# The missing link between cybercrime gangs

Yurii Khvyl (ikh@csis.dk)
Senior Malware Analyst at CSIS eCrime and Research & Intelligence Unit

# Agenda - overview

**Episode 1: The quest begins**

- Overview and abstract: Neverquest?
- Code and protocol analysis
- Prevalence and geographic spread

**Episode 2: Dead in the waters**

- 3 million credentials in the water from PONY to Neverquest
- What's PONY about? (demo)
- Web injects (search and replace)

**Episode 3: Glimpse at infrastructure**

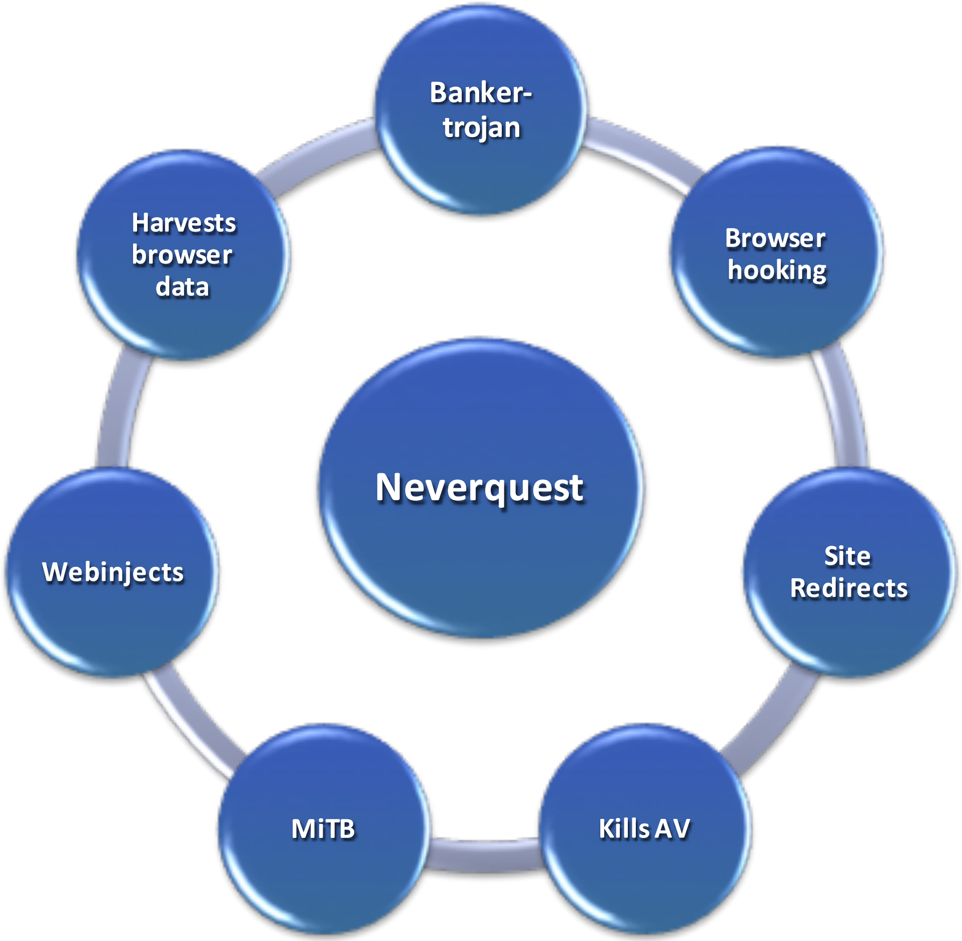
- Server infrastructure
- Panel and money mule accounts, potential loss of millions

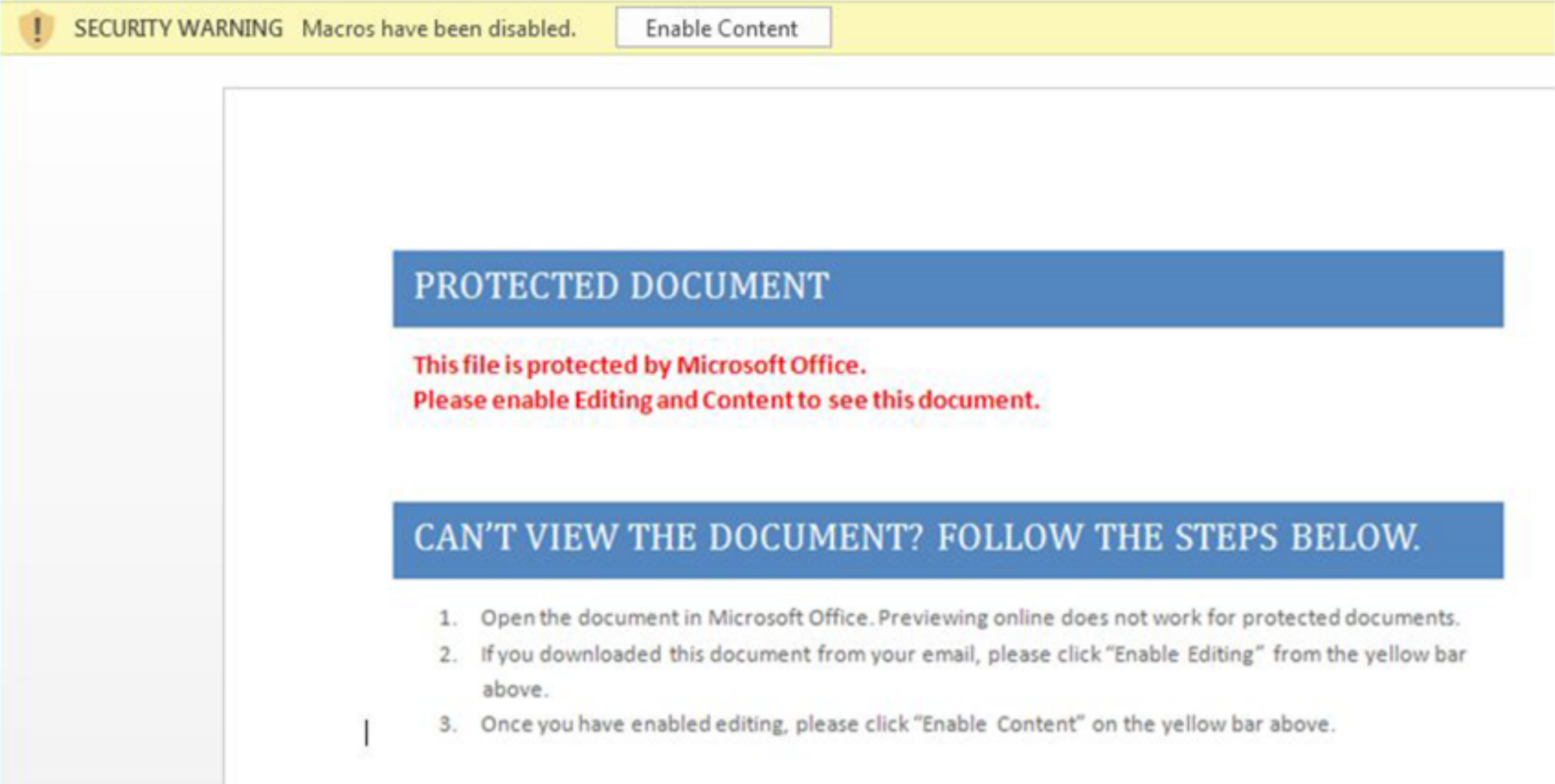
**Episode 4: The Missing Link …**

# Abstract

- Neverquest is also known as Vawtrak/Snifula
- Yet another Crime as a Service
- Ursniff was the foundation which later evolved into Gozi
- Gozi reemerged as "Gozi Prinimalka" (Hang Up)
- Neverquest was born based on that evolution in Trojan banking development
- It was first discovered in mid 2013
- In December 2014 we found Neverquest to implement Tor2web to hide C&C

# Overview: Neverquest





PROTECTED DOCUMENT

This file is protected by Microsoft Office.
Please enable Editing and Content to see this document.

