



<https://github.com/perdisci/amico>

Open Source Software

AMICO – Accurate Behavior-Based Detection of Malware Downloads

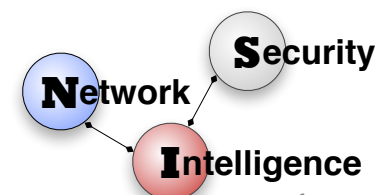
Presented by

Roberto Perdisci

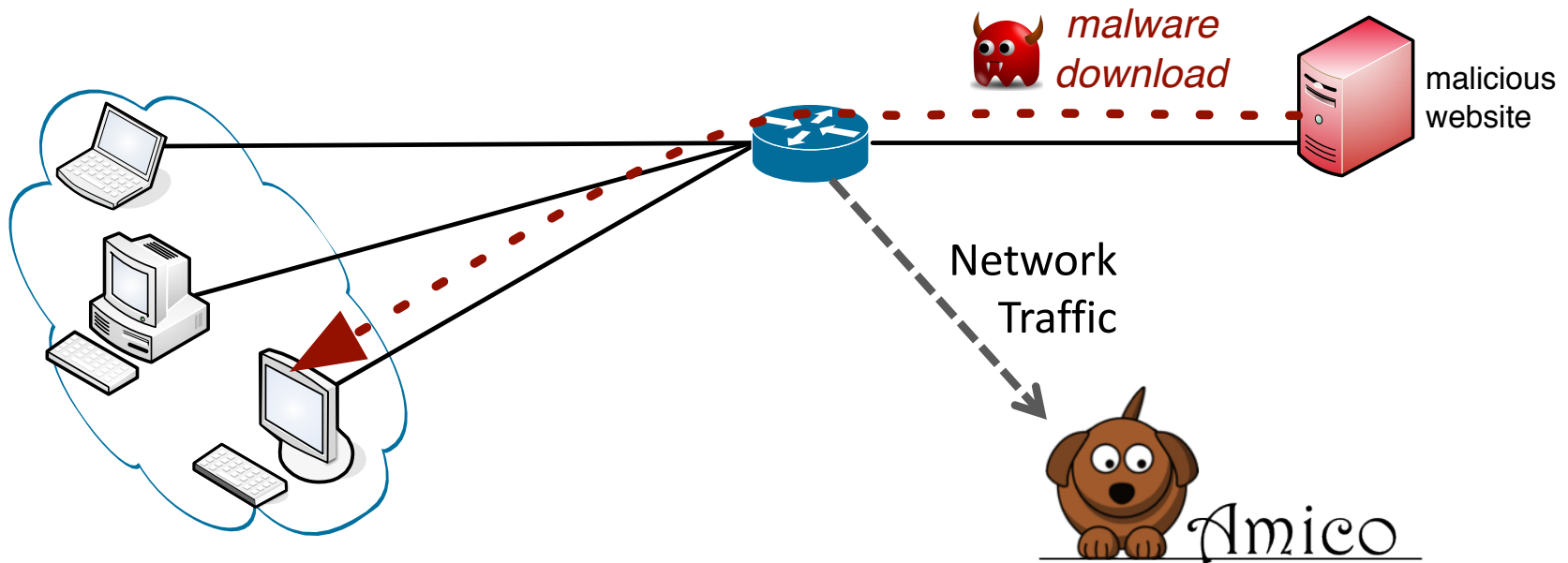
perdisci@cs.uga.edu



University of Georgia
Dept. of Computer Science



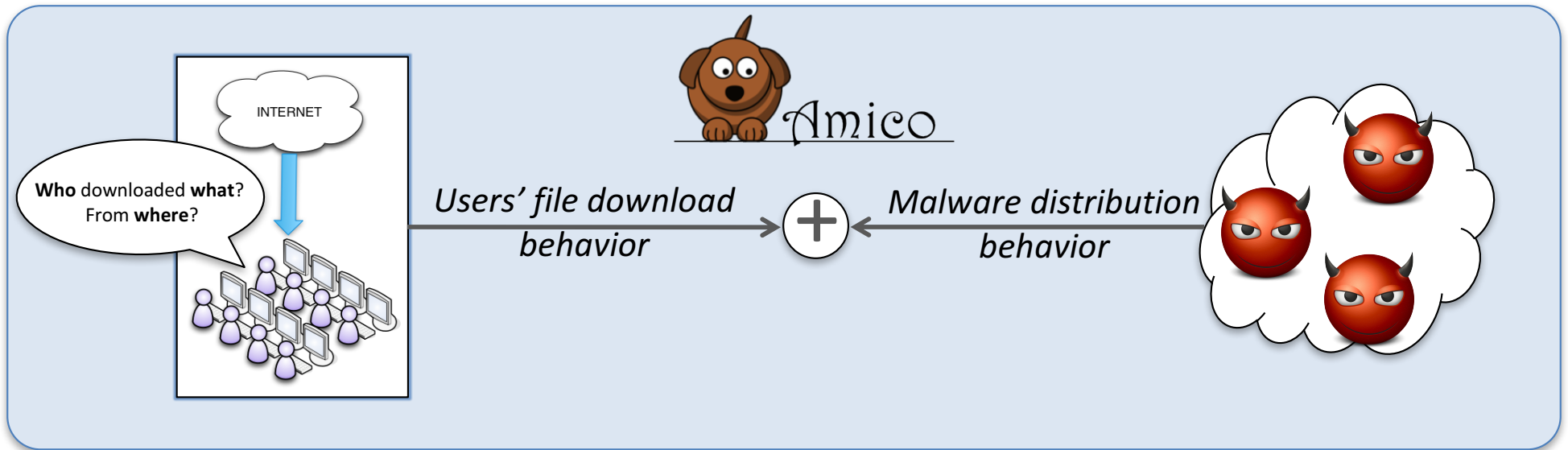
Passive Malware Download Detection



Detect Malware Downloads!

