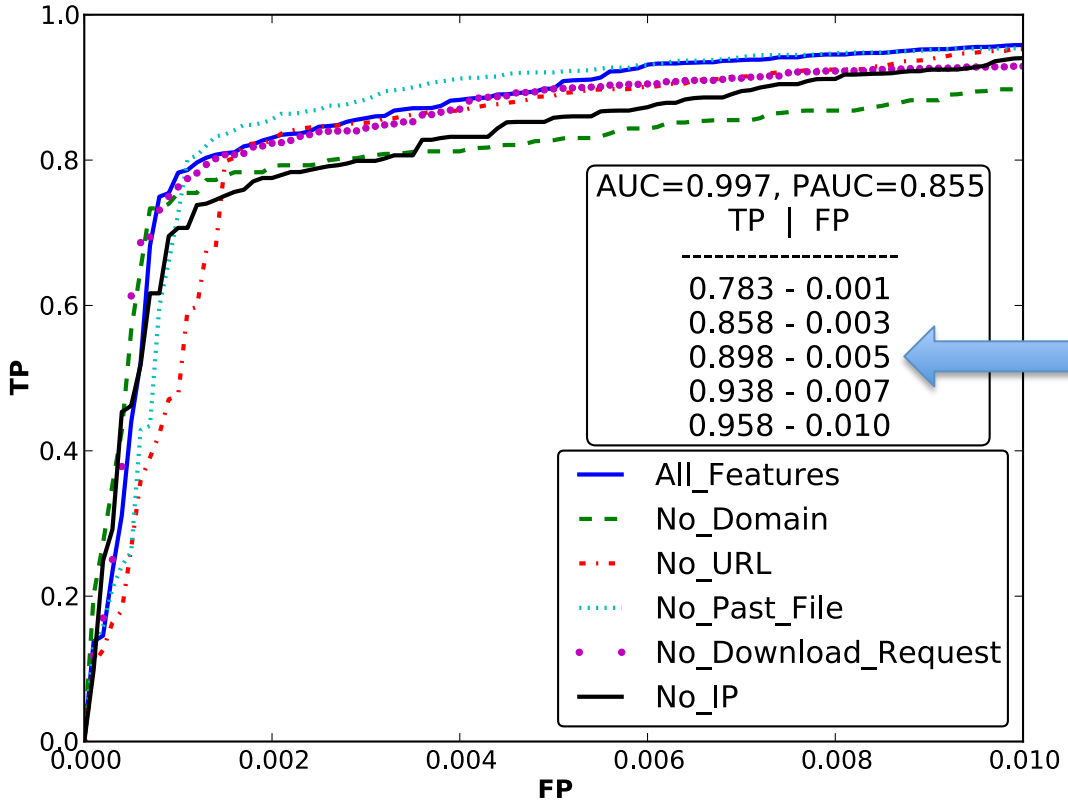


Leaving 1 feature group out



1 Feature group at a time

Deployment



89.8% Detection
0.5% FPs

Interesting Findings

Malware: **3,655**
(eventually confirmed)

virustotal

- **28% *unknonw*** malware downloads (1,031 of 3,655)
- AMICO detected **95.8%** of those

Zero day malware downloads:

- Initially undetected by trusted AVs
  - detected as malware after 1 month
- **5.1% *zero day*** malware downloads (187 of 3,655)
- AMICO detected **78.6%** of those!

Interesting Findings

Malware: **3,655**
(eventually confirmed)

- GSB detected only **2.5%** (93) malware downloads !!
- AMICO detected **95.8%** (3,412) of the missed malware downloads

- *Note*: GSB browsers already **block** other malware downloads

Push the Criminals Against the Wall!

Agile
Distribution
Infrastructure

Stable
Distribution
Infrastructure

Push the Criminals Against the Wall!

