Observations and Lessons Learned from Comparing Point-in-time Cleaning against Real-time Protection

Scott Wu
Program Manager, Microsoft

Agenda

- Point in time cleaning vs. RTP
- MSRT vs. Microsoft Security Essentials
- Threat events & impacts
- More on MSRT / Security Essentials

MSRT vs. Microsoft Security Essentials

- MSRT
  - Microsoft Windows Malicious Software Removal Tool
  - Deployed to Windows Update, etc. monthly since 2005
  - On-demand scan on prevalent malware
- Microsoft Security Essentials
  - Full AV
  - RTP
  - Inception in Oct 2009

Roles of Cleaner vs. RTP

- RTP is the solution
- One-off cleaner has its role
  - Quick response
  - Workaround
  - Baseline ecosystem cleaning
- Industry response & collaboration

Threat Events

MSRT Top 10 Threats

- **Worms** (some are bots) have longer lifespans
- Rogues move on quicker

Mar 2010		Apr 2010		May 2010		Jun 2010		Jul 2010		Aug 2010	
Frethog	979,427	Frethog	880,246	Frethog	465,351	Taterf	1,237,155	Taterf	797,935	Taterf	451,561
Taterf	497,582	Taterf	393,729	Taterf	447,849	Frethog	535,627	Alureon	493,150	Alureon	436,566
Rimecud	371,646	Alureon	308,673	Alureon	441,722	Rimecud	341,778	Frethog	473,996	Bubnix	348,120
Hamweq	289,603	Rimecud	289,629	Rimecud	318,041	Alureon	292,810	Bubnix	471,243	Rimecud	287,942
Conficker	286,091	Hamweq	250,286	Conficker	220,475	Conficker	237,348	Rimecud	280,440	Vobfus	251,335
Renos	202,495	Conficker	245,919	Hamweq	192,173	Hamweq	206,217	Conficker	173,745	Sality	249,249
PrivacyCenter	168,403	Renos	138,931	Renos	135,266	Renos	162,106	Renos	151,845	Frethog	241,009
FakeXPA	134,896	Bancos	129,627	Cutwail	125,334	Koobface	118,215	Hamweq	144,657	Conficker	216,057
Bancos	124,824	Bredolab	117,864	Bancos	97,586	Bancos	111,123	**FakeSpypro**	139,900	**FakeSpypro**	167,847
Alureon	124,771	**FakeXPA**	115,636	Oficla	87,967	Bredolab	109,050	Bancos	81,276	Renos	161,233

Security Essentials Top 10 Threats

- Worms dominate
- Exploits are commonly used

June 2010		July 2010		August 2010	
Autorun	676,058	Autorun	990,338	Pornpop	1,350,645
Conficker	389,610	**CVE-2008-5353**	541,422	Autorun	1,121,190
Rimecud	333,255	**CVE-2009-3867**	392,019	**CVE-2009-3867**	429,595
IframeRef	268,804	Conficker	370,760	**CVE-2008-5353**	415,110
Wimad	258,102	OpenConnection	318,032	Conficker	397,011
Taterf	250,497	Renos	306,413	Keygen	335,077
Obfuscator	229,396	**IframeRef**	300,664	Rimecud	331,815
Keygen	225,324	Rimecud	293,953	Renos	323,187
Renos	215,373	Keygen	257,684	OpenConnection	317,463
VBInject	206,645	FakeSpypro	255,940	Obfuscator	294,403

MSRT Top 10, by Country/Region

- One month vs. 12 months

August 2010		12 months	
United States	928,442	United States	9,441,827
Brazil	266,862	Brazil	2,571,129
Korea	220,321	Korea	2,156,838
Spain	171,632	Spain	1,782,187
France	142,340	**China**	1,345,176
Turkey	142,180	France	1,319,409
United Kingdom	103,531	Turkey	1,216,817
Mexico	101,539	United Kingdom	1,007,263
Taiwan	89,882	Taiwan	934,613
Germany	83,450	Mexico	914,727

Security Essentials on Select Threats

- Threats newly covered by MSRT
- Still need full AV!