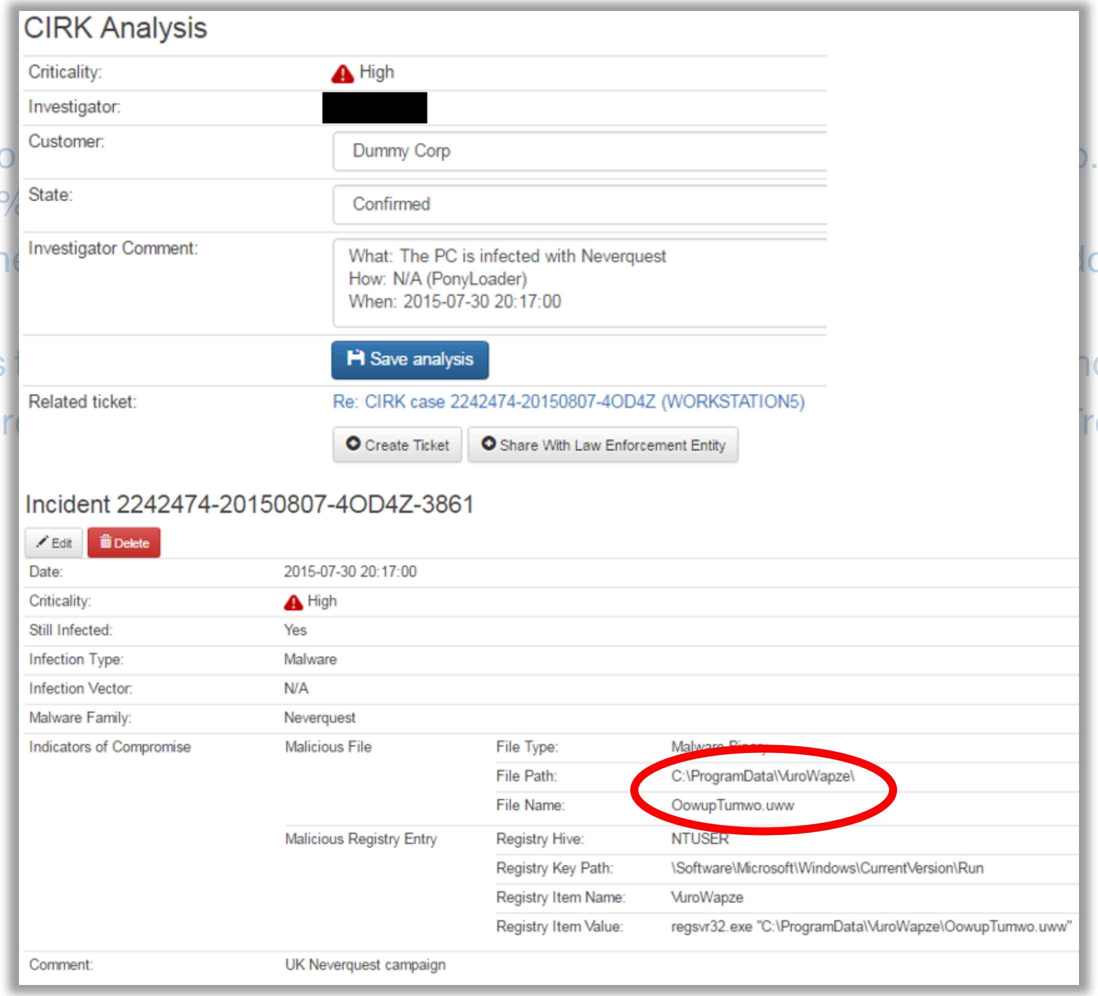
CAN'T VIEW THE DOCUMENT? FOLLOW THE STEPS BELOW.

1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document from your email, please click "Enable Editing" from the yellow bar above.
3. Once you have enabled editing, please click "Enable Content" on the yellow bar above.

d

# Abstract

- Upon executio .uww into %ProgramData%
- Neverquest the ding a run key to registry
- Next it enrolls t coded cookie value
- Neverquest pr rojan bankers.



## CIRK Analysis

| | |
|---|---|
| Criticality: | ▲ High |
| Investigator: | [redacted] |
| Customer: | Dummy Corp |
| State: | Confirmed |
| Investigator Comment: | What: The PC is infected with Neverquest<br>How: N/A (PonyLoader)<br>When: 2015-07-30 20:17:00 |
| | Save analysis |
| Related ticket: | Re: CIRK case 2242474-20150807-4OD4Z (WORKSTATION5) |
| | Create Ticket · Share With Law Enforcement Entity |

## Incident 2242474-20150807-4OD4Z-3861

Edit · Delete

| | | | |
|---|---|---|---|
| Date: | 2015-07-30 20:17:00 | | |
| Criticality: | ▲ High | | |
| Still Infected: | Yes | | |
| Infection Type: | Malware | | |
| Infection Vector: | N/A | | |
| Malware Family: | Neverquest | | |
| Indicators of Compromise | Malicious File | File Type: | Malware Binary |
| | | File Path: | C:\ProgramData\VuroWapze\ |
| | | File Name: | OowupTumwo.uww |
| | Malicious Registry Entry | Registry Hive: | NTUSER |
| | | Registry Key Path: | \Software\Microsoft\Windows\CurrentVersion\Run |
| | | Registry Item Name: | VuroWapze |
| | | Registry Item Value: | regsvr32.exe "C:\ProgramData\VuroWapze\OowupTumwo.uww" |
| Comment: | UK Neverquest campaign | | |

# Abstract

- Some weeks back (mid February 2016) it added several new targets related to banks in Israel: bankleumi.co.il, bankhapoalim.co.il, telebank.co.il.
- Several Neverquest campaigns have recently pushed the Point of Sale (PoS) malware “Abaddon” (small binary approx. 5-6KB)
- Latest new project/campaignID is Project 238
- Yet again we see new targets, including investment retirement services such as Vanguard and Paychex.
- **Infected users should fear for their entire retirement savings being stolen**.

# Binary

Current versions of Neverquest uses several layers to protect itself from detection and to trouble analysis e.g.:

- Anti-Emulator
- Anti-Debugger
- Anti-Analysis
- Anti-Antimalware
- Garbage Collection
- Hashing
- Encryption/Decryption
- Code injection
- Compression/Decompression

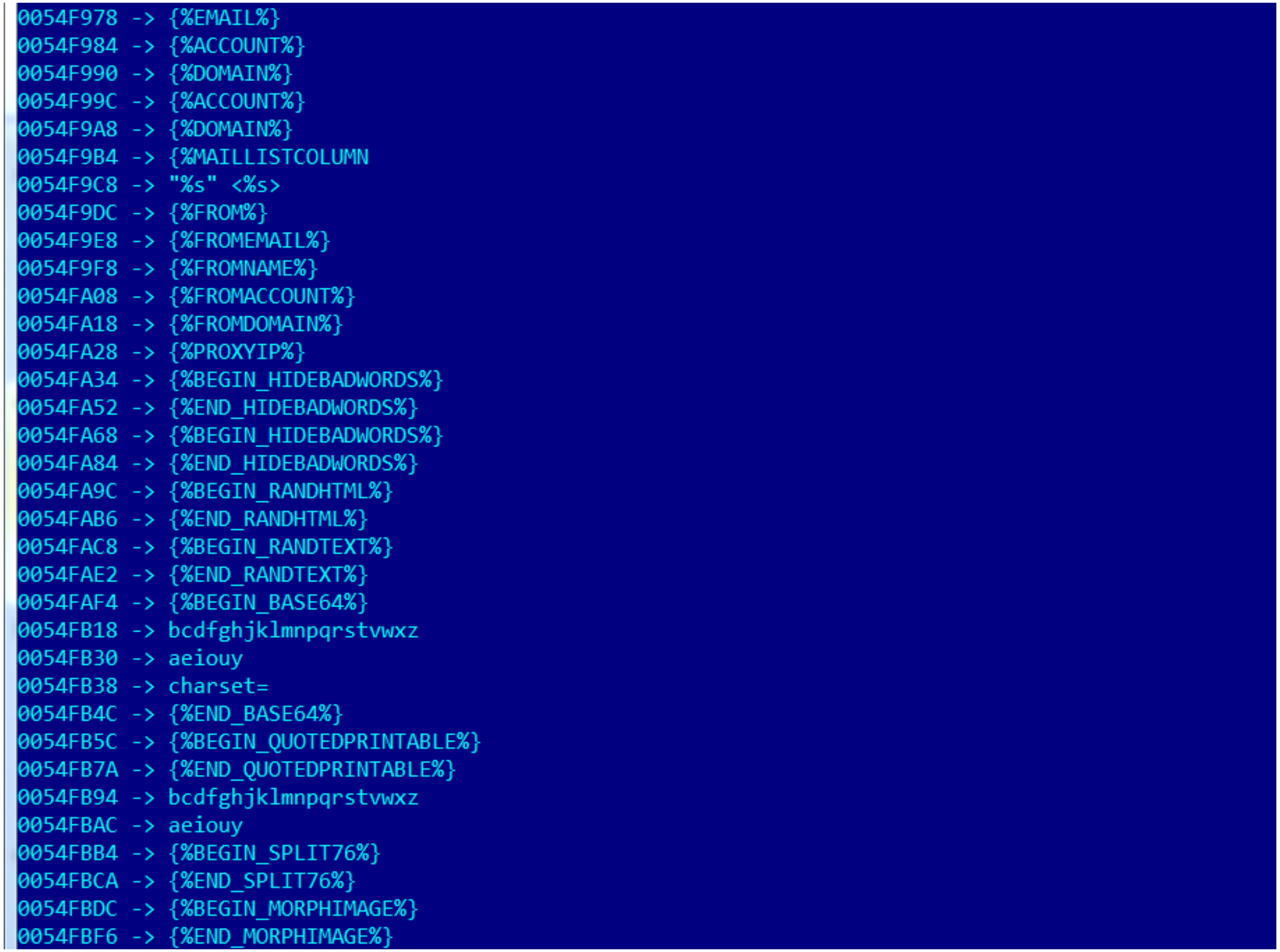
# Protocol

- The C&C responds with a list of items. After the first HTTP request from the infected client the server will typically respond with a configuration file and may also respond with a list of commands that the client will then execute.

| Offset | Value |
|---|---|
| x00\x10 | OK Download + Execute |
| x03 | Download Module |
| x1C | Update |
| X05 | Search files |