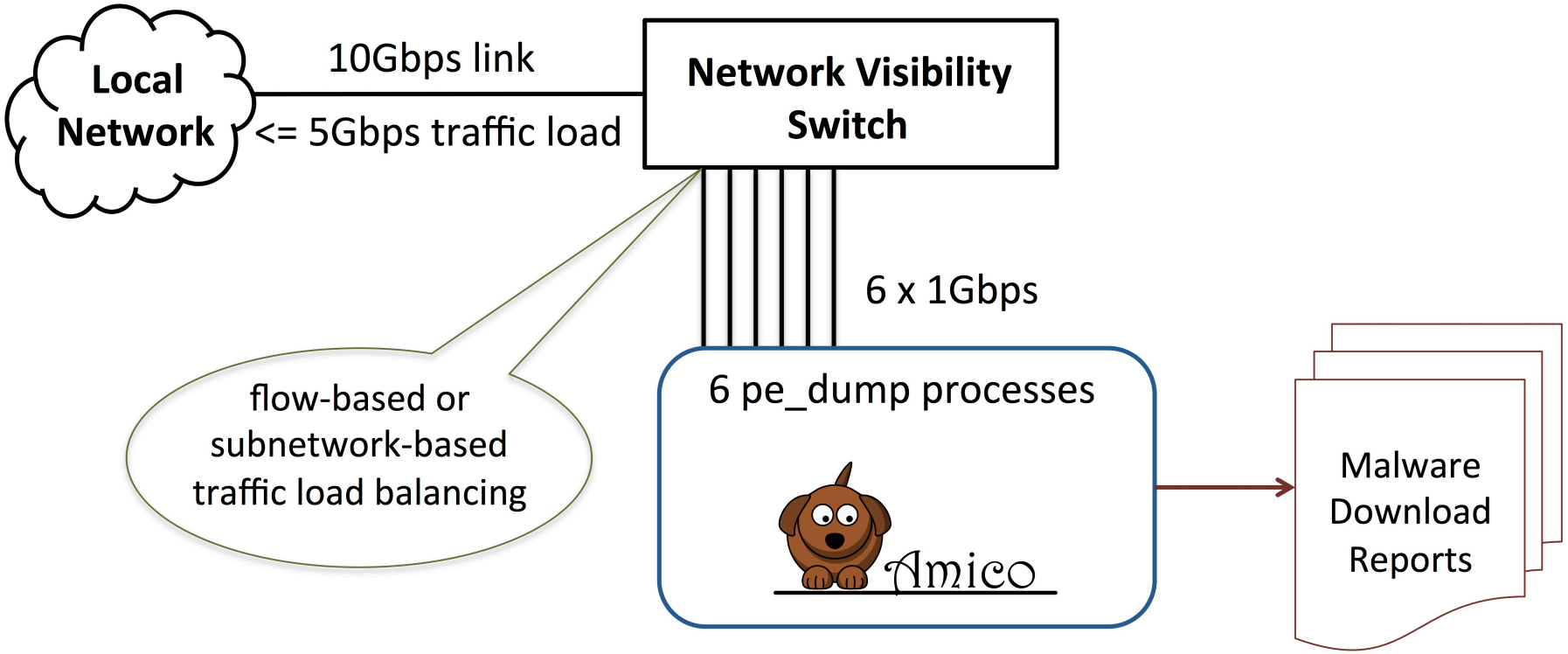
Agile
Distribution
Infrastructure

Stable
Distribution
Infrastructure

http://amico.googlecode.com
NSF ACI – SDCI Sec
DHS TTP

Currently deployed
at UGA main campus

Example Deployment



- **Important**: flow-based load balancing!
  - Allows for correct TCP flow reconstruction

Syslogs Example (Malware)

```
Aug  5 12:24:07 netbox1 python: PE file download
timestamp: 2014-08-05 12:23:00,
client_ip: x.x.x.x,
server_ip: 54.200.6.236, server_port: 80,
host: spyappforall.name,
url: /?
e=pcho&cht=2&dcu=1&cpatch=2&dcs=1&pf=1&unp=Azm9CdOLv7DVDyx
ECyFPg7x9Ae0KBfUKAe4MBG0VWznLDe4PBNq9geFI&publisher=95&dd=
4&country=US&ind=6575140181494437697&exid=0&ssd=6805163792
924606921&hid=13191006354824692162&osid=601&channel=0&sfx=
1&jc=1&category_name=PriceChop&install_date=20130805,
referrer: None,
sha1: 9b66a4f232b619f3f16b9bbb08ad02cffa92de77,
md5: 5644905b7058d45e2b7f956467ddee45,
file_size: 1205760, av_labels: 1,
corrupt: False,
amico_score: MALWARE#0.87#0.4
```

perdisci — perdisci@netbox1: ~ — ssh — 158×46

timestamp	md5	host	score	avs	corrupt	vt_query
2014-08-06 15:59:49	7f17dc6d67aaae71aab6514f005418c8	com.best-fileopenerapp.www	0.44		f	2014-08-06
2014-08-06 14:55:28	9def778ba0c95445ad6e3f3e39b52a62	com.adorikacontentportal.cdn	0.433		f	2014-08-06
2014-08-06 12:30:46	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	0.491	8	f	2014-08-06
2014-08-06 11:52:41	d19ee990987346b9c073a9e97c38afc4	org.microbesonline.meta	0.485	0	f	2014-08-06
2014-08-06 11:18:36	f3d3b89e434c68f1e5c97ac4edca629b	com.greatonlineapplications.www	0.521		f	2014-08-06
2014-08-06 11:06:14	e206f8289eb2b9b997ac397b82b0fa20	com.websteroidsapp.d	0.724	3	f	2014-08-06
2014-08-06 09:52:06	5a275a569dce6e2f2f0284d82d31310b	com.cnet.software-files-a	0.538	1	f	2014-08-06
2014-08-06 09:49:48	5a275a569dce6e2f2f0284d82d31310b	com.cnet.software-files-a	0.537	1	f	2014-08-06
2014-08-06 09:49:48	d05cf41a2e1e01e7842e2b643a6f2370	com.cnet.software-files-a	0.48	3	f	2014-08-06
2014-08-06 09:46:20	5a275a569dce6e2f2f0284d82d31310b	com.cnet.software-files-a	0.471	1	t	2014-08-06
2014-08-06 09:45:54	a27c6d338f4c2b7f9f951f911cd1b81a	com.fb-hosting-apps.cluster10.www-squid	0.903		f	2014-08-06
2014-08-06 09:18:15	11fcb6824b912480af7d54a8547dfcb8	com.wajam.dl	0.779	4	f	2014-08-05
2014-08-06 06:29:45	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	0.531	8	f	2014-08-06
2014-08-06 00:28:44	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	0.531	8	f	2014-08-06
2014-08-05 22:40:07	128de21c54ce7268b3c0fb100bdf25e2	com.jzip.cdn.download	0.451	4	f	2014-08-05
2014-08-05 21:06:27	11fcb6824b912480af7d54a8547dfcb8	com.wajam.dl	0.759	4	f	2014-08-05
2014-08-05 20:01:04	43d6426ed65859c1be7df4b125a90dbd	com.sfrgfiles.cdn	0.481		f	2014-08-05
2014-08-05 18:27:43	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	0.531	8	f	2014-08-06
2014-08-05 18:25:27	812b18c6dbda71d29600aa238e7f5043	com.down1oad4desktop.get	0.452		f	2014-08-05
2014-08-05 17:23:58	e206f8289eb2b9b997ac397b82b0fa20	com.websteroidsapp.d	0.724	3	f	2014-08-06
2014-08-05 17:00:06	6d1eb37e530843a326e072727468cfee	com.v47installer.dl2	0.527	4	f	2014-08-05
2014-08-05 14:31:33	b12f98b6fc58752bc411b801606f0144	com.software-updater.cdn	0.465	1	f	2014-08-05
2014-08-05 14:11:02	03dbf7c5bade8b5facdcbd5a0d7b8f68	info.wa				
2014-08-05 12:26:42	092e2beb0fd18d670ce2bfa361fb89ee	net.clo				
2014-08-05 12:23:13	ef7d5227360e42058d25f27d9db95de0	com.sup				
2014-08-05 12:23:08	71c2ea2b936ba80f4bad80937b369adf	com.sup				
2014-08-05 12:23:00	5644905b7058d45e2b7f956467ddee45	name.sp				

