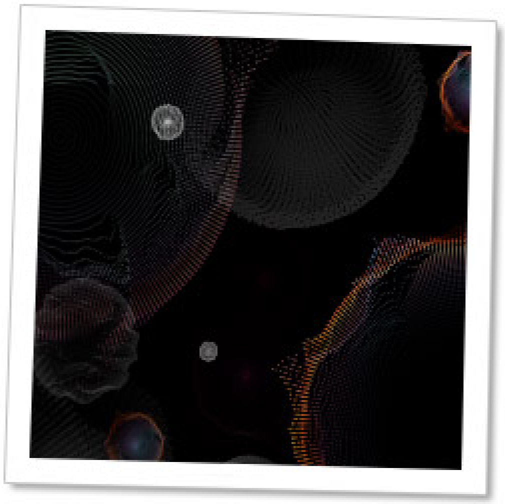
FIREBALL – The Chinese Malware of 250 Million Computers Infected

blog.checkpoint.com/2017/06/01/fireball-chinese-malware-250-million-infection/

June 1, 2017



Check Point Threat Intelligence and research teams recently discovered a high volume Chinese threat operation which has infected over 250 million computers worldwide. The installed malware, Fireball, takes over target browsers and turns them into zombies. Fireball has two main functionalities: the ability of running any code on victim computers– downloading any file or malware, and hijacking and manipulating infected users' web-traffic to generate ad-revenue. Currently, Fireball installs plug-ins and additional configurations to boost its advertisements, but just as easily it can turn into a prominent distributor for any additional malware.

This operation is run by Rafotech, a large digital marketing agency based in Beijing. Rafotech uses Fireball to manipulate the victims' browsers and turn their default search engines and home-pages into fake search engines. This redirects the queries to either yahoo.com or Google.com. The fake search engines include tracking pixels used to collect the users' private information. Fireball has the ability to spy on victims, perform efficient malware dropping, and execute any malicious code in the infected machines, this creates a massive security flaw in targeted machines and networks.

KEY FINDINGS

- Check Point analysts uncovered a high volume Chinese threat operation which has infected over 250 million computers worldwide, and 20% of corporate networks.

- The malware, called Fireball, acts as a browser-hijacker but and can be turned into a full-functioning malware downloader. Fireball is capable of executing any code on the victim machines, resulting in a wide range of actions from stealing credentials to dropping additional malware.
- Fireball is spread mostly via bundling i.e. installed on victim machines alongside a wanted program, often without the user's consent.
- The operation is run by Chinese digital marketing agency.
- Top infected countries are India (10.1%) and Brazil (9.6%)