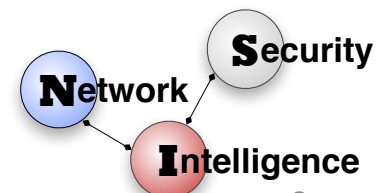


AMICO's Behavior-Based Detection Approach

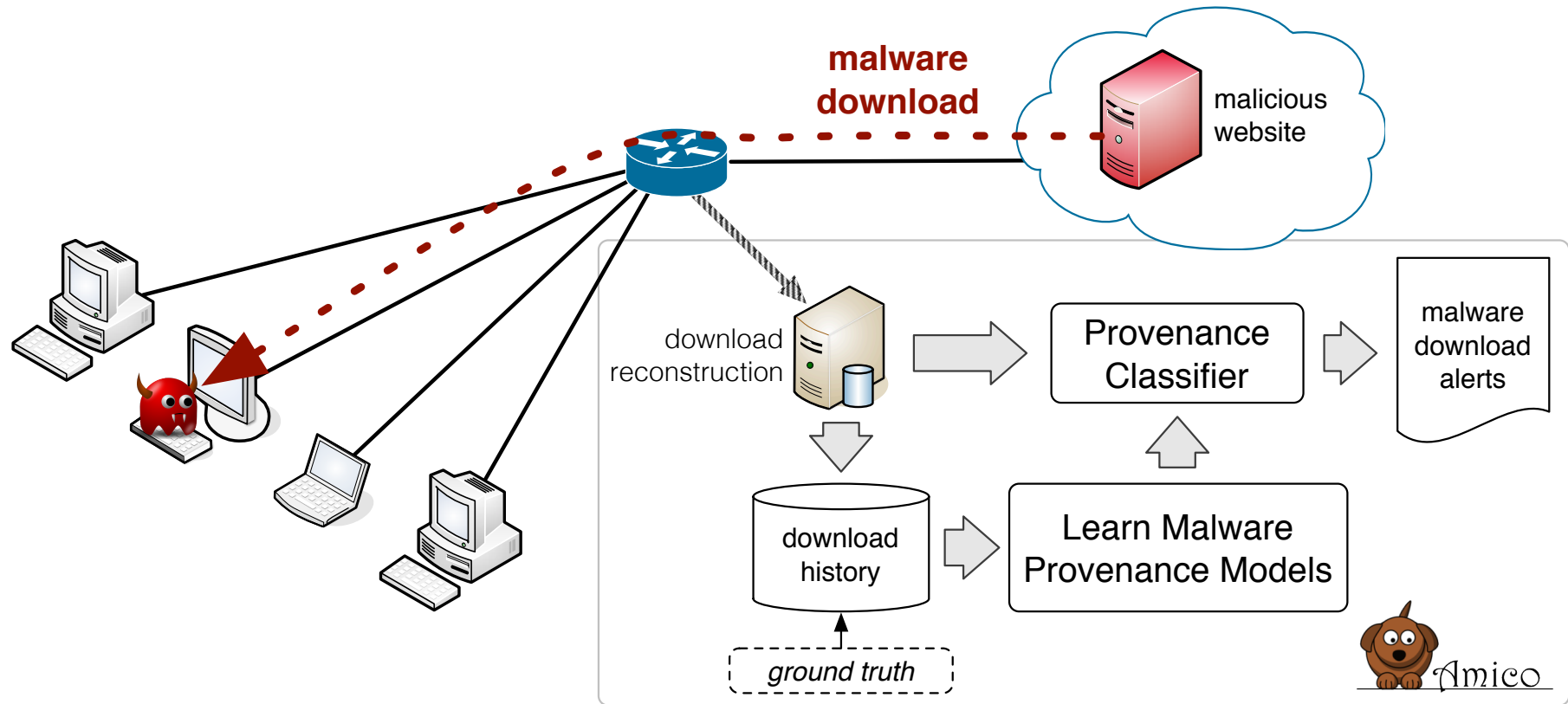


Key Observation: Malware Distribution Operations are “Agile”