June 2010		July 2010		August 2010	
Rimecud	333,255	Rimecud	293,953	Rimecud	331,815
FakeSpypro	195,700	FakeSpypro	255,940	FakeSpypro	216,295
Vobfus	101,567	Vobfus	119,024	Vobfus	156,693
FakeVimes	58,114	Pushbot	62,359	FakeVimes	85,241
Pushbot	40,585	Bubnix	42,439	Bubnix	62,398
Bubnix	37,946	FakeVimes	42,342	Pushbot	34,332
Oficla	31,623	Oficla	24,214	Oficla	25,915
Fakeinit	5,840	Fakeinit	7,368	PrivacyCenter	11,297
PrivacyCenter	3,357	PrivacyCenter	3,060	Fakeinit	5,679

MSRT Reinfection

- Removal tool is NOT a replacement for AV

Threat	yearly reinfection	yearly total infection	yearly reinfection rate
Worm:Win32/Taterf.B	1,913,467	5,814,094	32.91%
PWS:Win32/Frethog.gen!B	511,281	2,535,746	20.16%
PWS:Win32/Frethog.gen!H	363,923	1,411,087	25.79%
Trojan:Win32/FakeXPA	63,929	1,391,194	4.60%
Trojan:WinNT/Alureon.D	54,072	1,147,509	4.71%
Worm:Win32/Hamweq.A	183,246	1,045,606	17.53%
Worm:Win32/Conficker.B	196,290	1,042,713	18.82%
Worm:Win32/Conficker.C	151,612	864,660	17.53%
Trojan:Win32/Yektel.A	23,518	854,921	2.75%
Trojan:Win32/FakeSpypro	84,924	846,580	10.03%
all	**7.17 millions**	**48.28 millions**	**14.85%**

Win32/Oficla Trojan

- Oficla: first added to MSRT in May-2010
- Correlation: multiple threats on an infected machine
- Some were **confirmed** as same threat event

Security Essentials Apr2010 Other Family	% of Oficla detected machines	**MSRT May2010 Other Family**	% of Oficla infected machines	**Security Essentials May2010 Other Family**	% on Oficla detected machines
Meredrop	11.8%	*Cutwail*	8.1%	Ransom	17.5%
FakeRean	7.4%	*FakeRean*	3.0%	Meredrop	7.7%
Alureon	7.2%	Renos	2.2%	Qhost	6.9%
Obfuscator	6.4%	*Alureon*	1.6%	Obfuscator	6.5%
Renos	6.4%	Frethog	1.1%	Autorun	

MSE, month-1

MSRT, 1st month

MSE, month after MSRT inclusion

Win32/Oficla Business Model

- Oficla Toolkit – “Oficla-ware”
- USD450-700 per package
- Installed and spammed by multiple independent 'distributors'
- Spam: Cutwail partnership
- Eradication more difficult
- Need full AV!