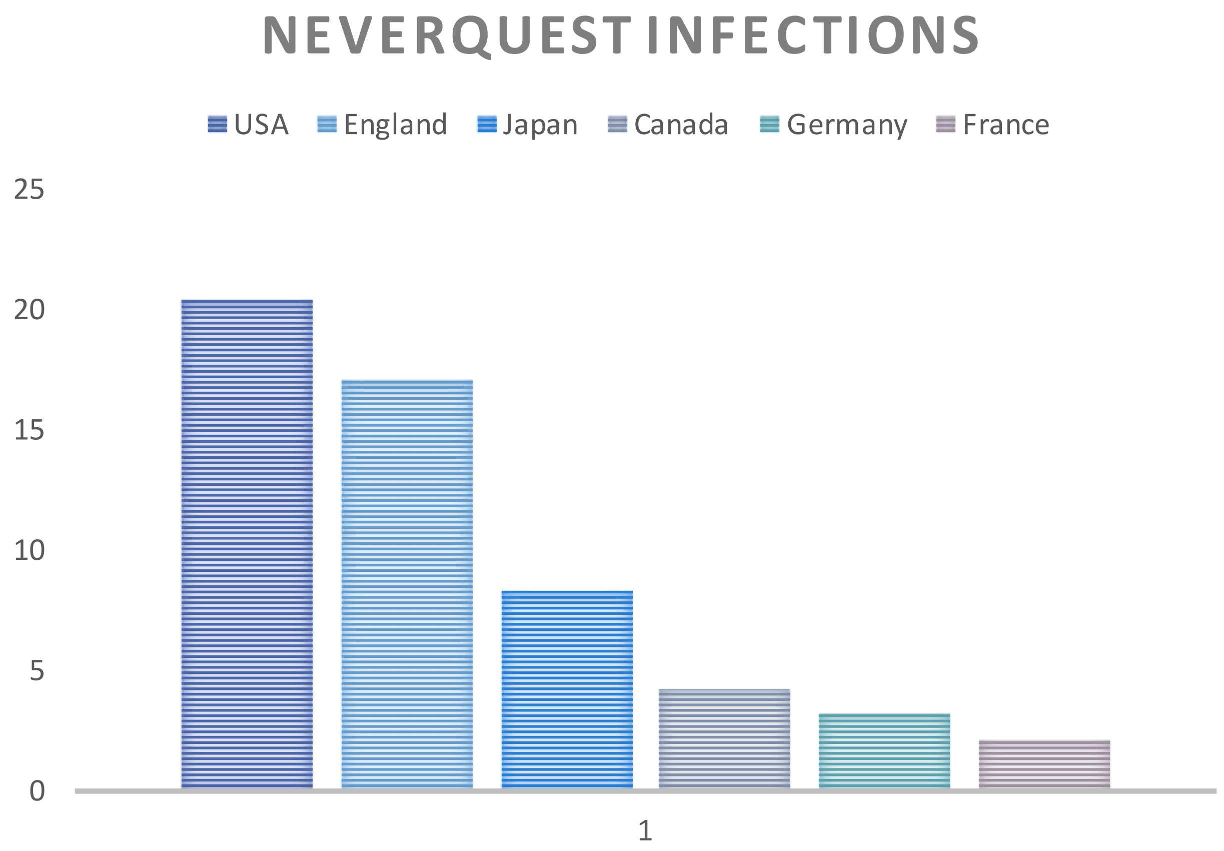
- For some time Neverquest makes use of a linear congruential generator (LCG) method added a pseudo random number generator (PRNG) to produce the key used to encrypt the data.
- On top of that data, it’s now being compressed with LZMAT library.

# *Neverquest – the missing link*

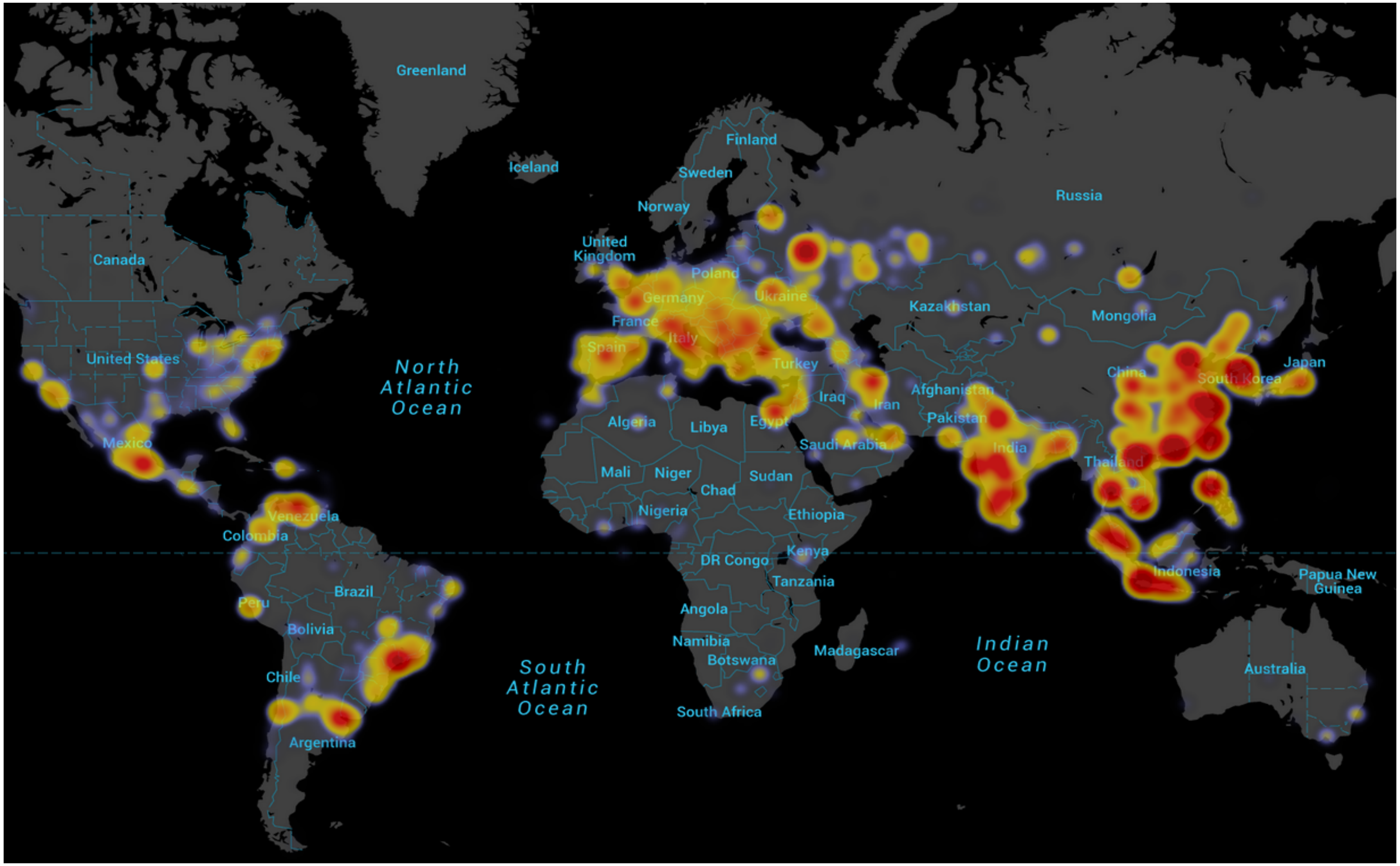


```
0054F978 -> {%EMAIL%}
0054F984 -> {%ACCOUNT%}
0054F990 -> {%DOMAIN%}
0054F99C -> {%ACCOUNT%}
0054F9A8 -> {%DOMAIN%}
0054F9B4 -> {%MAILLISTCOLUMN
0054F9C8 -> "%s" <%s>
0054F9DC -> {%FROM%}
0054F9E8 -> {%FROMEMAIL%}
0054F9F8 -> {%FROMNAME%}
0054FA08 -> {%FROMACCOUNT%}
0054FA18 -> {%FROMDOMAIN%}
0054FA28 -> {%PROXYIP%}
0054FA34 -> {%BEGIN_HIDEBADWORDS%}
0054FA52 -> {%END_HIDEBADWORDS%}
0054FA68 -> {%BEGIN_HIDEBADWORDS%}
0054FA84 -> {%END_HIDEBADWORDS%}
0054FA9C -> {%BEGIN_RANDHTML%}
0054FAB6 -> {%END_RANDHTML%}
0054FAC8 -> {%BEGIN_RANDTEXT%}
0054FAE2 -> {%END_RANDTEXT%}
0054FAF4 -> {%BEGIN_BASE64%}
0054FB18 -> bcdfghjklmnpqrstvwxz
0054FB30 -> aeiouy
0054FB38 -> charset=
0054FB4C -> {%END_BASE64%}
0054FB5C -> {%BEGIN_QUOTEDPRINTABLE%}
0054FB7A -> {%END_QUOTEDPRINTABLE%}
0054FB94 -> bcdfghjklmnpqrstvwxz
0054FBAC -> aeiouy
0054FBB4 -> {%BEGIN_SPLIT76%}
0054FBCA -> {%END_SPLIT76%}
0054FBDC -> {%BEGIN_MORPHIMAGE%}
0054FBF6 -> {%END_MORPHIMAGE%}
```