SHA256: 6f246241a265d3cac528e74e04ed26926091b87669ef863758acef23c67b8fbc

File name: 5644905b7058d45e2b7f956467ddee45.exe

Detection ratio: 15 / 54

Analysis date: 2014-08-06 04:12:23 UTC (16 hours, 20 minutes ago)

spyappforall.name

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural i

Antivirus	Result
AVG	Generic_r.RI
Ad-Aware	Gen:Variant.Adware.Dropper.105
Antiy-AVL	GrayWare[AdWare:not-a-virus]/Win32.MegaSearch
Avast	Win32:Adware-gen [Adw]
BitDefender	Gen:Variant.Adware.Dropper.105
Comodo	Application.Win32.Multiplug.R

virustotal

www-squid.cluster10. fb-hosting-apps.com

SHA256: a5eac3579ca18bb3e218e3bed5f4082f012682ecde630d667b7f76e95251ec2d

File name: salvation data bad sectors repair__3039_i1134147481_il1247321.exe

Detection ratio: 10 / 54

Analysis date: 2014-08-06 14:30:29 UTC (6 hours ago)

0 0

Analysis | File detail | Additional information | Comments 0 | Votes | Behavioural information

Antivirus	Result	Update
AVG	Ukra.EBB	20140806
Ad-Aware	Gen:Variant.Application.Bundler.Amonetize.11	20140806
AntiVir	ADWARE/Adware.Gen2	20140806
BitDefender	Gen:Variant.Application.Bundler.Amonetize.11	20140806
DrWeb	Adware.Bundle.5	20140806
ESET-NOD32	a variant of Win32/Amonetize.BK	20140806
F-Secure	Gen:Variant.Application.Bundler	20140806
GData	Gen:Variant.Application.Bundler.Amonetize.11	20140806
Malwarebytes	PUP.Optional.Amonetize	20140806