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



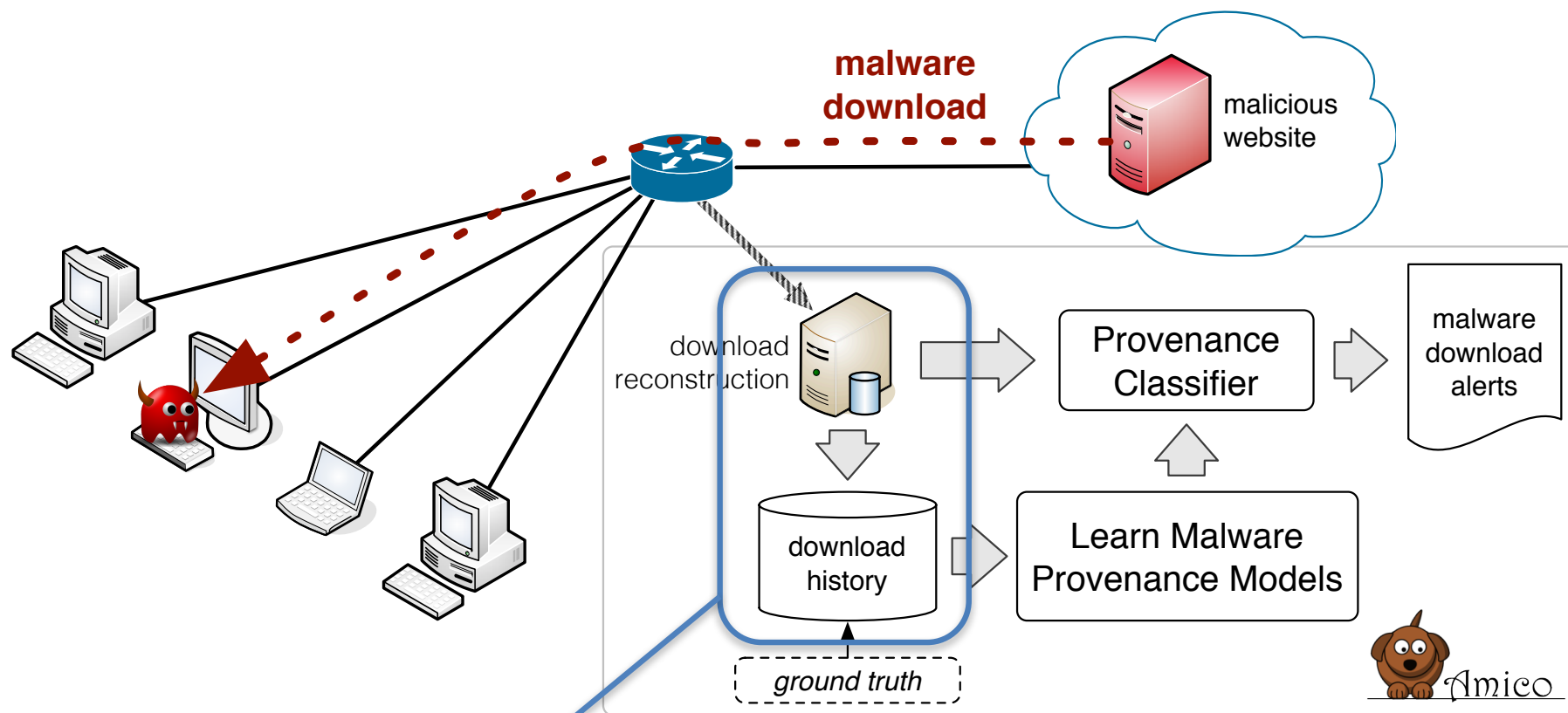
AMICO - System Overview



"Measuring and Detecting Malware Downloads in Live Network Traffic"
P. Vadrevu, B. Rahbarinia, R. Perdisci, K. Li, M. Antonakakis. ESORICS 2013



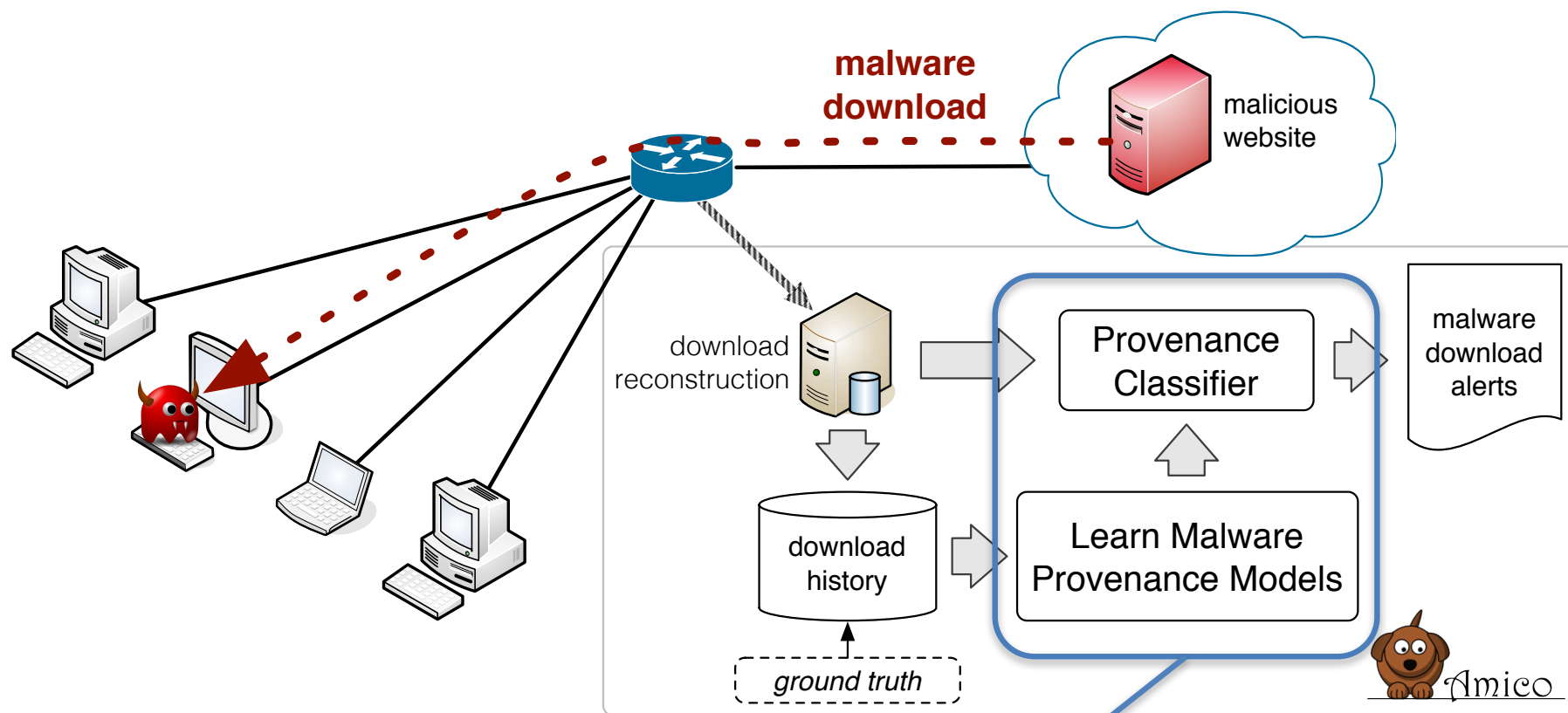
AMICO - System Overview



- Efficient passive TCP flow reconstruction
- Identify HTTP flows that carry a software download (EXE, APK, DMG, JAR)
- Store executable files and metadata (e.g., domains, IPs, URL, etc.)