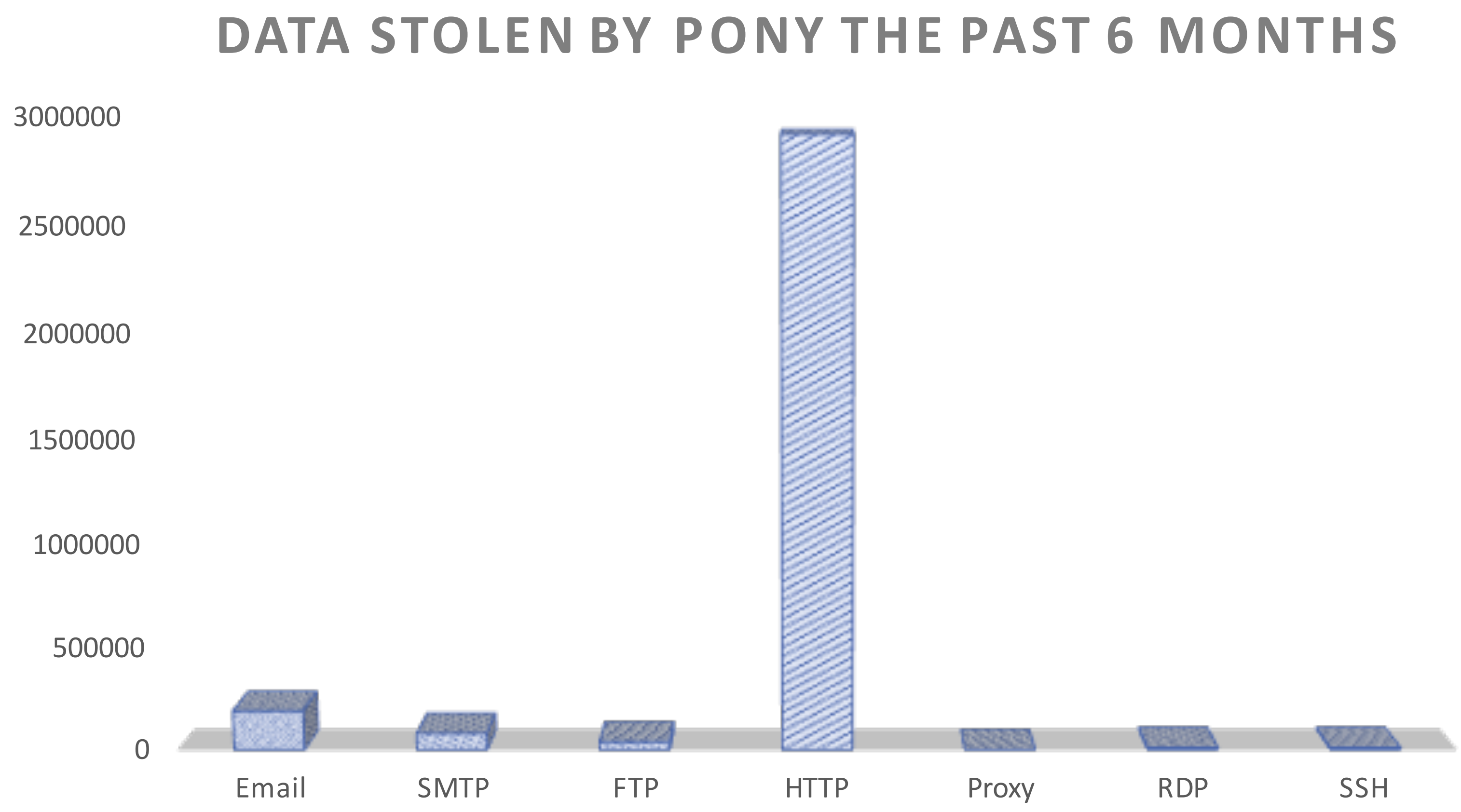
# Distribution and prevalence – all campaigns (1 month)



# Distribution and prevalence – all campaigns (1 year)

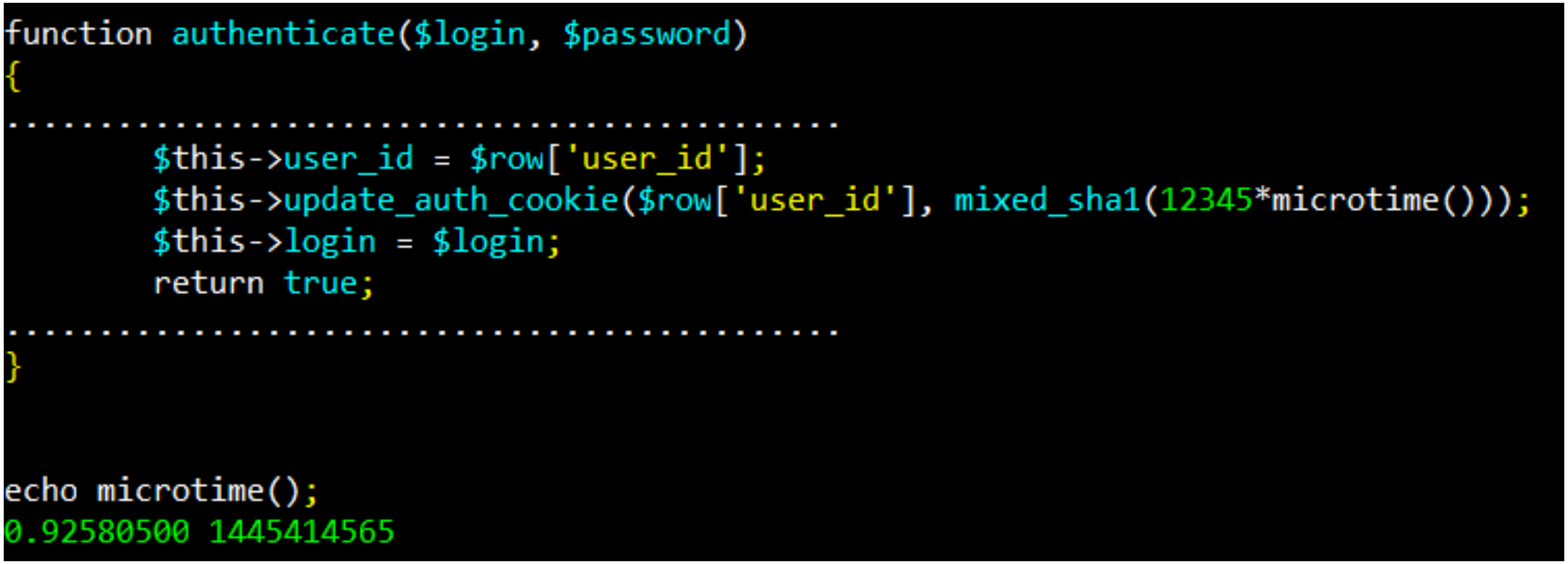


# Credentials lost PONY



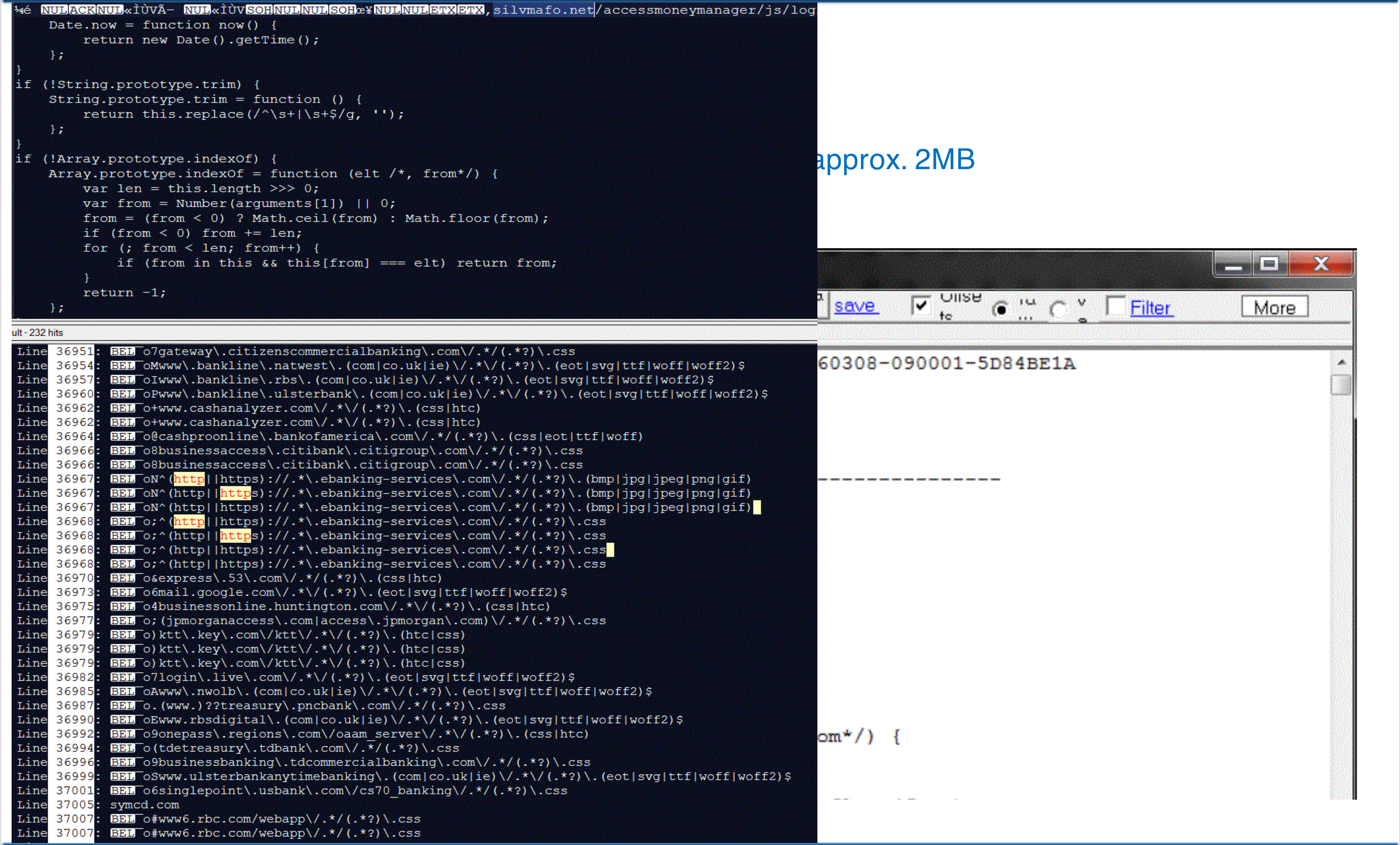
# Neverquest – the missing link

- Requirements should be authenticated for the user to be logged in the system
- Bug in auth_cookie generation



```
function authenticate($login, $password)
{
.............................................
        $this->user_id = $row['user_id'];
        $this->update_auth_cookie($row['user_id'], mixed_sha1(12345*microtime()));
        $this->login = $login;
        return true;
.............................................
}


echo microtime();
0.92580500 1445414565
```