Cloudfront used for malware distribution

date	MD5	host	size	score	tavs	avs	corrupt	vt_query
2014-10-15 03:11:45	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.559	8	29	f	2014-10-14
2014-10-14 23:54:11	5185c91d163c09a07636b6e3d9e6352c	net.cloudfront.d11ftuwdwpx4fl	526336	0.503	7	21	f	2014-10-15
2014-10-14 21:42:54	393653b494502b73d7714f92a5ef8e32	net.cloudfront.d1y4ipvfu7uj17	89544	0.407			f	2014-10-14
2014-10-14 20:18:41	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.559	8	29	f	2014-10-14
2014-10-14 19:47:38	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.559	8	29	f	2014-10-14
2014-10-14 19:30:25	16f87d3805eccdfa4ef672cad7824123	net.cloudfront.dpy22z83rm3zu	920795	0.699	0	2	f	2014-10-14
2014-10-14 19:30:25	5aa07bc79c99a89f2740114ddcda2423	net.cloudfront.dm930xmxv1gqs	151216	0.619	1	5	f	2014-10-14
2014-10-14 19:27:52	99e4e2005a507e28576cd2019f114614	net.cloudfront.dm930xmxv1gqs	582848	0.559	5	20	f	2014-10-14
2014-10-14 19:27:28	03a3ce6b8386592ce0fcc879477aa79b	net.cloudfront.dm930xmxv1gqs	15585	0.579			t	2014-10-14
2014-10-14 18:52:40	5185c91d163c09a07636b6e3d9e6352c	net.cloudfront.d11ftuwdwpx4fl	526336	0.454	7	21	f	2014-10-15
2014-10-14 12:54:50	16f87d3805eccdfa4ef672cad7824123	net.cloudfront.dpy22z83rm3zu	920795	0.61	0	2	f	2014-10-14
2014-10-14 12:52:04	29397e3bd61ac03d92451f00784593ba	net.cloudfront.dm930xmxv1gqs	582848	0.53			t	2014-10-14
2014-10-14 12:49:44	cf0c8a98cd2c35cd805dbb81b9bf3336	net.cloudfront.dm930xmxv1gqs	66368	0.53			t	2014-10-14
2014-10-14 08:09:04	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.559	8	29	f	2014-10-14
2014-10-13 23:53:50	5185c91d163c09a07636b6e3d9e6352c	net.cloudfront.d11ftuwdwpx4fl	526336	0.523	7	21	f	2014-10-15
2014-10-13 23:02:16	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.559	8	29	f	2014-10-14
2014-10-13 21:00:26	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.366	8	29	f	2014-10-14
2014-10-13 15:44:27	055812396c209a616d450c42fbb81106	net.cloudfront.d11ftuwdwpx4fl	526336	0.523			t	2014-10-13
2014-10-13 13:52:38	d5c496efe9c3a47ebb5dee34326c8924	net.cloudfront.d11ftuwdwpx4fl	526336	0.493			t	2014-10-13
2014-10-13 03:09:45	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.49	8	29	f	2014-10-14
2014-10-12 16:50:09	5185c91d163c09a07636b6e3d9e6352c	net.cloudfront.d11ftuwdwpx4fl	526336	0.473	7	21	f	2014-10-15
2014-10-12 12:45:16	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.489	8	29	f	2014-10-14
2014-10-12 10:29:09	5185c91d163c09a07636b6e3d9e6352c	net.cloudfront.d11ftuwdwpx4fl	526336	0.454	7	21	f	2014-10-15
2014-10-12 09:24:24	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.509	8	29	f	2014-10-14
2014-10-12 03:22:24	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.529	8	29	f	2014-10-14
2014-10-11 23:54:26	5185c91d163c09a07636b6e3d9e6352c	net.cloudfront.d11ftuwdwpx4fl	526336	0.454	7	21	f	2014-10-15
2014-10-11 21:20:23	61131c7f2511053f58b573a6bba8605a	net.cloudfront.d2sci4fopfy9a2	89816	0.58			t	2014-10-11
2014-10-11 20:59:40	5aa07bc79c99a89f2740114ddcda2423	net.cloudfront.dm930xmxv1gqs	151216	0.66	1	5	f	2014-10-14
2014-10-11 20:57:52	9fb9d49c2db7edd1084ab765d619f5c6	net.cloudfront.dm930xmxv1gqs	66368	0.531	4	18	f	2014-10-14
2014-10-11 18:02:22	89a4f917f2988b687d6bccf7bedbc8e0	net.cloudfront.d32k27yvyi4kmv	1848976	0.394			f	2014-10-11
2014-10-11 17:38:59	99e4e2005a507e28576cd2019f114614	net.cloudfront.dm930xmxv1gqs	582848	0.531	5	20	f	2014-10-14
2014-10-11 17:37:07	9fb9d49c2db7edd1084ab765d619f5c6	net.cloudfront.dm930xmxv1gqs	66368	0.531	4	18	f	2014-10-14
2014-10-11 15:18:11	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.531	8	29	f	2014-10-14
2014-10-11 14:30:07	16f87d3805eccdfa4ef672cad7824123	net.cloudfront.dpy22z83rm3zu	920795	0.591	0	2	f	2014-10-14
2014-10-11 14:28:12	5aa07bc79c99a89f2740114ddcda2423	net.cloudfront.dm930xmxv1gqs	151216	0.631	1	5	f	2014-10-14
2014-10-11 14:23:16	99e4e2005a507e28576cd2019f114614	net.cloudfront.dm930xmxv1gqs	582848	0.571	5	20	f	2014-10-14
2014-10-11 14:21:10	9fb9d49c2db7edd1084ab765d619f5c6	net.cloudfront.dm930xmxv1gqs	66368	0.571	4	18	f	2014-10-14
2014-10-11 12:23:10	1e3aa93bb4f2e0f4b60f78ef9764aec5	net.cloudfront.dm930xmxv1gqs	401920	0.611	5	14	f	2014-10-11
2014-10-11 09:16:00	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.531	8	29	f	2014-10-14
2014-10-11 03:13:41	092e2beb0fd18d670ce2bfa361fb89ee	net.cloudfront.d2sci4fopfy9a2	89816	0.531	8	29	f	2014-10-14