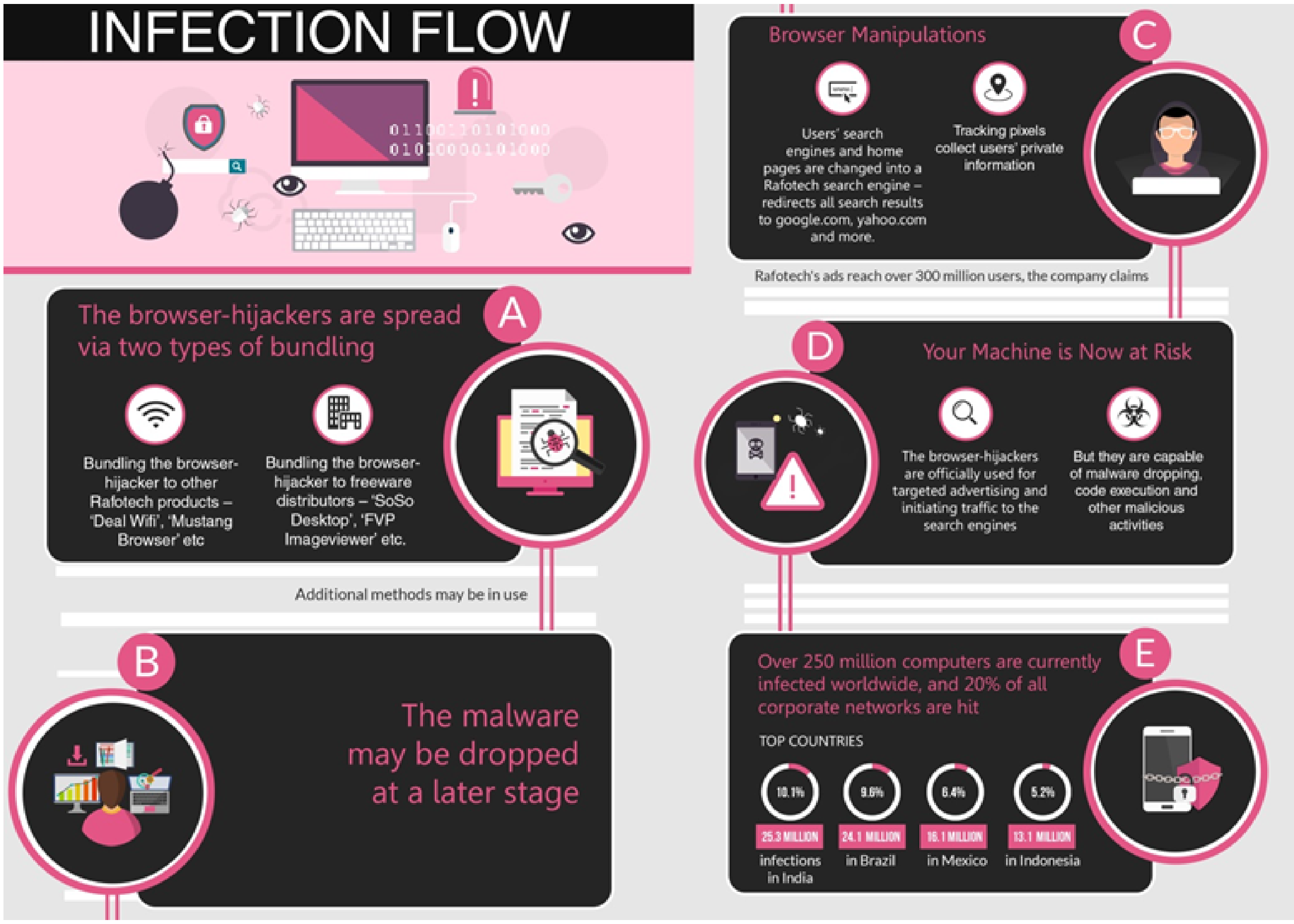

INFECTION FLOW
01100110101000
01010000101000
The browser-hijackers are spread via two types of bundling
A
Bundling the browser-hijacker to other Rafotech products – 'Deal Wifi', 'Mustang Browser' etc
Bundling the browser-hijacker to freeware distributors – 'SoSo Desktop', 'FVP Imageviewer' etc.
Additional methods may be in use
B
The malware may be dropped at a later stage
Browser Manipulations
C
Users' search engines and home pages are changed into a Rafotech search engine – redirects all search results to google.com, yahoo.com and more.
Tracking pixels collect users' private information
Rafotech's ads reach over 300 million users, the company claims
D
Your Machine is Now at Risk
The browser-hijackers are officially used for targeted advertising and initiating traffic to the search engines
But they are capable of malware dropping, code execution and other malicious activities
Over 250 million computers are currently infected worldwide, and 20% of all corporate networks are hit
E
TOP COUNTRIES
10.1%
9.6%
6.4%
5.2%
25.3 MILLION
infections in India
24.1 MILLION
in Brazil
16.1 MILLION
in Mexico
13.1 MILLION
in Indonesia

Figure 1: Fireball Infection Flow

250 MILLIONS MACHINES AND 20% OF CORPORATE NETWORKS WORLDWIDE INFECTED

The scope of the malware distribution is alarming. According to our analysis, over 250 million computers worldwide have been infected: specifically, 25.3 million infections in India (10.1%), 24.1 million in Brazil (9.6%), 16.1 million in Mexico (6.4%), and 13.1 million in Indonesia (5.2%). The United States has witnessed 5.5 million infections (2.2%).

Based on Check Point's global sensors, 20% of all corporate networks are affected . Hit rates in the US (10.7%) and China (4.7%) are alarming;but Indonesia (60%), India (43%) and Brazil (38%) have much more dangerous hit rates.

Another indicator of the incredibly high infection rate is the popularity of Rafotech's fake search engines. According to Alexa's web traffic data, 14 of these fake search engines are among the top 10,000 websites, with some of them occasionally reaching the top 1,000.