# Neverquest – the missing link



```
¼é NULACKNUL«ÌÙVÃ- NUL«ÌÙVSOHNULNULSOHœ¥NULNULETXETX,silvmafo.net/accessmoneymanager/js/log
    Date.now = function now() {
        return new Date().getTime();
    };
}
if (!String.prototype.trim) {
    String.prototype.trim = function () {
        return this.replace(/^\s+|\s+$/g, '');
    };
}
if (!Array.prototype.indexOf) {
    Array.prototype.indexOf = function (elt /*, from*/) {
        var len = this.length >>> 0;
        var from = Number(arguments[1]) || 0;
        from = (from < 0) ? Math.ceil(from) : Math.floor(from);
        if (from < 0) from += len;
        for (; from < len; from++) {
            if (from in this && this[from] === elt) return from;
        }
        return -1;
    };
```

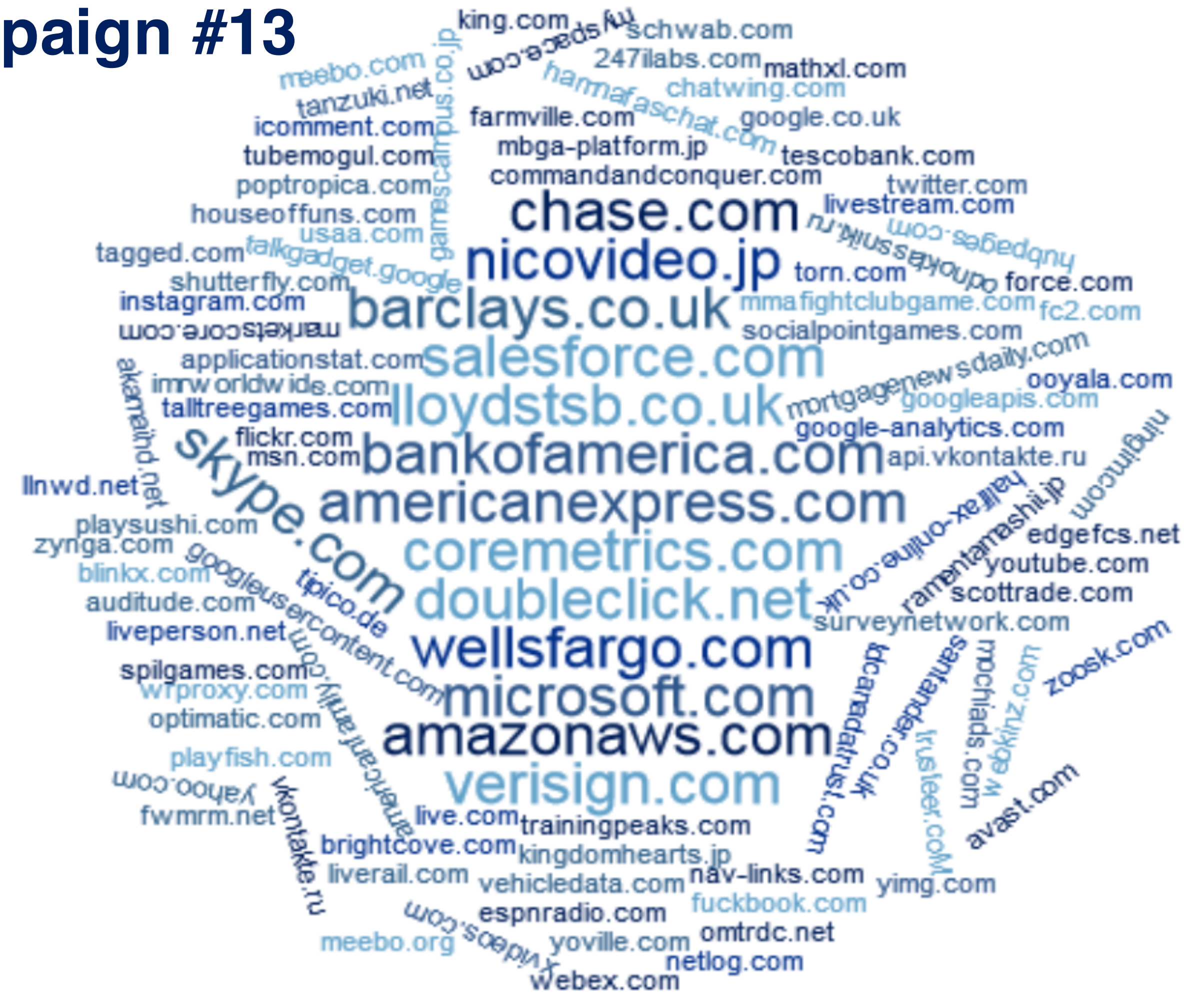
ult - 232 hits

```
Line 36951: BEL o7gateway\.citizenscommercialbanking\.com\/.*/(.*?)\.css
Line 36954: BEL oMwww\.bankline\.natwest\.(com|co.uk|ie)\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36957: BEL oIwww\.bankline\.rbs\.(com|co.uk|ie)\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36960: BEL oPwww\.bankline\.ulsterbank\.(com|co.uk|ie)\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36962: BEL o+www.cashanalyzer.com\/.*\/(.*?)\.(css|htc)
Line 36962: BEL o+www.cashanalyzer.com\/.*\/(.*?)\.(css|htc)
Line 36964: BEL o@cashproonline\.bankofamerica\.com\/.*/(.*?)\.(css|eot|ttf|woff)
Line 36966: BEL o8businessaccess\.citibank\.citigroup\.com\/.*/(.*?)\.css
Line 36966: BEL o8businessaccess\.citibank\.citigroup\.com\/.*/(.*?)\.css
Line 36967: BEL oN^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.(bmp|jpg|jpeg|png|gif)
Line 36967: BEL oN^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.(bmp|jpg|jpeg|png|gif)
Line 36967: BEL oN^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.(bmp|jpg|jpeg|png|gif)
Line 36968: BEL o;^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.css
Line 36968: BEL o;^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.css
Line 36968: BEL o;^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.css
Line 36968: BEL o;^(http||https)://.*\.ebanking-services\.com\/.*/(.*?)\.css
Line 36970: BEL o&express\.53\.com\/.*/(.*?)\.(css|htc)
Line 36973: BEL o6mail.google.com\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36975: BEL o4businessonline.huntington.com\/.*\/(.*?)\.(css|htc)
Line 36977: BEL o;(jpmorganaccess\.com|access\.jpmorgan\.com)\/.*/(.*?)\.css
Line 36979: BEL o)ktt\.key\.com\/ktt\/.*\/(.*?)\.(htc|css)
Line 36979: BEL o)ktt\.key\.com\/ktt\/.*\/(.*?)\.(htc|css)
Line 36979: BEL o)ktt\.key\.com\/ktt\/.*\/(.*?)\.(htc|css)
Line 36982: BEL o7login\.live\.com\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36985: BEL oAwww\.nwolb\.(com|co.uk|ie)\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36987: BEL o.(www.)??treasury\.pncbank\.com\/.*/(.*?)\.css
Line 36990: BEL oEwww.rbsdigital\.(com|co.uk|ie)\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 36992: BEL o9onepass\.regions\.com\/oaam_server\/.*\/(.*?)\.(css|htc)
Line 36994: BEL o(tdetreasury\.tdbank\.com\/.*/(.*?)\.css
Line 36996: BEL o9businessbanking\.tdcommercialbanking\.com\/.*/(.*?)\.css
Line 36999: BEL oSwww.ulsterbankanytimebanking\.(com|co.uk|ie)\/.*\/(.*?)\.(eot|svg|ttf|woff|woff2)$
Line 37001: BEL o6singlepoint\.usbank\.com\/cs70_banking\/.*/(.*?)\.css
Line 37005: symcd.com
Line 37007: BEL o#www6.rbc.com/webapp\/.*/(.*?)\.css
Line 37007: BEL o#www6.rbc.com/webapp\/.*/(.*?)\.css
```