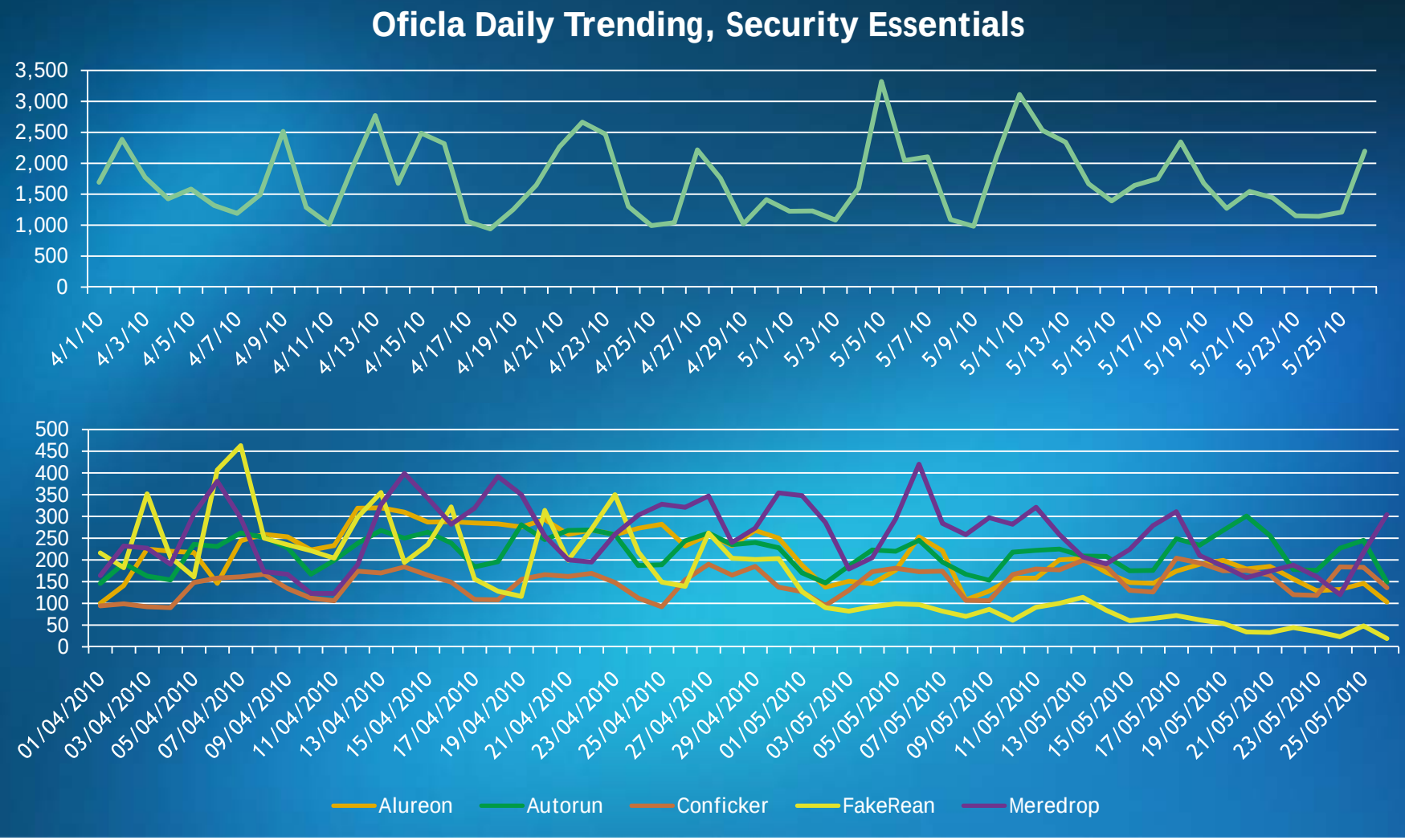
Observed Oficla Servers

- Dominated by .cn and .ru

124.217.239.26	ks45tn2.cn	designfolkov.ru	solomacosx.org
193.104.22.61	ldsma.com	det0xcorp.kz	sprutsss.in
77.221.153.183	lightobmen.ru	dionada.com	spuperrrtransfer.com
84.19.161.62	luboydomen.cn	dnsresourcecenter.com	sscanner.ru
87.118.81.62	magentox.net	dosuguss.net	system-dns.net
91.188.59.21	malahovplus.com	ecountertracker.cc	system-on.com
ablegang.com	marketingsites.info	elkadoman2.net	system-resolve.com
adjamadja.cn	mirikas.cn	enzoforfree.ru	tomorrrrow.cn
adm1n.ru	modsm.com	everybots.com	topdns24.com
adv.businessmaster.in	mutant-star.net	ezsdo.com	topdns241.com
aervrfhu.ru	myldxs.com	factoryofgood.ru	topdns341.com
andige.net	mylodka.net	fernandohuentos.com	umor.uz.ua
antiviruspc-update.com	myxmad.com	findactions.net	underskyz.cn
apsight.ru	nebuhai.com	flashvideomovie.com	uploadfilm1.org
autotradersuk.net	netmegasite.net	fooofle.ru	vampirizmu.net
avppi.com	newdaypeace.org	freesoftware-multimedia.com	vanus.biz
baksomania2010.ru	nonstopacc.com	frogber.com	vertelitt.com
bankmob1l.cc	omega5.cn	funnylive2010.ru	vitamelatonin.biz
bizevery.com	papaanarhia.cn	garavangzik.com	web-pings.net
brainzzz.net	postfolkovs.ru	googga.com	winxpupdate.org
buyexplaine.com	poteriapoter.com	hoopforbes.com	wow.telesweet.net
centralsheep.com	puthere.info	hulejsoops.ru	www.freecapch.info
client158.faster-hosting.com	republicdemocracy.cn	ieksmanskasdk.com	www.yoookolai.ru
da-google.com	salamangzan.com	inroyal.info	xtubez.org
dabubbagump.com	santorinc.com	ipv6i.tw	yaftop.com
dallynews.cn	servhb.com	itnatcompip.com	yarostt.net
davidbredov.ru	sktdo.com	justmyl.com	ydopr.com
davidopolko.ru	sogom.net	klirricon.com	zflaersroot.cn