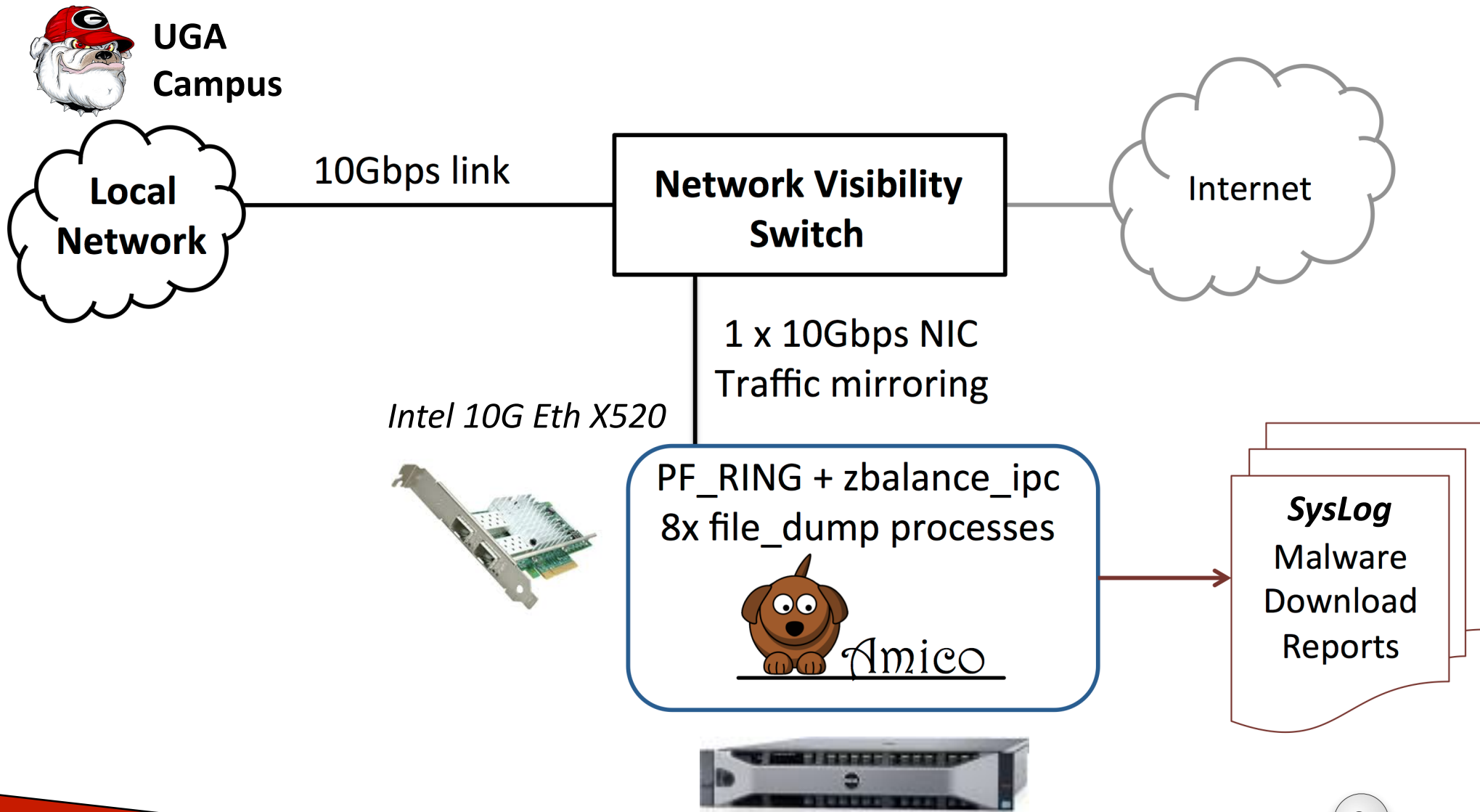
AMICO - System Overview



- Machine Learning module
- Automatically learns from past malicious/benign downloads
- Detects malicious downloads based on provenance info



Real-World Pilot Deployment



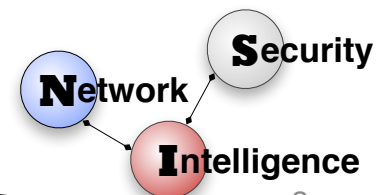
Recent Stats (UGA Pilot)

(March 1 2017 – April 15 2017)

- Detected **1,183 malicious downloads**

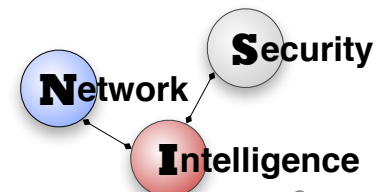
(AMICO Score > 0.7)

- Clients: 844 distinct IPs
- Downloads: 1,078 DMG, 87 EXE, 17 APK, 1 JAR
- Files: **96 DMG, 58 EXE, 10 APK, 1 JAR**
- False Alerts: 9 downloads (7 EXE, 1 DMG, 1 APK)
- *Still Unknown* to VT: **55** downloads
- **18 confirmed “Zero Days”** (previously unknown to VT)



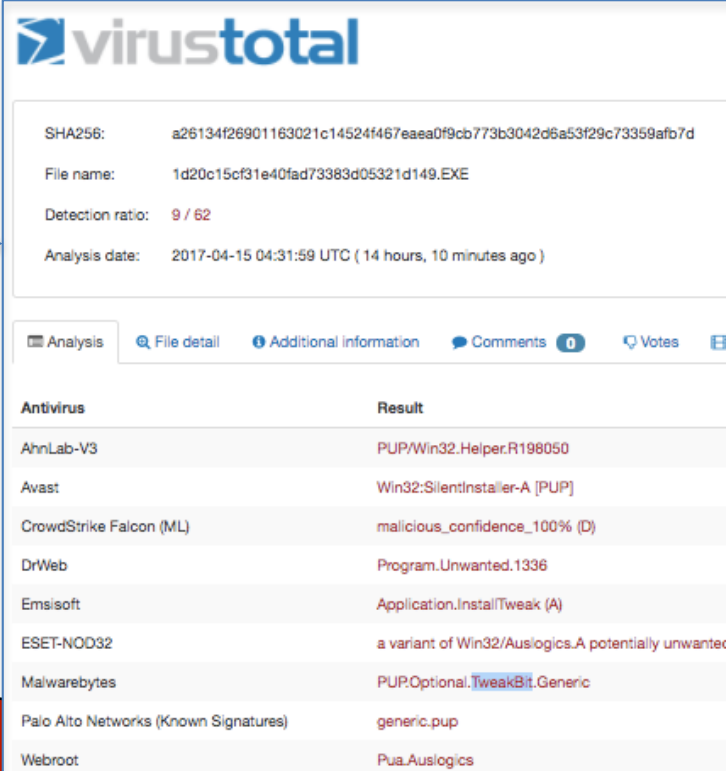
SysLog Example

- Apr 14 09:24:56 netbox2 start_amico.py:
- file download -- timestamp: 2017-04-14 09:23:46
- client_ip: 172.21.x.x, server_ip: 45.79.194.109
- server_port: 80, host: downloads.tweakbit.com
- url: /go/src_ep_cnet_optimizer_PCR_3steps_970x66_v1/en/pc-repair/stub/pc-repair-setup.exe
- referrer: None
- sha1: dff9f365b4d7b2e330e7c41bfbd1e9697438bb77
- md5: 1d20c15cf31e40fad73383d05321d149
- file_size: 356864
- *av_labels: None*
- corrupt: False
- file_type: EXE
- amico_score: MALWARE#0.792