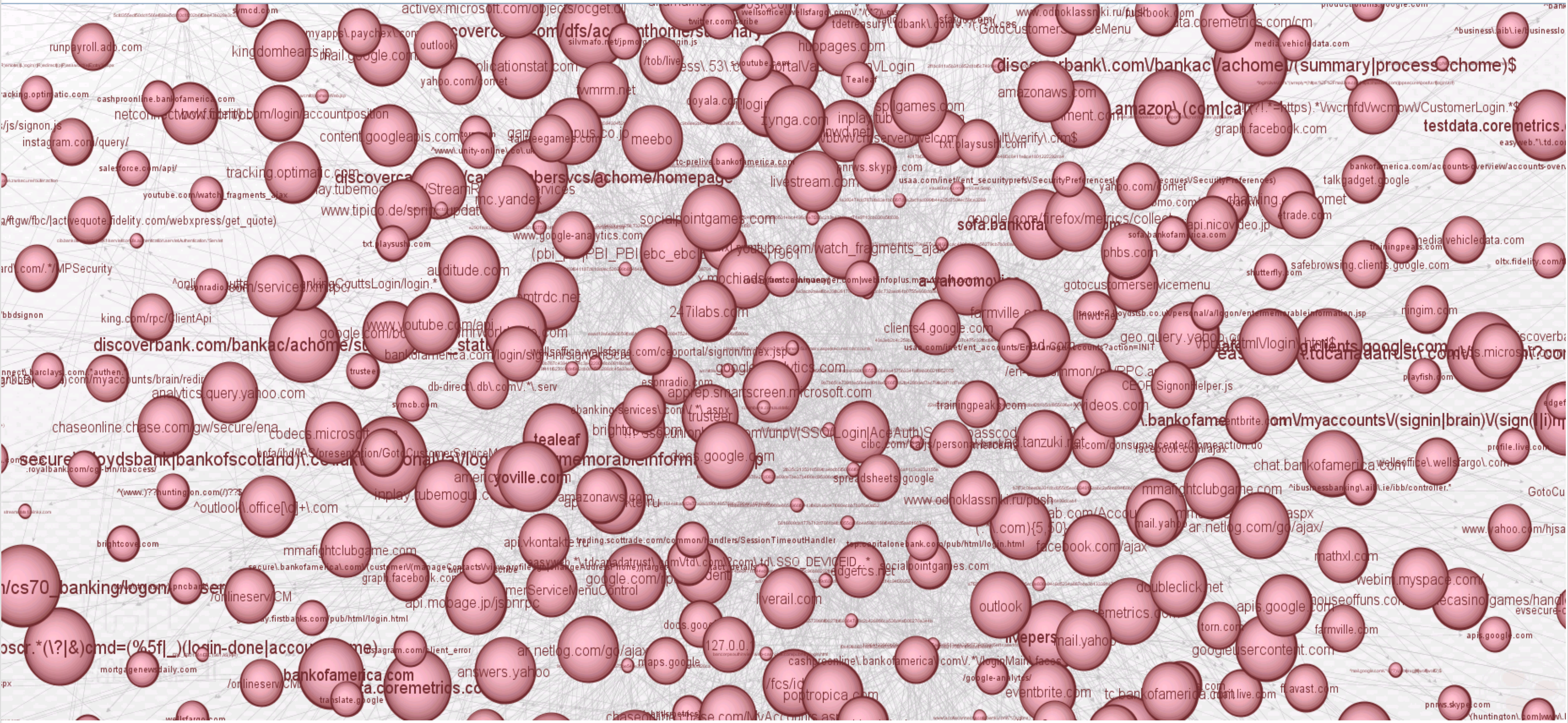
approx. 2MB

```
60308-090001-5D84BE1A
--------------
om*/) {
```

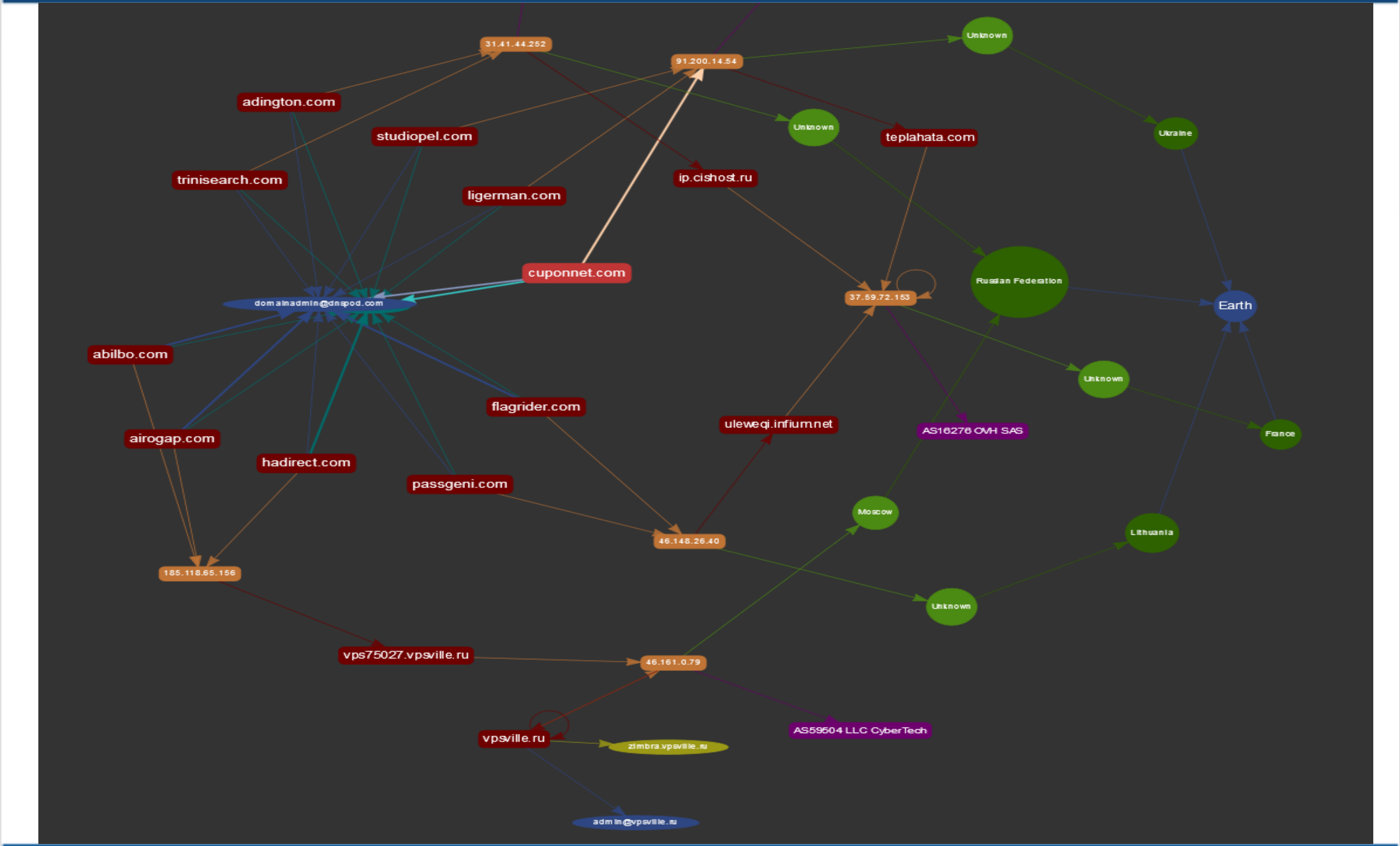
## The targets campaign #13



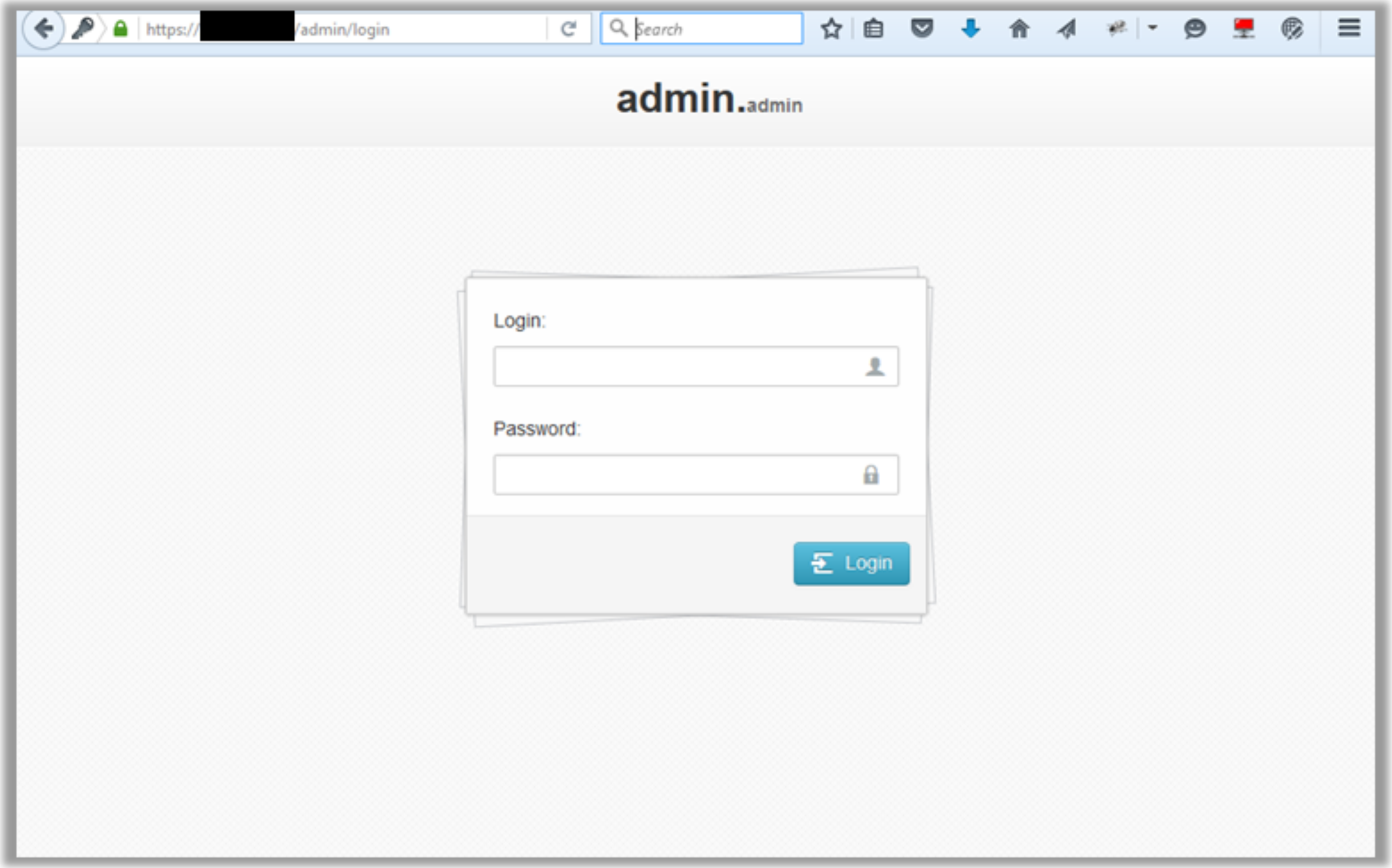
# All unique Neverquest targets =1054 – oh my