Win32/Oficla Trending

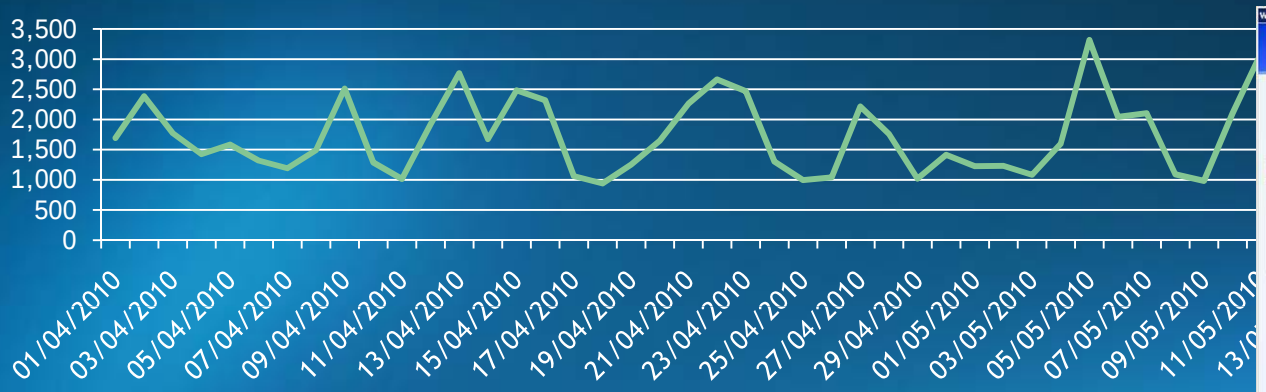
- Daily activities varied
- Diversified partnership

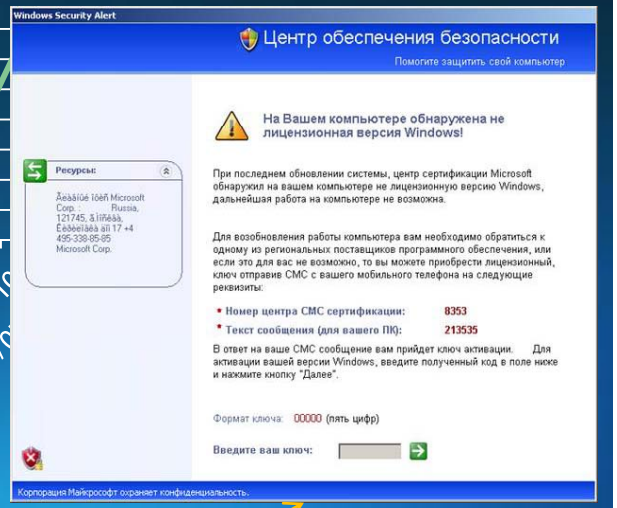


Win32/Oficla Trending, (cont')