SysLog Example

- Apr 14 09:24:56 netbox2 start_amico.py:
- file download -- timestamp: 2017-04-14 09:23:46
- client_ip: 172.21.x.x, server_ip: 45.79.194.109
- server_port: 80, host: downloads.tweakbit.com
- url: /go/src_ep_cnet_optimizer_PCR_3steps_970x66_v1/en/pc-repair/stub/pc-repair-setup.exe
- referrer: None
- sha1: dff9f365b4d7b2e330e7c41bfbd1e9697438bb77
- md5: 1d20c15cf31e40fad73383d05321d149
- file_size: 356864
- **av_labels: None** → appeared in VT one day later
- corrupt: False
- file_type: EXE
- amico_score: MALWARE#0.792



SHA256: a26134f26901163021c14524f467eaea0f9cb773b3042d6a53f29c73359afb7d

File name: 1d20c15cf31e40fad73383d05321d149.EXE

Detection ratio: 9 / 62

Analysis date: 2017-04-15 04:31:59 UTC (14 hours, 10 minutes ago)

Antivirus	Result
AhnLab-V3	PUP/Win32.Helper.R198050
Avast	Win32:SilentInstaller-A [PUP]
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)
DrWeb	Program.Unwanted.1336
Emsisoft	Application.InstallTweak (A)
ESET-NOD32	a variant of Win32/Auslogics.A potentially unwanted
Malwarebytes	PUP.Optional.TweakBit.Generic
Palo Alto Networks (Known Signatures)	generic.pup
Webroot	Pua.Auslogics



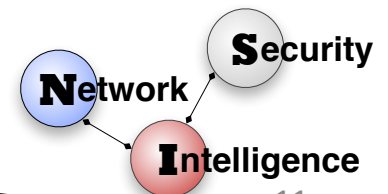
Example System Configuration

- Dell PowerEdge R730 Rack Server
- 2 x Intel® Xeon® 2.1GHz, 8C/16T
- 32GB RAM
- 4x2TB HDD
- 1Gbps NIC (e.g., Broadcom)
- 1 x Intel 10G Eth X520 DP SPF+
- Linux OS (e.g., Ubuntu Server 16.04)
- PF_RING + 10G Intel ZC driver (free for EDU)



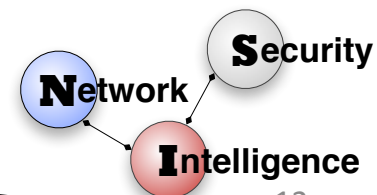
< \$6,000

- Recommended num. of CPU cores = Your Gbps of traffic X 2
 - E.g., if you have 6Gbps of traffic, use 12 CPU cores
- **Operational Skills:** Linux sys/network admin skills needed for deployment



Current Deployments

- UGA – entire campus network
 - Deployed since 2014
- UAB – entire campus network
 - Upcoming – scheduled for 15 May 2017
- GaTech – entire campus network
 - In progress, used to assist DARPA research
- Pilot preparation experience with UAB
 - Email-based communication to prepare the environment
 - Suggested HW box specs/configuration
 - Guidelines for obtaining/installing PF_RING+ZC drivers
 - On-site deployment (scheduled in May)
 - Finalize AMICO deployment and system tuning
 - Remote assistance throughout the first phases of pilot (2-3 months)





Amico

<https://github.com/perdisci/amico>



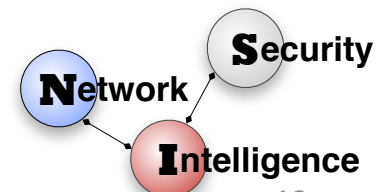
perdisci@cs.uga.edu



Funded by the *NSF Advanced Cyber-Infrastructure* and *DHS Transition to Practice* programs