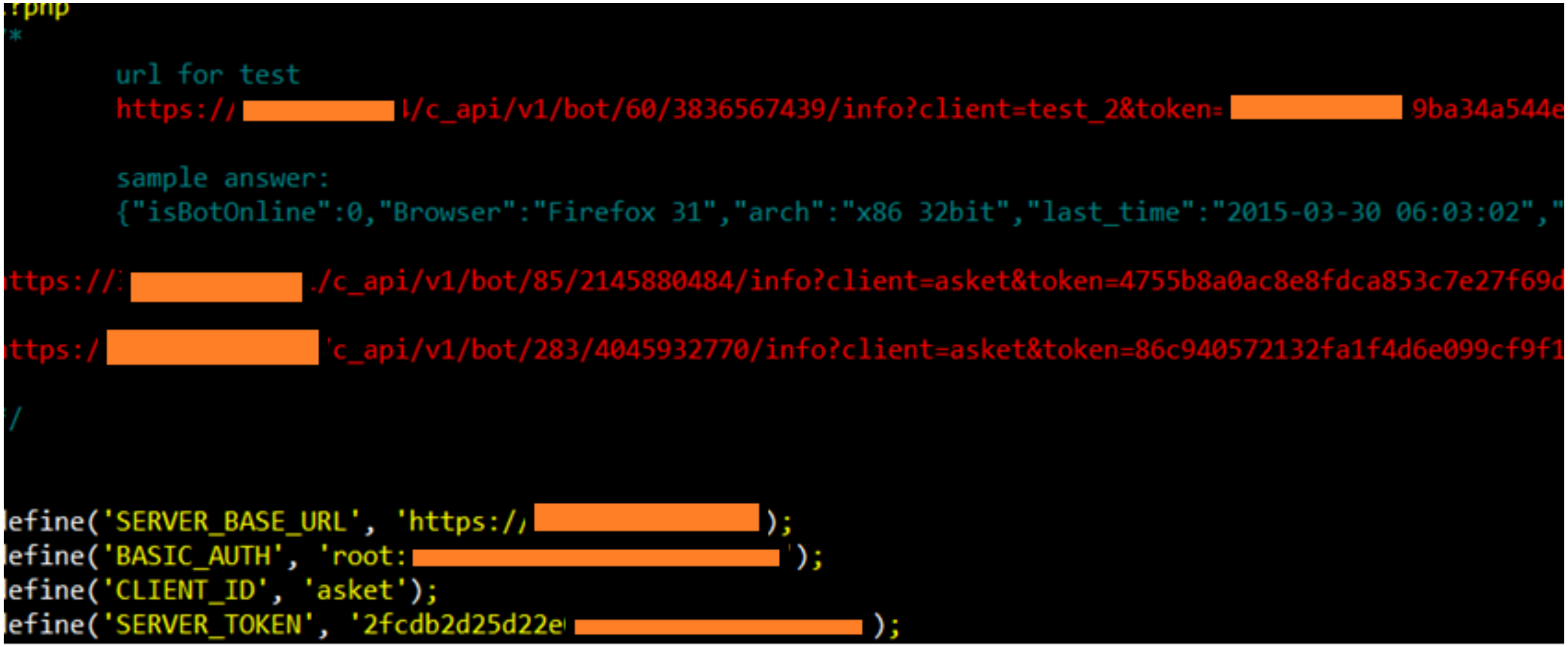


# Neverquest – the missing link



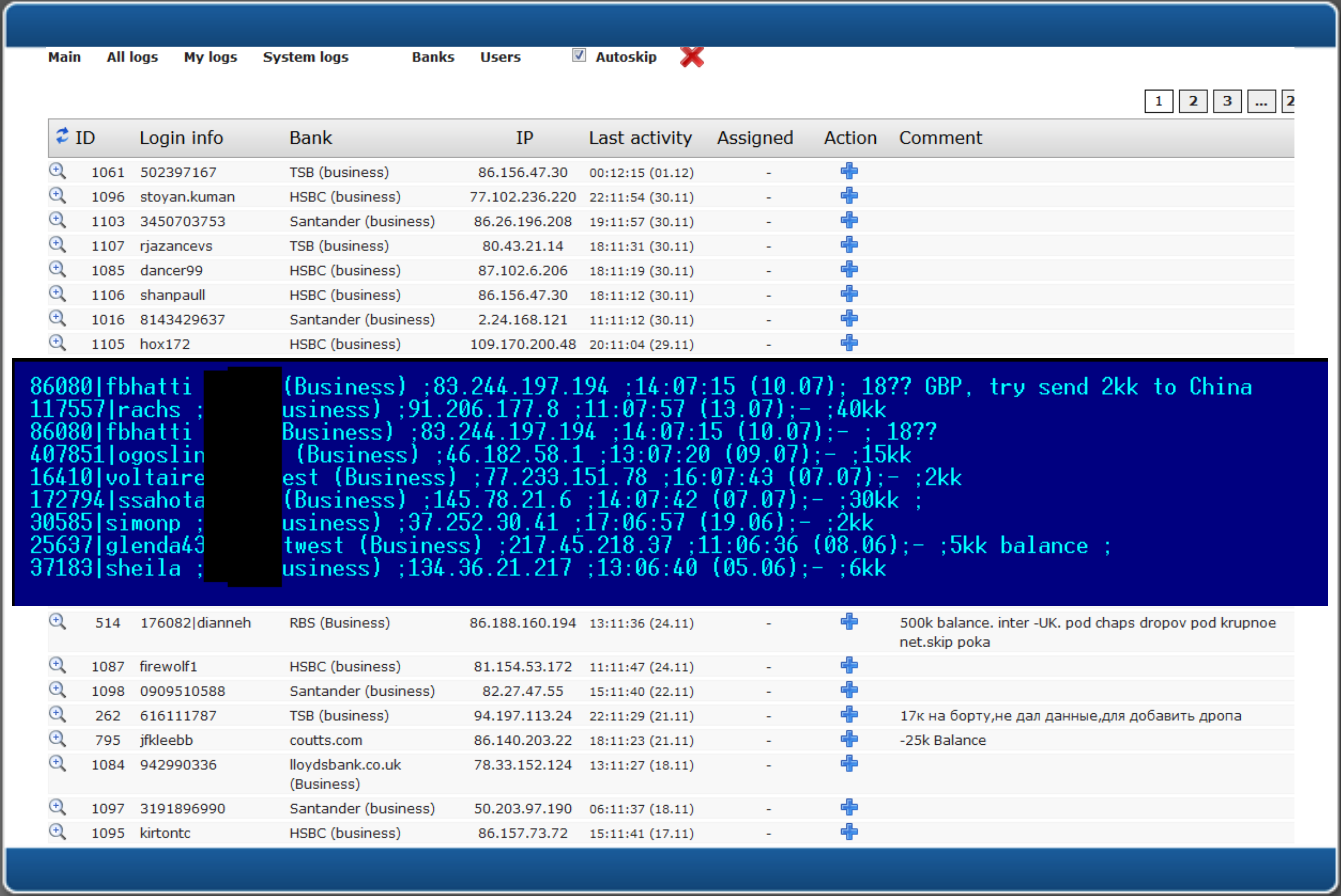
# *Neverquest – the missing link*





```
?php
/*
       url for test
       https://[redacted]/c_api/v1/bot/60/3836567439/info?client=test_2&token=[redacted] 9ba34a544e

       sample answer:
       {"isBotOnline":0,"Browser":"Firefox 31","arch":"x86 32bit","last_time":"2015-03-30 06:03:02","

ttps://[redacted]./c_api/v1/bot/85/2145880484/info?client=asket&token=4755b8a0ac8e8fdca853c7e27f69d

ttps:/[redacted]'c_api/v1/bot/283/4045932770/info?client=asket&token=86c940572132fa1f4d6e099cf9f1

/


efine('SERVER_BASE_URL', 'https:/[redacted]);
efine('BASIC_AUTH', 'root:[redacted]');
efine('CLIENT_ID', 'asket');
efine('SERVER_TOKEN', '2fcdb2d25d22e[redacted]);
```