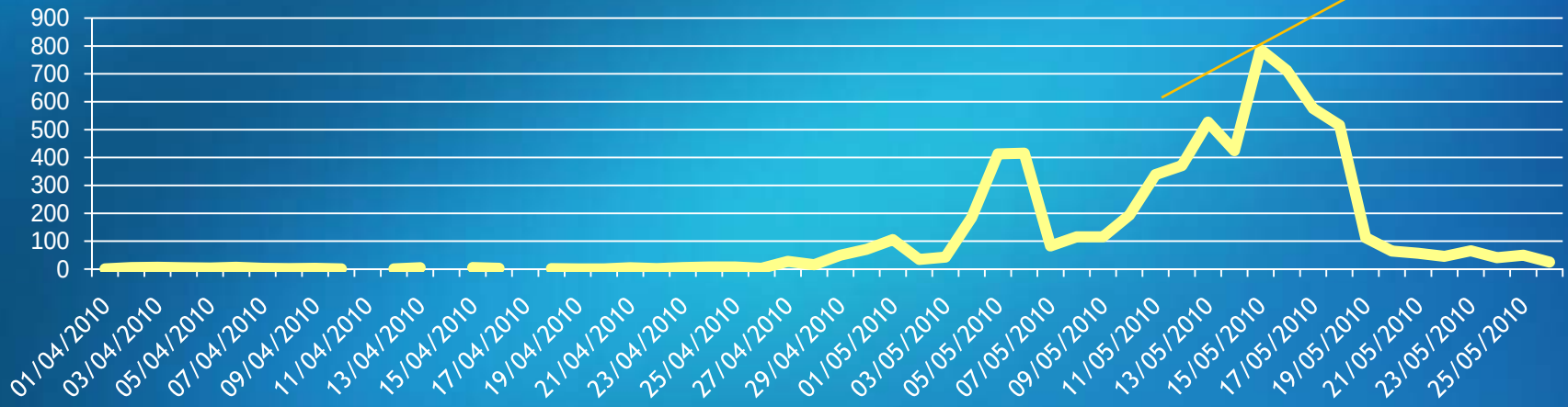
- Partner with "Ransom-ware"?