“Kyle and Stan” Malware Campaign

date	MD5	host	server	size	score	avs	vt_query
2014-10-06 08:37:23	6fd90ea27f3fc3c782190c62e89f0b60	com.5nx67dv2ps.ajaohqp7lhz	188.165.146.111	1390688	0.447		2014-10-06
2014-10-05 12:54:27	51894341a4f6d1adeb62166bbcfb3638	com.323m9vqobm.cdlrdysj0fu	92.222.193.4	354485	0.735		2014-10-05
2014-10-03 09:45:08	bc539d3cba7615286f4aac4273ef7eaf	com.jjusdwp8mx.8sa7dfw	188.165.120.20	1390512	0.599		2014-10-03
2014-10-03 09:44:33	04b54e8f5d7a3ccbad77bd7058e51556	com.jjusdwp8mx.cvhwt3d7	188.165.146.100	1390512	0.625		2014-10-03
2014-10-02 16:59:35	7792cf5aa4d6ce2607a241056e044dae	com.63bphnq4s6.zwlraizqh	92.222.193.19	1393096	0.583		2014-10-02
2014-10-02 09:12:12	3c257c57a8e8449810b47931a1f168a0	com.z79x2vbhh3.utdahp	92.222.125.30	1393080	0.599		2014-10-02
2014-10-01 22:13:48	2c01966f4b00428f4782dce019a5ac3b	com.r0kr3xkbix.dya9hlfe	92.222.117.199	1393120	0.614		2014-10-02
2014-10-01 22:09:30	21222f15428624ff3c0febb1d3595207	com.r0kr3xkbix.a7hcpcf8dpbe	92.222.117.103	1393128	0.599		2014-10-02
2014-10-01 21:13:17	bbc9fbd1ab7c2d2871e582897fc047c8	com.9d3791kwoo.fztqlwkj	92.222.117.196	1390528	0.76		2014-10-02
2014-09-25 11:45:59	f46835d64f04bbbd797a53b5ed999b0d	com.mxp698.kyle	92.222.193.16	1353632	0.497		2014-09-26
2014-09-25 11:45:32	44cee915cda159ae67aad9258dc366ee	com.mxp698.kyle	92.222.193.16	1353632	0.583		2014-09-26
2014-09-23 14:58:48	dd231a63fc5684482fb90c16360e0b0b	com.mxp4119.kyle	92.222.125.5	1366888	0.537		2014-09-23
2014-09-18 12:01:24	5edadfd018f7450e6e49fffeb1f8a539	com.mxp2391.kyle	188.165.146.89	1056632	0.495		2014-09-19
2014-09-18 09:06:47	7e5026bf4e15483dea8e152ef8e91f73	com.mxp2392.kyle	188.165.146.89	1056120	0.512		2014-09-18
2014-09-16 12:38:30	8e0dacfbc7271f2e30d9f930e11be6e7	com.mxp4116.kyle	188.165.146.126	53713	0.401		2014-09-16
2014-09-15 21:03:39	51ed873239a4457ab29720adc5b83d57	com.mxp1194.kyle	92.222.97.29	14282	0.583		2014-09-16
2014-09-15 20:49:02	335fe308052b85ef3cadf0228ef893f4	com.mxp4117.kyle	92.222.125.27	1344648	0.497		2014-09-16
2014-09-15 16:49:29	538f95ca280e9bd2eb1418fdce31ed97	com.mxp4117.kyle	188.165.146.84	14301	0.682		2014-09-16
2014-09-14 13:07:28	61c50454e732f660d0a5d4d802b39bb2	com.mxp4116.kyle	92.222.125.27	79817	0.541		2014-09-14
2014-09-13 22:09:17	7e0f139641d058d61bf6f6fdc4bc9dbc	com.mxp2387.kyle	92.222.97.14	1344632	0.437		2014-09-13
2014-09-13 10:31:21	e1adb3cd9e1c9d6600ab69e1b3dd54d6	com.mxp2387.kyle	92.222.97.14	1344648	0.583		2014-09-13
2014-09-12 20:47:54	c2f78420886c6040d85952223d232b96	com.nectophrynoides.dl	188.165.230.78	865656	0.74	14	2014-09-12
2014-09-12 19:28:18	c5bca5252eb8373b0d61f7cc2a97e997	com.expertareyou.dl	188.165.230.78	398384	0.859	16	2014-09-25
2014-09-11 21:20:07	fd09e5c8d116a1ba5c66c7e2d30d5b37	com.buddyauth.updates	188.165.224.162	664064	0.799	0	2014-09-13
2014-09-09 22:03:41	feb0aada82207ccd8ec26bab0efec181	com.mxp4113.kyle	92.222.193.15	1339528	0.483		2014-09-10
2014-09-09 19:59:37	37017eb54f193bdf1854d063e596601a	com.mxp2385.kyle	188.165.146.89	1339448	0.657		2014-09-09
2014-09-09 14:21:07	58e45b71360323d31baa8869cd3c6bb6	com.mxp1193.kyle	188.165.146.71	1339720	0.721		2014-09-09
2014-09-09 09:06:37	feaa9045e30ecb94fd32aac587f18ea2	com.mxp2375.kyle	92.222.193.14	1255544	0.483		2014-09-09
2014-09-08 22:29:36	20bd30be10788c6a364fb4af6a372d97	com.mxp2375.kyle	92.222.125.24	1255552	0.583		2014-09-08
2014-09-07 22:23:04	d7498a4fdac09584afee8491954d7f21	com.4yftfs.dl	188.165.230.78	233208	0.719	14	2014-09-07
2014-09-07 20:04:07	c114bf333b5629c80eae34bad2640276	com.mxp2368.kyle	188.165.146.123	1515186	0.729		2014-09-07
2014-09-07 13:38:07	6b2cb1d0e566bec99da510b91dcfce54	com.mxp2367.kyle	92.222.97.26	1526896	0.583		2014-09-07
2014-09-06 00:28:29	1bc3b1ef213637f527e4daff8d603da4	com.rarlabs.www	188.165.200.151	1922688	0.553	1	2014-10-03
2014-09-05 22:11:40	61253d353c7cb349a26209e970fcd72b	com.mxp4103.kyle	92.222.97.22	1527104	0.553		2014-09-05
2014-09-05 17:21:40	ecf340a79677b847a8bf5fbac8be5776	com.mxp2364.kyle	92.222.97.24	1526912	0.461		2014-09-05
2014-09-05 09:51:10	df96a3be44cad13e10ed5c2222749263	com.mxp4102.kyle	188.165.146.95	79817	0.741		
2014-09-04 11:21:14	c7cb8fd9977149c0d4807a3046617909	com.mxp4102.kyle	188.165.146.95	1526800	0.801		
2014-09-04 00:32:20	151bc2ee26dca775117463aba62edc27	com.mxp2360.kyle	92.222.125.17	1265280	0.599		2014-09-04
2014-09-03 21:16:20	1a43b4b015821e4b920caef690db7e15	com.mxp1182.kyle	188.165.146.94	1265352	0.76		2014-09-03