# Neverquest – the missing link



| | ID | Login info | Bank | IP | Last activity | Assigned | Action | Comment |
|---|---|---|---|---|---|---|---|---|
| 🔍 | 1061 | 502397167 | TSB (business) | 86.156.47.30 | 00:12:15 (01.12) | - | ➕ | |
| 🔍 | 1096 | stoyan.kuman | HSBC (business) | 77.102.236.220 | 22:11:54 (30.11) | - | ➕ | |
| 🔍 | 1103 | 3450703753 | Santander (business) | 86.26.196.208 | 19:11:57 (30.11) | - | ➕ | |
| 🔍 | 1107 | rjazancevs | TSB (business) | 80.43.21.14 | 18:11:31 (30.11) | - | ➕ | |
| 🔍 | 1085 | dancer99 | HSBC (business) | 87.102.6.206 | 18:11:19 (30.11) | - | ➕ | |
| 🔍 | 1106 | shanpaull | HSBC (business) | 86.156.47.30 | 18:11:12 (30.11) | - | ➕ | |
| 🔍 | 1016 | 8143429637 | Santander (business) | 2.24.168.121 | 11:11:12 (30.11) | - | ➕ | |
| 🔍 | 1105 | hox172 | HSBC (business) | 109.170.200.48 | 20:11:04 (29.11) | - | ➕ | |

```
86080|fbhatti [redacted](Business) ;83.244.197.194 ;14:07:15 (10.07); 18?? GBP, try send 2kk to China
117557|rachs ;     usiness) ;91.206.177.8 ;11:07:57 (13.07);- ;40kk
86080|fbhatti      Business) ;83.244.197.194 ;14:07:15 (10.07);- ; 18??
407851|ogoslin      (Business) ;46.182.58.1 ;13:07:20 (09.07);- ;15kk
16410|voltaire     est (Business) ;77.233.151.78 ;16:07:43 (07.07);- ;2kk
172794|ssahota     (Business) ;145.78.21.6 ;14:07:42 (07.07);- ;30kk ;
30585|simonp ;     usiness) ;37.252.30.41 ;17:06:57 (19.06);- ;2kk
25637|glenda43     twest (Business) ;217.45.218.37 ;11:06:36 (08.06);- ;5kk balance ;
37183|sheila ;     usiness) ;134.36.21.217 ;13:06:40 (05.06);- ;6kk
```

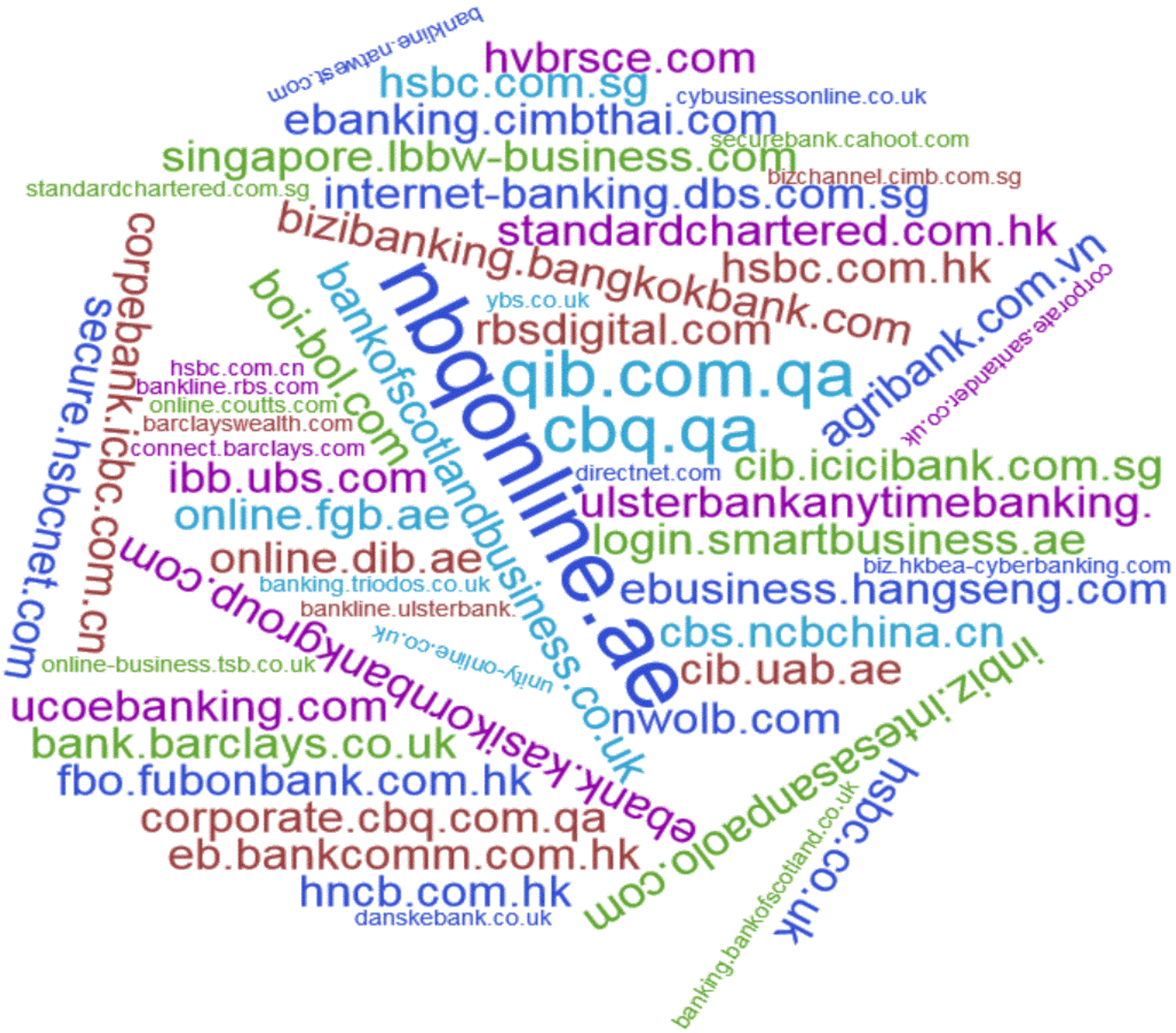
| | ID | Login info | Bank | IP | Last activity | Assigned | Action | Comment |
|---|---|---|---|---|---|---|---|---|
| 🔍 | 514 | 176082\|dianneh | RBS (Business) | 86.188.160.194 | 13:11:36 (24.11) | - | ➕ | 500k balance. inter -UK. pod chaps dropov pod krupnoe net.skip poka |
| 🔍 | 1087 | firewolf1 | HSBC (business) | 81.154.53.172 | 11:11:47 (24.11) | - | ➕ | |
| 🔍 | 1098 | 0909510588 | Santander (business) | 82.27.47.55 | 15:11:40 (22.11) | - | ➕ | |
| 🔍 | 262 | 616111787 | TSB (business) | 94.197.113.24 | 22:11:29 (21.11) | - | ➕ | 17к на борту,не дал данные,для добавить дропа |
| 🔍 | 795 | jfkleebb | coutts.com | 86.140.203.22 | 18:11:23 (21.11) | - | ➕ | -25k Balance |
| 🔍 | 1084 | 942990336 | lloydsbank.co.uk (Business) | 78.33.152.124 | 13:11:27 (18.11) | - | ➕ | |
| 🔍 | 1097 | 3191896990 | Santander (business) | 50.203.97.190 | 06:11:37 (18.11) | - | ➕ | |
| 🔍 | 1095 | kirtontc | HSBC (business) | 86.157.73.72 | 15:11:41 (17.11) | - | ➕ | |

# The Missing Link (Gootkit, Tinba and Neverquest)

- At least two campaigns related to Neverquest shares infrastructure with Shifu, Tinba and Gootkit
- In those two campaigns we have a 100% identical list of corporate banking targets with primary focus on the UK but also on Qatar, Hong Kong, and United Arab Emirates

| | Tinba | Gootkit | Neverquest |
|---|---|---|---|
| Hash | 4d1ad74191725927d76b44b0388b6de6 | 4d86ae4acf5bec6939e6270bfc9216e8 | 67EED9D7AAB4C7E32343CE8CD1EF0F54 |
| Domain | https://sslanalitics.com/ful/ | https://sslanalitics.com/ful/ | https://sslanalitics.com/tyt/ |
| Corporate targets | 100% | 100% | 100% |
| All targets | 52,20% | 41,90% | 100% |

# *Neverquest – the missing link*


bankline-natwest.com
hvbrsce.com
hsbc.com.sg
cybusinessonline.co.uk
ebanking.cimbthai.com
securebank.cahoot.com
singapore.lbbw-business.com
standardchartered.com.sg
bizchannel.cimb.com.sg
internet-banking.dbs.com.sg
bizibanking.bangkokbank.com
standardchartered.com.hk
hsbc.com.hk
agribank.com.vn
corporate.santander.co.uk
corpebank.icbc.com.cn
secure.hsbcnet.com
boi-bol.com
bankofscotlandbusiness.co.uk
nbqonline.ae
ybs.co.uk
rbsdigital.com
qib.com.qa
hsbc.com.cn
bankline.rbs.com
online.coutts.com
barclayswealth.com
connect.barclays.com
cbq.qa
directnet.com
cib.icicibank.com.sg
ibb.ubs.com
ulsterbankanytimebanking.
online.fgb.ae
login.smartbusiness.ae
online.dib.ae
biz.hkbea-cyberbanking.com
banking.triodos.co.uk
ebusiness.hangseng.com
bankline.ulsterbank.
ebank.kasikornbank.com
unify-online.co.uk
cbs.ncbchina.cn
online-business.tsb.co.uk
cib.uab.ae
inbiz.intesasanpaolo.com
ucoebanking.com
nwolb.com
bank.barclays.co.uk
fbo.fubonbank.com.hk
hsbc.co.uk
corporate.cbq.com.qa
eb.bankcomm.com.hk
hncb.com.hk
danskebank.co.uk
banking.bankofscotland.co.uk