Oficla Daily Trending, Security Essentials





Win32/Ransom on Oficla infected machines

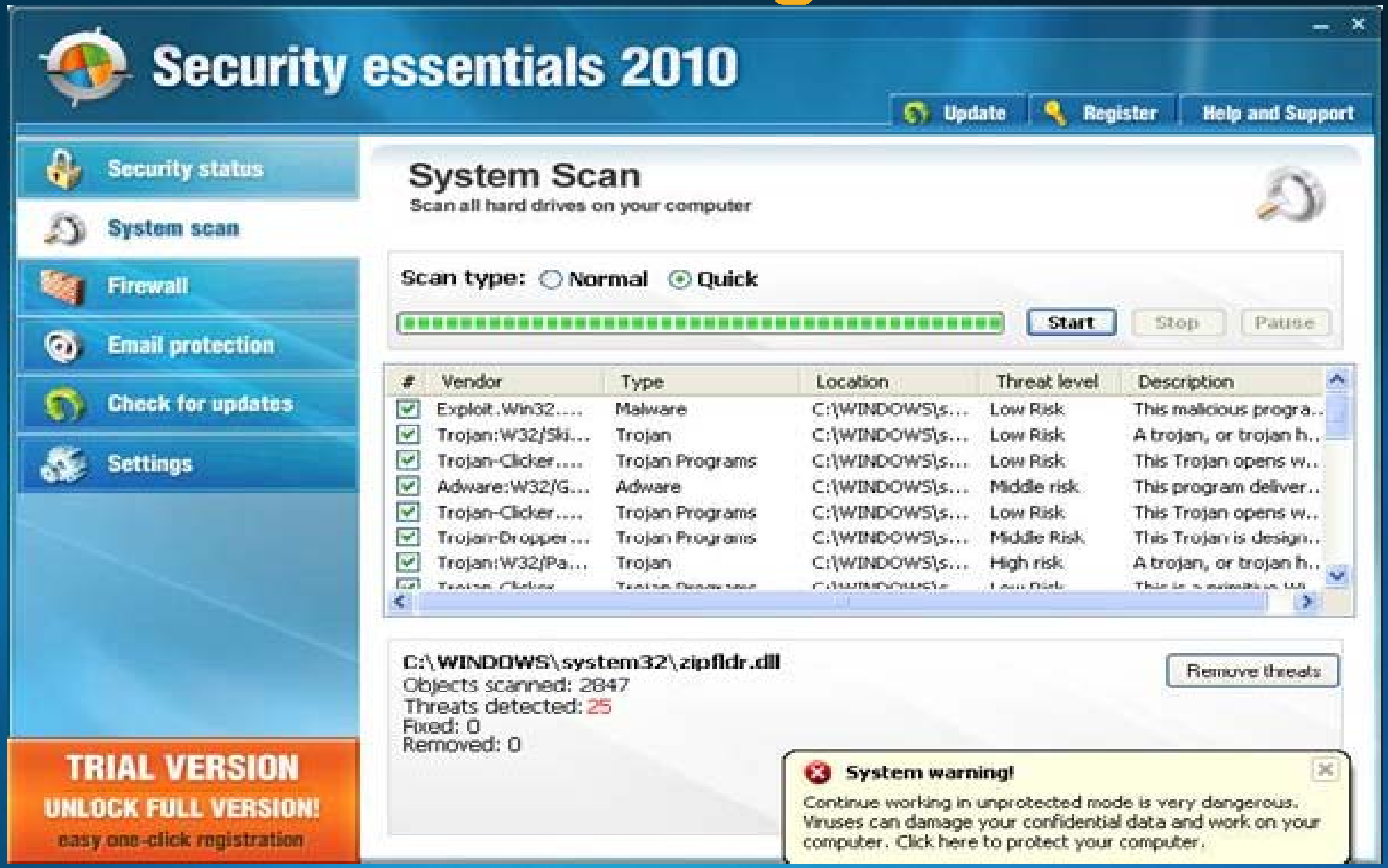


Win32/Rimecud Worms

- Added to MSRT in Jan 2010
- a.k.a butterfly/Mariposa botnet
- Rimecud Toolkit, similar to Oficla model
- Other **worms** infected/attacked the same machines
- USB, IM, Skype infection channel

Security Essentials Dec2009 Other Family	% of Rimecud detected machines	**MSRT Jan2010 Other Family**	% of Rimecud infected machines	**Security Essentials Jan2010 Other Family**	% of Rimecud detected machines
Autorun	**30.5%**	**Hamweq**	**9.6%**	**Autorun**	**31.3%**
Taterf	18.1%	**Taterf**	1.6%	**Conficker**	17.0%
Conficker	16.7%	IRCbot	0.8%	**Taterf**	15.1%
DelfInject	12.0%	Renos	0.5%	DelfInject	13.3%
Sality	11.2%	**Conficker**	0.5%	Sality	11.2%

Win32/FakeInit Rogues



Win32/Koobface

- Confirmed VBInject partnership: anti-detection
- Another confirmed payload: Win32/FakeXPA

MSRT Aug2010 Other Family	**% of Koobface Infected Machines**	**Security Essentials Aug2010 Other Family**	**% of Koobface detected Machines**
FakeSpypro	8.4%	Malagent	22.1%
Alureon	4.8%	Alureon	18.6%
Renos	3.7%	Renos	16.3%
FakeXPA	2.3%	**VBInject**	14.6%
Vobfus	2.1%	CVE-2008-5353	14.4%

MSRT Covered Online Game PWS

- Still detected by Security Essentials…still need full AV!

August 2010 MSRT		August 2010 Security Essentials	
Taterf	415,144	Taterf	157,365
Frethog	224,923	Frethog	58,914
Magania	32,255	Lolyda	12,968
Lolyda	21,441	Ceekat	3,609
Ceekat	4,048	Magania	2,056
Helpud	519	Helpud	163
Corripio	201	Tilcun	25
Tilcun	130	Zuten	17
Zuten	103	Storark	15
Storark	19		