“Kyle and Stan” Malware Campaign

date	host	url
2014-10-13	com.zg4xbr33.0nacts	/sugjXy746datY9hyrcKlTkTw6umYlwkiU97hMzKTJUgOWByy9qKs4WQaijkGI3R-PM-fvGmYor2lBDovA2xhkjStkHcEu8g_E1CH0YkGSnUDHv_X0Mf5c4WgzYmAsw9h
2014-10-13	com.zg4xbr33.kilna5bg8p	/x2Lp7VqhheG4ThX2Z9pjUmT6KHKGLkuC5Bt8wigUX5fJG_t4L302Z64GjrSIdKVfTkdpHpGoo5Lqm2yAh6b8byOv01ZcyG7BpuyzUgs8a0BIKBNgzO_tpeoB6rbycF-E
2014-10-13	com.h4xd4nhz.pdtpahhzr	/0YJXiANmKFoSQa3wDXgjAro9qrquKH_M66hMxYywRBJfHtg5-ZnNCiq8NCtY1IlcZsV6m8WbP6ESFzc4e2GXj5CxZ8hZ3mEcmqbVC_rSSVqs55Lfve-4HyVD4WYcUK_H
2014-10-13	com.5ozb49tv.4qdqtecvbgk6	/4NDk04yw7uo1EwnyzIcPCkVIxuB0twnfiXmm37_fSjFNq0iHE7mTnFif5yXtGI4uzjkxfHcdue4hrDJ3xvEm3bpoBxmLuiV6x9-FQeoHevTJ55rSBCvETNPSKkIoKTB-
2014-10-12	com.g06bky5m0p.zolmtdm	/yyuFK6pDVYCLJZFcqflq-A3CiH6YaXNxivbopHvPN5WezQbtueb8FqayIRuxIBmD6IAfd-Bw1MUlp9dk89LmdNsjd7V21X0iqKYK4O6yHWtQ1mK1DxXmYDscckiyyjp8
2014-10-11	com.5bnoww26v1.9yt2hjld1d	/OahDvPifJArbYrq79B-m9oabKNCL8Oc-v0nGF5gqmBT7U4nbMD9Yp5DbFkdzZNV7PNV7eB6MMGaHDBGw4ojSDwvrGrbSYvLgoRgvwGNahO-coqGXg26xLZYVFfJpWRLN
2014-10-11	com.5bnoww26v1.gbdjtvhffcfs	/626JjQQyLTtrN_REdHsl35Nztl56DIBSzMBUG-2uaKRIiP3jMYxJEAoxcDAkfSchUd6q5YZwXNhLWVgSVdUf1ql8pPBcMm2kT8FHyIeVMkWxV_G0ASzktVXuf4m-6r9s
2014-10-11	com.5bnoww26v1.pqdrhd6x	/SazHHitXnZHc15JgiMwt2yMKWcrvLjYCaAYXs5w6SuItU2fTW_TGsUQy3g3DFdrLSCaE9YU8AC6yC3bthynLSjqlROhsgHbGzb-LApTFCnDCGYoyY4HnHSiKJGGb6cn2
2014-10-09	com.1q63o2bhtn.4ghxa8zd	/-QUIfX4PtEMpTBTG5sUs27YdvvuQ93NGE_pqteo-bSZKG9cfmVidriDbbIy9v6i20aRWOtDVkkT43hOIHzLSsE-716qakt6KvEYXWCdEBBKnLannf5Irt_T2dRwtnmzU
2014-10-09	com.1q63o2bhtn.inpwhvktk5t1	/YOgUAb0ugnbHuAbLkWv6atkdwrRyNovpNx1wlYWlMQiKi8XUAkwENlUhth_NfKtABnRWfjkeP6qO_6L7MD9dSX0R1VSAVWdvo2B0tk6A05pi8bxrtXApc0t1_xkyzULx
2014-10-08	com.5rbo4tp3ok.k0lgarq	/pfsmXT3enBrNvERu7Q97rPQ_sW_hprWssb-IClS1MgUjYZw_mBrchLda7QfShnvFv-JIihCUIUJllZ1Bqu2LUUQela2yqAC9OkxWSX0uUwASCsjoH5t3vQ-F3kqrLXsM
2014-10-08	com.5rbo4tp3ok.dmp5a1hrl	/MI4SHPWgdwQ8SFAmBJzxSePJzwIJe-9DeHRw7QFJ0zszn_RAO51TOZBsHyAg6pMbWJdJsIuYw1eM0P5JLPL4XRHENnscEnXmQu-Hn_qII2s7aHSatJ0FRIIOfhirNeb8
2014-10-07	com.5rbo4tp3ok.wlauagbic	/iMrDLa6EEXTTBe_Yal-ygoOVN_4WaAufcm_DwQ5g9dcfhCHAcbevZHCrM4NrrTsVNvAlZ-dBSdKLD0mtfybRFVJ7FbQfuIGOxdGHUZDEQFpZQ2JILM46Umelzc_J2PfJ
2014-10-06	com.h8m8brjvp0.lidgl20mbbl9	/pZzErieHNovA8zGOxbQDsofFxjfmy9yVQm7SDm_TZaTPZBGGlS3oyCDVahzDh2tyVDLlnwdSTapK8s19CnsZinYBSPSUUAlqzxjY6jU0J7y09ZuT-jKpnS6nSIF2j-m8