University of Georgia
Dept. of Computer Science



“Kyle & Stan” Malware Campaign

timestamp	md5	host	url_substring
2014-10-07 20:46:56	a50affe80f6073231b9954d18a863d48	com.5rbo4tp3ok.wlauagbic	/iMrDLa6EEXTTBe_Yal-ygo0VN_4WaAufcm_DwQ
2014-10-06 23:40:22	4c4e8f8924fa341d1669aafaa52e468a	com.h8m8brjvp0.lidgl20mbbl9	/pZzErieHNovA8zG0xbQDsofFxjfy9yVQm7SDm
2014-10-06 18:13:49	36911d73743c3dfac3ad937317ea1fdb	com.bzkm3mhonv.mytohw79	/asdeqFVu7DP0_UySN_4Ti4mQcCVuJRgeRKxwEL
2014-10-06 17:05:02	181dfffe4a97a68f4c468f83025c9628	com.h8m8brjvp0.2wahagsemzg	/A3N_SYJSU7gqEjnGDlhx3I2QQ8lisgaZARDoqh
2014-10-06 08:47:00	f0699b7590410f4b3e8c39dc0767657a	com.5pqtst0kxpb.cklgl9zgzk0mt	/JzQIYOClt90Fi0q9-Z9R5r2didDvRhdVvYqWgUy
2014-10-05 13:04:33	30bdaa77fcd09d1016c1377538ea9a74	com.bpqot5ynq2.imaat8qb8z	/g_Crx4Y3PhQhD82S7i9e28NKAjS0r0hHDfvJDh
2014-10-05 12:54:27	51894341a4f6d1adeb62166bbcfc3638	com.323m9vqobm.cdldysj0fu	/kpcf-Bq8jP1Tf27A9Z4ye36F0v7Sok6IQG75q8
2014-10-04 19:35:10	cf1f8d516db4a2167e41b94876f6a896	com.tnr0mkb8py.3calp2vo	/zs5M73K_SqL4MYhw7fqBXC9oNN7xQPBsYR4z8d
2014-10-04 19:35:06	359517d1f124b55ef37432d749e928e7	com.tnr0mkb8py.n1pph5fr1lof	/00q0afp_oRFAR7ZTqytCVy7r-EyGX3004GrjEr
2014-10-03 22:35:26	36f15bd2dc936de27d198f5cca99d39e	com.b1o9qz6i1p.oaafht	/z-oPA2lAqG-TYHgjeiyK7fsYdsYi---Db3Mm9oI
2014-10-03 21:48:10	8222d7bc45ea17915ad87b2adc2d47b6	com.b1o9qz6i1p.0jpxh3em	/9Mmrr6sIOVKyRn0SpA0X9ar8Ys0t8PhBfz_Nz9
2014-10-03 15:52:00	b2127e857fa1726770a7b829a1117197	com.b1o9qz6i1p.rdpma03pvjcv	/cbJTr2uGQbSqEYy5VqMmB60MVXQeBxnKiXfEXK
2014-10-03 09:45:08	bc539d3caba7615286f4aac4273ef7eaf	com.jjusdwp8mx.8sa7dfw	/M-9iyA02PB0xEiRYJ6SW0VfP9fW86dAexjIjKs
2014-10-03 09:44:33	04b54e8f5d7a3ccbad77bd7058e51556	com.jjusdwp8mx.cvhwt3d7	/zrRp9u_HEpeGhfxMczeKC9Mo00lCaWbI5tBhI5
2014-10-02 16:59:35	7792cf5aa4d6ce2607a241056e044dae	com.63bphnq4s6.zwlraizqh	/wU5B0MRHN4lCM5QI_SIDpp1lmw889Nr7Ttbq1E
2014-10-02 09:12:12	3c257c57a8e8449810b47931a1f168a0	com.z79x2vbhh3.utdahp	/0c4eLwclDoZ1t_MZQnAxEMMQfhrMbb00SMhqv
2014-10-01 22:13:48	2c01966f4b00428f4782dce019a5ac3b	com.r0kr3xkbix.dya9hlfe	/D209N4ukStFCZ4DHT9SpfJMvTS8IMls6TCM6Pm
2014-10-01 22:09:30	21222f15428624ff3c0febb1d3595207	com.r0kr3xkbix.a7hcpcf8dpbe	/0iEGqb88F96R6b0KyIWIZnLudw9nZ5NVH4kBh
2014-10-01 21:13:17	bbc9fbd1ab7c2d2871e582897fc047c8	com.9d3791kwoo.fztqlwkj	/fMtWBRFE4h16Q1U_4bGcezVwgV5J1ia6F4FM_P
2014-10-01 19:57:47	cd31b935d0d808651e332691c3a37514	com.65w3dki4ux.yml1pd	/X-bkIh7-pBNv0ChNXgouJ3lerqF5oXJ_o5qGcm
2014-09-25 11:45:32	44cee915cda159ae67aad9258dc366ee	com.mxp698.kyle	/j5G7i2JDifzLQu9fytSkyEPBd5AvKhkz10cFaK
2014-09-23 14:58:48	dd231a63fc5684482fb90c16360e0b0b	com.mxp4119.kyle	/LiyoQLbDZ8q_d6M_1N0uUI8Jiv_yLDA5t5auL_
2014-09-18 09:06:47	7e5026bf4e15483dea8e152ef8e91f73	com.mxp2392.kyle	/nGtCauEJcAZ-7KBT5wmIFJaFB3pD_0EzGqMj9V
2014-09-15 21:03:39	51ed873239a4457ab29720adc5b83d57	com.mxp1194.kyle	/N747M42R9T4qg7ffbACp-05c0ZY8gjYDq13vKx
2014-09-15 16:49:29	538f95ca280e9bd2eb1418fdce31ed97	com.mxp4117.kyle	/7iSBh0mLB02kZl44ann1yxJnuVXLIZrGvlyeP
2014-09-14 13:07:28	61c50454e732f660d0a5d4d802b39bb2	com.mxp4116.kyle	/UecZZItuoCsTXPpSUUnLhwz_gJwYRIhp_EfrT
2014-09-13 10:31:21	e1adb3cd9e1c9d6600ab69e1b3dd54d6	com.mxp2387.kyle	/SmQIEj9NldgJPIbcqPyVs6YDsJjeI1gbBHSDm
2014-09-11 10:02:11	d4648214da3b60af369699a457404b93	com.mxp4116.kyle	/QHYq0Hgmz2uYpC4rpWbN9JEIaA0L1ByAOPRU4Q
2014-09-09 19:59:37	37017eb54f193bdf1854d063e596601a	com.mxp2385.kyle	/qKu5r-71aXQ1uBkNfNB0t9MD-uTnN3vejB7kcx
2014-09-09 14:21:07	58e45b71360323d31baa8869cd3c6bb6	com.mxp1193.kyle	/_eDeui0ltjefP9QwCqfHR95zYzuKDrFd4QMcPC
2014-09-08 22:29:36	20bd30be10788c6a364fb4af6a372d97	com.mxp2375.kyle	/BYAeCUC73700qeLkFVZXmL8MreDr2Zfkt7LK2g
2014-09-08 14:50:21	470dc6635ade7d22eb38118cc921930d	com.mxp4110.kyle	/ISiyoPyKY0bvLke3wdifBYr6j1PG4T_HqpCHEk
2014-09-07 20:04:07	c114bf333b5629c80eae34bad2640276	com.mxp2368.kyle	/IF9dqf42xrF0MSVeZs0YFAHltXUUEX3o1tbY1C
2014-09-07 13:38:07	6b2cb1d0e566bec99da510b91dcfce54	com.mxp2367.kyle	/p-FIbfXDSZ7F4zeSid94KkDG0acYDEZNT71r2t
2014-09-07 04:12:18	2f43065d9312f8be3712dc7c1e2c571e	com.mxp4103.kyle	/puK0fC8DsylpBEbBnQwdILbiUFsH_92-ePP9ra
2014-09-06 13:07:50	078dbf4272ca0fd77455a9f50e036071	com.mxp4103.kyle	/n1ecgvmgGF0RUGMyHqx48hYcJRHbju5goWNV6E
2014-09-05 23:33:59	17955285c8f2dceab925bef0aa340738	com.mxp4103.kyle	/ZBoF5lmWR9VvijtEww1HXbvKMO-RuIjw2DS1N6
2014-09-05 22:11:40	61253d353c7cb349a26209e970fcd72b	com.mxp4103.kyle	/tLwXSWiMtwxIhrfeS3byLbhW9zAUKPBhMduL_
2014-09-05 12:44:37	31a3daceef2c48a9681785bf41eec24e	com.mxp2364.kyle	/HP1N0XV6hzPhZwxuNBozCJtaCIw-0nNfc6g5p
2014-09-05 09:51:10	df96a3be44cad13e10ed5c2222749263	com.mxp4102.kyle	/a-pgu3-GAqpNMeHhFULXsmgk0GQOA70smmHL90