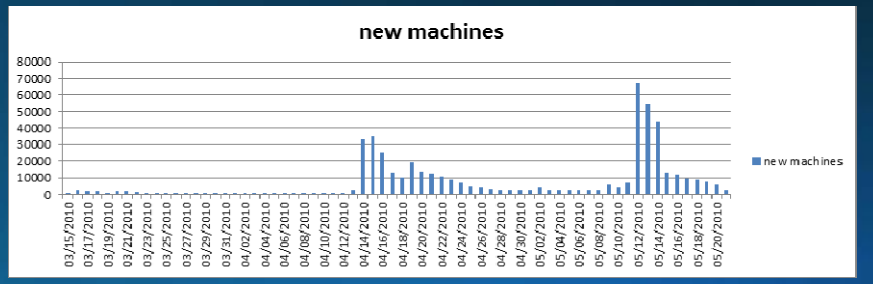
Online Banking PWS Variants

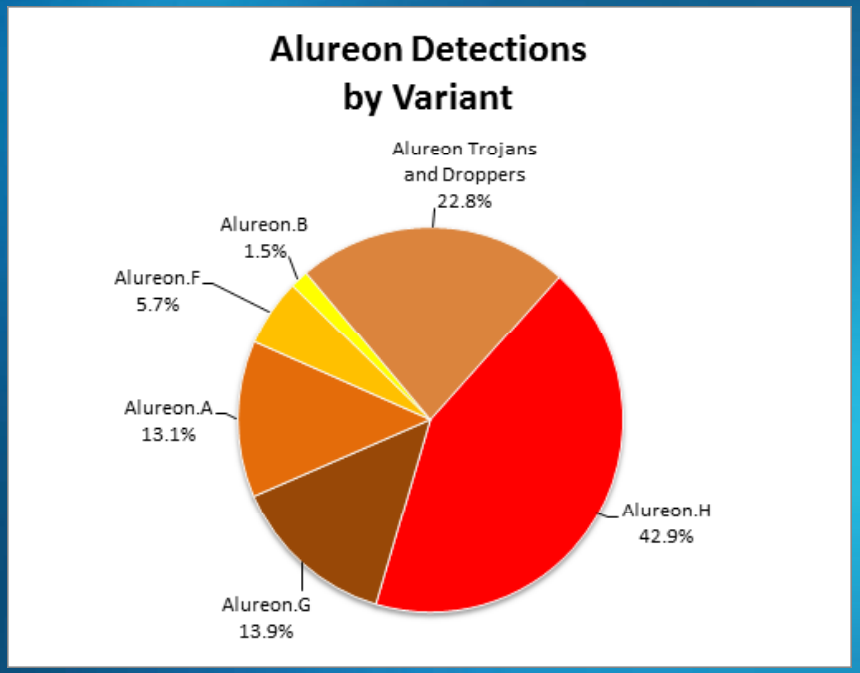
- More downloaders (Banload) by Security Essentials

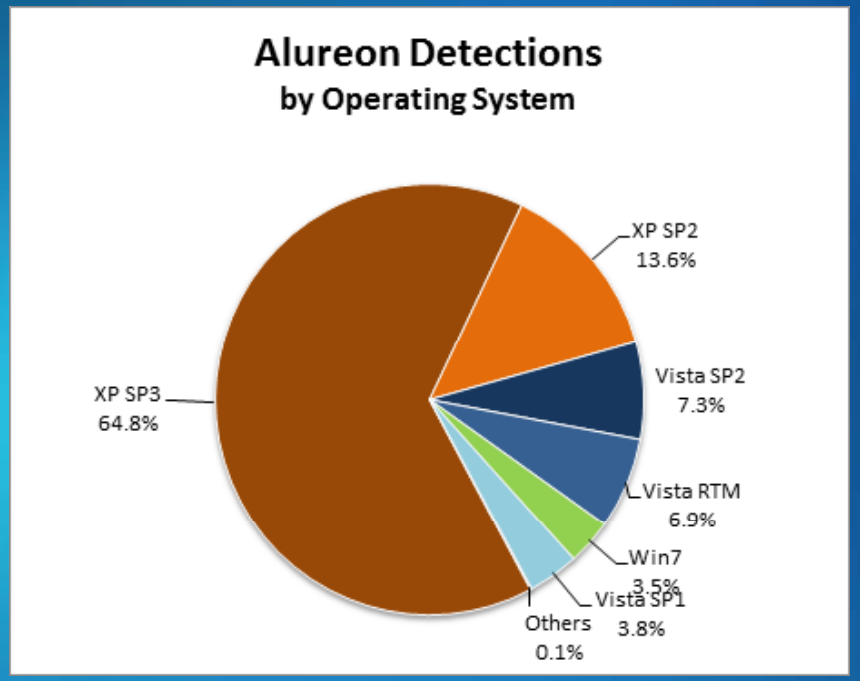
MSRT Aug 2010		Security Essentials Aug 2010	
TrojanSpy:Win32/Bancos.VI	51,141	TrojanSpy:Win32/Bancos.OO	20,328
TrojanSpy:Win32/Bancos.DI	30,928	TrojanDownloader:Win32/Banload.KJ	16,318
TrojanSpy:Win32/Bancos.AZT	23,969	TrojanSpy:Win32/Bancos.DV	15,527
TrojanSpy:Win32/Bancos.DV	22,514	TrojanDownloader:Win32/Banload.PF	12,441
TrojanSpy:Win32/Bancos.VH!sys	18,862	TrojanSpy:Win32/Bancos.DI	12,101
TrojanSpy:Win32/Bancos.PI	8,746	TrojanDownloader:Win32/Banload.OV	11,102
TrojanSpy:Win32/Bancos.OO	8,593	TrojanDownloader:Win32/Banload.PC	8,571
TrojanSpy:Win32/Banker.QI	8,588	TrojanDownloader:Win32/Banload.OZ	6,325
TrojanDownloader:Win32/Banload.gen!N	6,808	TrojanSpy:Win32/Bancos.gen!A	5,834
TrojanSpy:Win32/Bancos.KY	4,819	TrojanSpy:Win32/Bancos.PI	5,010