2014-10-06	com.bzkm3mhonv.mytohwt9	/asdeqFVu7DPO_UySN_4Ti4mQcCVuJRgeRKxwEl-6JKcgi5C2DjgjlJYHR9fHhVepX-do50Is6xIGcJk74NY5Jm97tP0HHFEn3myqJxogcCK19luuPBlUyRC0Iq3A51yv
2014-10-06	com.h8m8brjvp0.2wahagsemzg	/A3N_SYJSU7gqEjnGDlhx3I2QQ8lisgaZARDoqh-HQYDTQOIC3lqtenJj9vXsMYWSV28guiXLiMMKWqHrQ7XXL92622jfa7p_Q3lxW1aSIVUuxY0_IQF8IGXyMNE3_uuy
2014-10-06	com.5pqts0kxbp.cklgl9zgk0mt	/JzQIYOClt9OFiOq9-Z9R5r2didDvRhdVyQwgUyFwwDP5DDuc7tfWOTp-_yuD7aG2iR0_pBngj5FjozTSKZUqSp-EbNRt1FHU_8A0WmmvXjapleZ1EdpmOO0sohUkrShs
2014-10-05	com.bpqot5ynq2.imaat8qb8z	/g_Crx4Y3PhQhD82S7i9e28NKAjSOr0hHDfvJDhfbdoMlCBxiWJLd86BjBVqRilRdwGgGr02tIpvIgN1ZI6teBkvWEbXySJRcNchPxhhvjls7qRXnEEAa88kj4xQAxqbh
2014-10-05	com.323m9vqobm.cdlrdysj0fu	/kpcf-Bq8jP1Tf27A9Z4ye36F0v7Sok6IQG75q8lMKMIkdVXLdcPujAUyPOmLwcgPv1m-3YdDmpYPw38SSDIVNrY4Kd1m_VLoIMQGqis5f6SNf7847VSTTvFh3tcgeTGh
2014-10-04	com.tnr0mkb8py.3calp2vo	/zs5M73K_SqL4MYhW7fqBXC9oNN7xQPBsYR4z8dVaPZhQiNetGs0lVySenh4cq5bxDEOOpMaBASpmBbedwIacw1dpvulTmwIu09n_kkvjug6OGP7kYGVpiKnuquiXz3Xu
2014-10-04	com.tnr0mkb8py.n1pph5fr1lof	/0OqOafp_oRFAR7ZTqytcVy7r-EyGX3OO4GrjErXZSIi0mB4-qgEcMCjZefV2RmeSAaaHVhs2AeP8tJCOrHCOYLIHU7rB-G-dK-w2SjYAnKLSgQJVgd1auaAWMAC7Q119
2014-10-03	com.b1o9qz6i1p.ooafht	/z-oPA2lAqG-TYHgjeiyK7fsYdsYi--Db3Mm9oI_jsmPQtoOSScjyC_xOqes_HQeQpmgyMK0pPluOFnGZOwkCuR0yNOFTW0xZI6bWI60AHOSTavIzt7JJvaqUIjY6c0Yq
2014-10-03	com.b1o9qz6i1p.0jpxh3em	/9Mmrr6sIOVKyRnOSpA0X9ar8Ys0t8PhBfz_Nz9lrHIOlcLj2Qz87-6K8nmotUN5obduecXbKT0HuYP1GXA4z96LeTrUNC34FNbBki_TYzhu_S89zl35JgYXAj0NeEtdW
2014-10-03	com.b1o9qz6i1p.rdpma03pvjcv	/cbJTr2uGQbSqEYy5VqMmB6OMVXQeBxnKiXfEXK1YW0w0njltkX7ZzYxAjicqMp-Dnsply4s4GEmRfqYaggaMD7ypZnAr-_QwmO36yQ4XjWYsEPReVAQ7UMQIkPOTVE09
2014-10-03	com.jjusdwp8mx.8sa7dfw	/M-9iyA02PBOxEiRYJ6SWOVfP9fW86dAexjIjKsvfxoS5l1_PDsZRYvXeT7EQj98TrN8CStf_y5gA7ZzeFyr4jWQ9TuhBJGa71pqgoZvz9yKbQLEzEsuLZ_powhA8fx2u
2014-10-03	com.jjusdwp8mx.cvhwt3d7	/zrRp9u_HEpeGhfxMczeKC9MoOOlCaWbI5tBhI5DaA_A_BNeCRhdvQOZzjr6mG1tNuoziSu6KCgFH2W5ptTH18b0bjGZWQun9Dx4QjI__oZ0aqgHREKpsTeeGVsXCJWZp
2014-10-02	com.63bphnq4s6.zwlraizqh	/wU5BOMRHN4lCM5QI_SIDpp1lmw889Nr7Ttbq1E1kvrWwrCFOBoFq2UstPmSFipIG2mLzLIb2Tq4KrQwRycMD81gvfL1i_aL-1vFAVfkeTdyG0GwExIJ93CR6_USNfDL9
2014-10-02	com.z79x2vbhh3.utdahp	/Oc4eLWclDoZ1t_MZQNnAxEMMQfhrMbbOOSMhqv0QPpu9jld4Fg-I4EDm-bzYouVOz_6MhMynrIiumt5UdMlkLaRnSn5rIPm0JmXhSc9pBpzBSe-nGfjPSyPrhJH1qli8
2014-10-01	com.r0kr3xkbix.dya9hlfe	/D2O9N4ukStFCZ4DHT9SpFjMVTS8IMls6TCM6PmLTH8UNKXLS629gl-eD88sr0M6RfiH5gi5YOMGJhnW-J0u3BrK-9jmUpkY-wHNOmh-F0n3Obmn1k6oqEIa72ATB5jvA