“Install-cdn” Malware Campaign

timestamp	md5	host	score	tavs	avs	vt_query
2015-04-02 12:39:22	ac336a1f87d565727dd474b1ee91926e	net.frameddisplay.install-cdn	0.602	2	26	2015-04-03
2015-04-02 11:23:14	9ddca7a04d79a67c95f6d9d427218458	net.sunrisebrowse.install-cdn	0.618	4	27	2015-04-03
2015-04-02 11:12:47	86e66e57832051b69ce14d385c70ebcf	com.klippal.install-cdn	0.573			2015-04-03
2015-04-02 10:35:26	0fb1968e5872850f5767e8824b66efe7	info.appenable.install-cdn	0.642	4	29	2015-04-03
2015-04-02 10:11:59	386eaa5aa50db489ca49f0cecc30eb74	net.frameddisplay.install-cdn	0.582	2	25	2015-04-03
2015-04-02 08:57:57	a25ea139a702a88eff5fbafbedd99dc1	com.cdnhigheraurum.install-cdn	0.607			2015-04-03
2015-04-02 08:38:10	386eaa5aa50db489ca49f0cecc30eb74	net.frameddisplay.install-cdn	0.586	2	25	2015-04-03
2015-04-02 08:19:15	386eaa5aa50db489ca49f0cecc30eb74	net.frameddisplay.install-cdn	0.623	2	25	2015-04-03
2015-04-02 08:16:41	267d86fdd6d4ff966df555715ab5b8ce	net.betterbrowse.install-cdn	0.567			2015-04-03
2015-04-02 04:44:19	648922b79ba36f53de907d7b35af2f5b	net.frameddisplay.install-cdn	0.614			2015-04-03
2015-04-02 03:31:24	beb012090fffed8806010cb4c507d5a0	net.betterbrowse.install-cdn	0.501			2015-04-03
2015-04-01 23:18:25	4a3dbc6f4028c5239e5b29e258b9d715	net.betterbrowse.install-cdn	0.547			2015-04-03
2015-04-01 22:45:12	ae6ef2bd26aa545be4400e28adbbd0a0	com.useclearthink.install-cdn	0.577			2015-04-03
2015-04-01 22:45:03	b3241b4c45a3f4a480d387cc19544fa4	net.frameddisplay.install-cdn	0.566			2015-04-03
2015-04-01 22:01:26	b3241b4c45a3f4a480d387cc19544fa4	net.frameddisplay.install-cdn	0.582			2015-04-03
2015-04-01 21:54:49	ae32b32111d7d66c609b77347bac8a23	net.sunrisebrowse.install-cdn	0.602	4	28	2015-04-03
2015-04-01 21:47:24	b3241b4c45a3f4a480d387cc19544fa4	net.frameddisplay.install-cdn	0.586			2015-04-03
2015-04-01 21:43:46	6aef165abeb49f8825ffe088647834be	info.appenable.install-cdn	0.642	4	31	2015-04-03
2015-04-01 21:38:34	f4109213d2c51ec5da63b797bded8af5	com.klippal.install-cdn	0.573			2015-04-03
2015-04-01 21:33:18	a0cf813756be99658dbce82b26eb1cc2	info.enterdigital.install-cdn	0.643	5	32	2015-04-03
2015-04-01 20:32:01	26af97ea8b262cfc339785fcf5072736	info.enterdigital.install-cdn	0.651	5	32	2015-04-03
2015-04-01 19:53:36	e56b8f4320c1828855da769d1c461317	net.sunrisebrowse.install-cdn	0.602	4	26	2015-04-03
2015-04-01 19:42:35	4b49d6a266ad9e47ec6503b5f1893cdd	info.appenable.install-cdn	0.602	4	32	2015-04-02
2015-04-01 18:36:51	7ba3bef6cd6e0dd5b3dbeb0900183000	com.klippal.install-cdn	0.573			2015-04-03
2015-04-01 17:09:51	4b49d6a266ad9e47ec6503b5f1893cdd	info.appenable.install-cdn	0.605	4	32	2015-04-02
2015-04-01 16:59:39	78ec9b1941bdb658d8f70ef8a18c401d	com.advanceelite.install-cdn	0.614	3	25	2015-04-02
2015-04-01 16:46:11	a6ae1c13e6235e16b03346bb3cf959b3	net.frameddisplay.install-cdn	0.602	2	26	2015-04-02
2015-04-01 16:45:16	a6ae1c13e6235e16b03346bb3cf959b3	net.frameddisplay.install-cdn	0.586	2	26	2015-04-02
2015-04-01 12:46:50	7055a5c8e00a94171e3f22c96fad668e	com.advanceelite.install-cdn	0.587	3	26	2015-04-02
2015-04-01 12:18:32	ba156ea1831685c088edd21fe5905a76	info.appenable.install-cdn	0.616	4	29	2015-04-02
2015-04-01 12:01:10	ba156ea1831685c088edd21fe5905a76	info.appenable.install-cdn	0.626	4	29	2015-04-02
2015-04-01 11:49:20	4ea2ce12f62f4292b364e7a390432e93	com.klippal.install-cdn	0.582			2015-04-02
2015-04-01 09:15:53	92ac368e7fa715ab76fc80fa36b6b67b	net.sunrisebrowse.install-cdn	0.622	4	28	2015-04-02
2015-04-01 08:45:33	5255294011d48f7a931bed1252e5b207	com.browsestudio.install-cdn	0.634	3	29	2015-04-02
2015-04-01 06:59:11	24c5599ade4e2668f007f9f7f4f6471b	net.frameddisplay.install-cdn	0.643	2	26	2015-04-02
2015-04-01 01:58:00	6f16686b262d5bc93eb76a2bc5b8bf15	net.frameddisplay.install-cdn	0.615	2	26	2015-04-02
2015-03-31 21:59:58	3a561156103f16abda75b7bdcc857b29	com.advanceelite.install-cdn	0.583	3	27	2015-04-02
2015-03-31 21:41:14	3a561156103f16abda75b7bdcc857b29	com.advanceelite.install-cdn	0.583	3	27	2015-04-02
2015-03-31 21:36:40	830196e2333ef9e3b2ecd564d27258ee	com.klippal.install-cdn	0.568			2015-04-02

```
amico_file_dumps=> SELECT timestamp,md5,host,server,type,score,tavs,avs,vt_query FROM amico_summary_2 where score>0.5 and timestamp > '20160101' and type='EXE'
' and (corrupt='f' or avs is not null) and host like '%.%.intva31' order by timestamp desc;
```