Win32/Alureon

- half million reported bots Apr2010 – May2010
- MS10-015 error handling







Threats per Detected Machine

- Full AV
  - Real time blocking
  - Scheduled scan
  - Full signature set

Security Essentials Apr2010				MSRT Apr2010			
Family	Threat Count	Machine Count	Threats per Machine	Family	Threat Count	Machine Count	Threats per Machine
Total	32,925,166	4,604,583	**7.2**	Total	4,733,245	3,408,383	**1.4**
Autorun	1,599,148	592,025	2.7	Frethog	1,140,591	880,246	1.3
Conficker	3,661,008	356,745	10.3	Taterf	459,681	393,729	1.2
Wimad	958,510	297,726	3.2	Rimecud	316,333	289,629	1.1
Rimecud	777,348	285,896	2.7	Hamweq	277,432	250,286	1.1
Obfuscator	779,254	280,130	2.8	Conficker	278,530	245,919	1.1

Selected Bots Reported by MSRT

- Top bots covered by MSRT
- An important weapon in fighting botnet

Month	Alureon	Cutwail	Hamweq	Hupigon	IRCbot	Pushbot	Rbot	Rustock	Slenfbot	Srizbi	Waledac	Bubnix
Sep-09	356,048	121,333		28,373	54,998		29,968	104,812	16,616	2,199	18,057	
Oct-09	290,031	118,234		27,018	42,926		33,441	58,138	25,434	1,403	14,486	
Nov-09	246,401	126,861		22,240	76,984		27,813	37,870	14,913	1,194	13,642	
Dec-09	154,732	133,213	740,962	24,592	57,822		24,580	34,041	11,171	1,131	10,170	
Jan-10	222,187	102,070	500,803	43,170	110,084		24,645	27,548	14,584	1,017	17,678	
Feb-10	198,459	82,295	338,509	43,946	48,978	219,919	15,867	19,611	11,373	820	10,909	
Mar-10	121,085	105,475	282,493	73,454	39,185	119,880	14,939	15,094	12,418	784	16,167	
Apr-10	323,278	101,412	282,045	58,489	32,305	86,831	15,854	12,982	10,025	635	3,603	
May-10	447,436	143,022	234,543	50,438	43,058	78,182	16,366	9,774	12,634	529	3,399	
Jun-10	292,810	102,618	206,217	49,703	31,284	106,359	13,682	8,325	9,559	524	2,123	
Jul-10	493,150	77,734	144,657	72,909	21,088	80,313	9,375	7,260	6,724	327	908	471,243
Aug-10	436,566	71,043	152,220	70,426	27,541	87,259	13,306	6,094	7,940	479	1,252	287,942

Wrap-up

- Full AV for protection
- On-demand cleaning tool to help clean ecosystem
- Quick response with on-demand cleaner, guide users to full AV
- Research on threat events and stay ahead of malware groups

Microsoft®

Your potential. Our passion.™