2014-10-01	com.r0kr3xkbix.a7hcpcf8dpbe	/OiEGqb88Fd96R6bOKyIWIznLudw9nZ5NVH4kBh8oMq5lzKmhOBQdbAbyMbxAaQbemdJlXlTqcRQhG7qMoxgLMB63szVsEzLYGytQ9yHXwH_lDPSYYARMdjD_Eacl_pbN
2014-10-01	com.9d3791kwoo.fztqlwkj	/fMtwBRFE4h16Q1U_4bGcezVwgV5J1ia6F4FM_PMp2sPV282TdGBkVber1u_Ke7Tuk4v7x-S6ZkRyy7rxO2YpdaOjP3bRgdWSWJb-bAnBan3b0Rj1_WZtoW8GwrELbPDz
2014-10-01	com.65w3dki4ux.yml1pd	/X-bkIh7-pBNv0ChNXgouJ3lerqF5oXJ_o5qGCmLj0BWU5jc9km9GU5BZYCbdPMA21tYOH201LeGW9E87uq8ER5wi0LisICpX-8Ag1YbdDsNUhNrN-EYuJ6Yp-KStNQY-
2014-09-25	com.mxp698.kyle	/j5G7i2JDifzLQu9fytSkyEPBd5AvKhkz1OcFaKrr9mlpRnHdphEocOxscUoyLCsDMcPsQ1oW_KCDFvTKETSev5-N5y6GWgy63jWI-Ay2Tw8QXFq2Kodh26ZoEDm-hW9q
2014-09-23	com.mxp4119.kyle	/LioyQLbDZ8q_d6M_1NOuUI8JiV_ylDA5t5auL_ZViGSfOf-fF1Vk98JmTznRYuSCMlpV8ryusXNecJAGeb0CkBfHPxsWNWvEAAzibLMKx98
2014-09-18	com.mxp2392.kyle	/nGtCauEJcAZ-7KBT5wmIFJaFB3pD_0EzGqMj9VH1nuGwX2jI5YsCIhmq9ayZ254PoyEGATeGwkPiqB7i1p8PxH0mB2mRX3x8yHSn2qsDe_M1FzyiognK0BwfTMoJuti8
2014-09-15	com.mxp4117.kyle	/7iSBh0mLBO2kZl44ann1yxJnuVXlIZrGvzlYeP5p52QukPToW9BMi7vZJyo8hNiVgOF1fCwDBnvwDu_K6FiI9qQ9GIXtmr3e6YAkov0yb9w
2014-09-14	com.mxp4116.kyle	/UecZZItuoCsTXPpSUUnLHwzg_JWuYRIhp_EfrT1W6c9Liwz8j11BEFa22Q2jRibl20zU9GFXp2js0pyNUToe99f4JCULMvBiukV9PfThwzs
2014-09-13	com.mxp2387.kyle	/SmQIEj9NlDgJPIbcqxPyVs6YDsJjeI1gbBHSDm1imVeReHjkyPUp5wEqRKT8I0qImjxOoKCUyFcMqxsAHOjwBC9Y5-_ilVDBHk79WVPr6Dsebblx6ev1s2uXQ6IY6QYj
2014-09-11	com.mxp4116.kyle	/QHYqOHgmz2uYpC4rpWBn9JEIaA0L1ByAOPRU4QALlJ628pwidg6pzTQObg-HlAzvZzUbnaXpuLTT-k-3NAqESA8SSIAr_AULZT6i_Qnf074
2014-09-09	com.mxp2385.kyle	/qKu5r-71aXQ1uBkNfNB0t9MD-uTnN3vejB7kcxJ08P22m95Mv6tLnvXMgcu-bw0F2_mbQBQ6FxR4SPA23_SIOUQj3ovLzXKHAfBQdJItT3Hm36y_sDJKlSuHdSx3PUle
2014-09-08	com.mxp2375.kyle	/BYAeCUC737OOqelkFVZXml8MreDr2Zfkt7LK2gh0selExjfsbWgyCp9YKEZgmuYQAmq0JzuxhWdoL5Jwiofz91SAAfxIN5lVg9rx7v7ug8QIQrW04Vur81ljNNd6swHC
2014-09-08	com.mxp4110.kyle	/ISiyoPyKYObvLke3wdifBYr6j1PG4T_HqpCHEk-ecPJnU3Vb4ESW8kGeAPsVYXz3M7tHeqmW2oF3sGZpgoWkh2RDThxJS10BNJYIcF7Fmm4
2014-09-07	com.mxp2368.kyle	/IF9dqf42xrFOMSVeZs0YFAHltxUUEx3o1tbY1CZNHnOAW56ZgbtS6GoD5J0pEpOkeCffeCMH9eDhmicyZbotVv15TyZYNIBgIDemTBK7E9v0mrI4yPMmCWVahjJJXzL9
2014-09-07	com.mxp2367.kyle	/p-FIbfXDSZ7F4zeSid94KkDG0acYDEZNT71r2teLiMb4tk1012VtbVU3OPs90Ej3zjy4v2vwl5Flbr-C6DvuRHn7PMY9gGF4nHk2wbTrHSG-Yegj2EcwdcxF-TToiMR4

perdisci@cs.uga.edu

Amico http://amico.googlecode.com