timestamp	md5	host	server	type	score	tavs	avs	vt_query
2016-05-16 17:38:53	529cb1f56ba259f83a8f925bf622f613	info.technologycipher.intva31	52.72.142.4	EXE	0.642	0	5	2016-05-16
2016-05-16 17:38:08	529cb1f56ba259f83a8f925bf622f613	info.technologycipher.intva31	52.72.142.4	EXE	0.662	0	5	2016-05-16
2016-05-09 11:06:07	20bc96281ee08407a29a54922c99907d	info.preciousinterface.intva31	52.72.142.4	EXE	0.708	0	1	2016-05-09
2016-04-26 13:37:05	695f882c722843ddfdb0a626f4cc20e	info.twininstall.intva31	52.72.142.4	EXE	0.66	1	12	2016-04-26
2016-04-19 08:26:53	bb55b5a74ce0617d4773acc2ebf3139	info.firststarload.intva31	52.72.142.4	EXE	0.68	3	15	2016-04-19
2016-04-18 11:04:28	96117c85541aa11652bd4f953f9435ac	info.propelbyte.intva31	52.72.142.4	EXE	0.699			2016-04-18
2016-04-18 03:25:17	f44b069fd47f554543a21fd07baae77f	info.computerbeta.intva31	52.6.18.250	EXE	0.571			2016-04-18
2016-04-18 03:23:39	1bb69956d1444b5afec617be913a9b3f	info.instituteautomation.intva31	52.72.142.4	EXE	0.895	2	14	2016-04-18
2016-04-18 03:23:38	1bb69956d1444b5afec617be913a9b3f	info.instituteautomation.intva31	52.72.142.4	EXE	0.724	2	14	2016-04-18
2016-04-17 13:45:27	e1f6deaf2611b07f519a8879fb5f33ad	info.inspiredesktop.intva31	52.72.142.4	EXE	0.68	4	17	2016-04-17
2016-04-13 09:33:48	2f7bd59c9b23f0d2c111453d3198ad02	info.beginvac.intva31	52.72.142.4	EXE	0.917	2	7	2016-04-13
2016-04-13 09:33:12	2f7bd59c9b23f0d2c111453d3198ad02	info.beginvac.intva31	52.72.142.4	EXE	0.628	2	7	2016-04-13
2016-04-12 09:54:04	28bb75177affb5e769d898cb79c28f16	info.innovatesite.intva31	52.72.142.4	EXE	0.628	2	8	2016-04-12
2016-04-11 19:10:03	327231b7e9c7c45653f06ab4bd361e68	info.visionaryhyper.intva31	52.72.142.4	EXE	0.937	2	7	2016-04-11
2016-04-11 19:08:14	327231b7e9c7c45653f06ab4bd361e68	info.visionaryhyper.intva31	52.72.142.4	EXE	0.648	2	7	2016-04-11
2016-04-09 11:42:35	f24d83757ec7270ea2acaf7ba2898dba	info.computermarketing.intva31	52.72.142.4	EXE	0.672	1	6	2016-04-09
2016-04-06 14:21:11	dcf4ec1678bcea6c5d88fc29da00a25f	info.memoryproperties.intva31	52.72.142.4	EXE	0.701	2	10	2016-04-06
2016-04-05 11:55:46	03097b2ac03d1cf5beeb7eb049b47a9	info.cpufinancing.intva31	52.72.142.4	EXE	0.664	2	12	2016-04-05
2016-04-03 20:25:52	a61204fdeee866515a374e570a38f7e3	info.droveexpert.intva31	52.72.142.4	EXE	0.922	2	9	2016-04-03
2016-04-03 13:37:23	a61204fdeee866515a374e570a38f7e3	info.droveexpert.intva31	52.72.142.4	EXE	0.628	2	9	2016-04-03
2016-03-30 21:58:40	378f8caf901336ce950a83a40b7fe1f7	info.peripheralincorporated.intva31	52.72.142.4	EXE	0.901	1	2	2016-03-30
2016-03-30 13:53:51	b7f9f2abad93cd9edbb6d60bfff4cfff	info.peripheralincorporated.intva31	52.72.142.4	EXE	0.613	1	4	2016-03-30
2016-03-29 01:06:25	6ebfb4f2a50f2f1e95cafe83789f8f81	info.computerbeta.intva31	52.6.18.250	EXE	0.723	1	7	2016-03-29
2016-03-29 01:06:25	6ebfb4f2a50f2f1e95cafe83789f8f81	info.computerbeta.intva31	52.6.18.250	EXE	0.813	1	7	2016-03-29
2016-03-25 05:30:48	59edaeb1c450462745c9abddfdda516f	info.computingcase.intva31	52.73.18.100	EXE	0.968	5	25	2016-03-24
2016-03-25 05:29:21	59edaeb1c450462745c9abddfdda516f	info.computingcase.intva31	52.73.18.100	EXE	0.942	5	25	2016-03-24
2016-03-24 21:28:54	59edaeb1c450462745c9abddfdda516f	info.computingcase.intva31	52.73.18.100	EXE	0.631	5	25	2016-03-24
2016-03-18 09:12:46	6306871a2ba84ae8a6ddcd3dbd7e941	info.memorydriver.intva31	52.72.142.4	EXE	0.543	3	11	2016-03-18
2016-03-10 12:35:24	cdf4c34f58b0f7fb909126ea163e3b52	info.mousedata.intva31	52.73.18.100	EXE	0.507	1	15	2016-03-10

(29 rows)