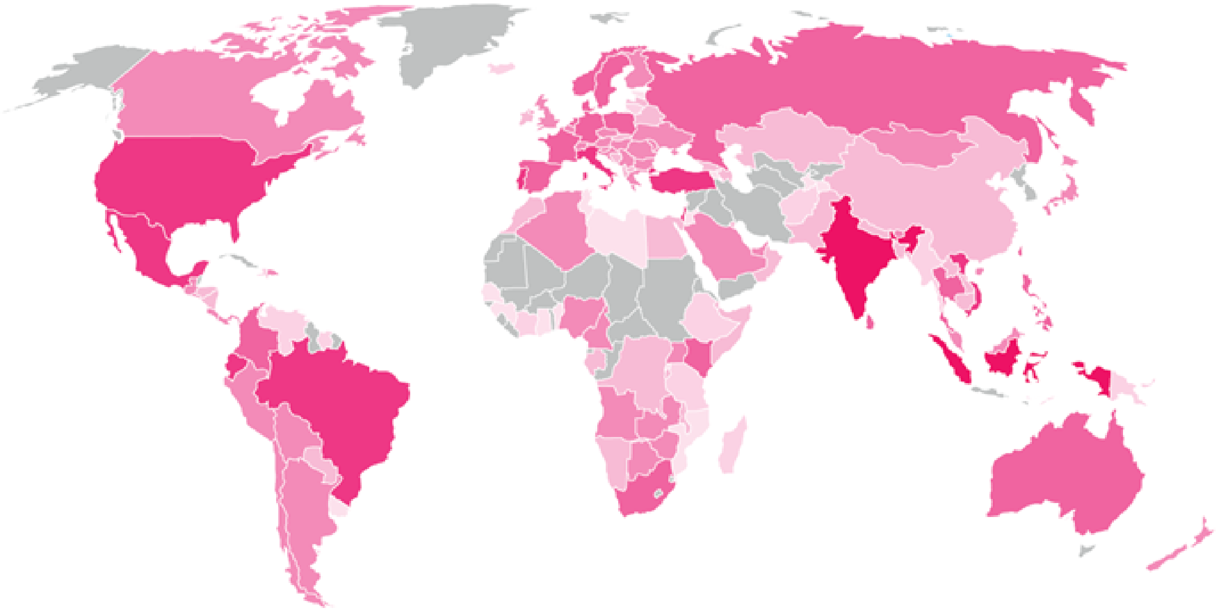


Figure 2: Fireball Global Infection Rates (darker pink = more infections)

Ironically, although Rafotech doesn't admit it produces browser-hijackers and fake search engines, it does (proudly) declare itself a successful marketing agency, reaching 300 million users worldwide – coincidentally similar to our number of estimated infections.

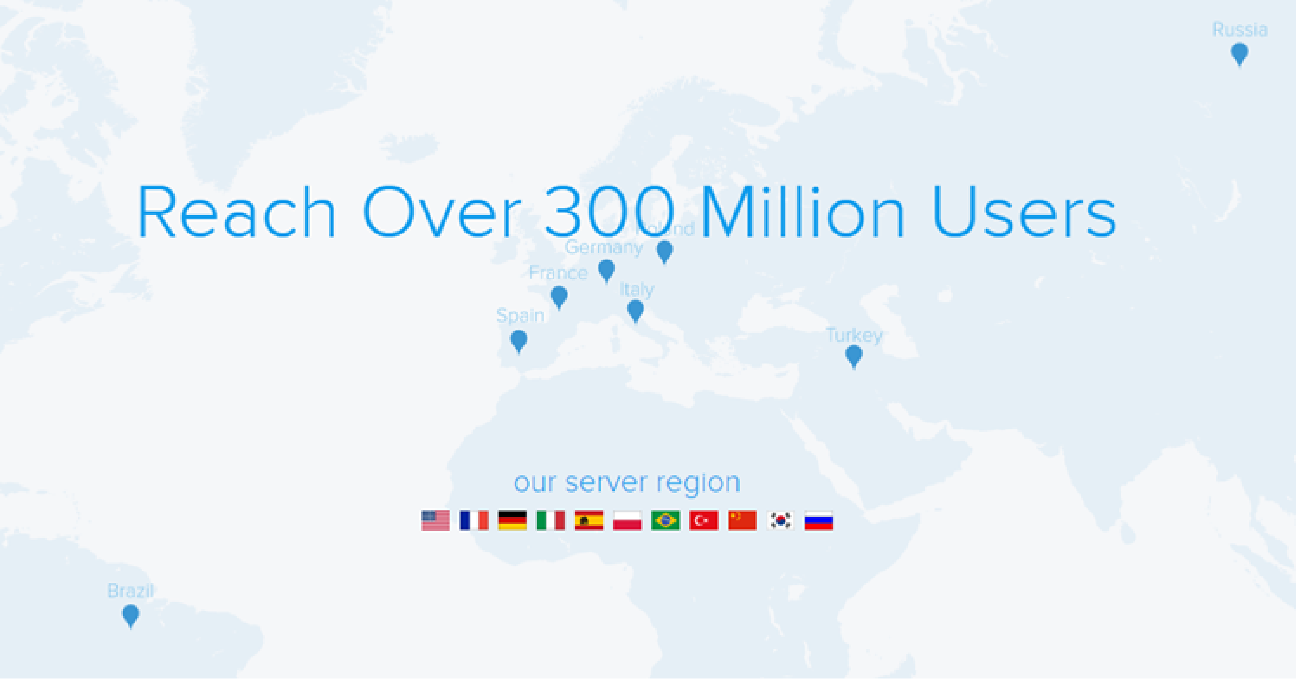


Figure 3: Rafotech's Advertisement on the Company's Official Website

A BACKDOOR TO EVERY INFECTED NETWORK

Fireball and similar browser-hijackers are hybrid creatures, half seemingly legitimate software (see the **GOING UNDER THE RADAR** section), and half malware. Although Rafotech uses Fireball only for advertising and initiating traffic to its fake search engines, it can perform any action on the victims' machines These actions can have serious consequences. How severe is it? Try to imagine a pesticide armed with a nuclear bomb. Yes, it can do the job, but it can also do much more.

These browser-hijackers are capable on the browser level. This means that they can drive victims to malicious sites, spy on them and conduct successful malware dropping.

From a technical perspective, Fireball displays great sophistication and quality evasion techniques, including anti-detection capabilities, multi-layer structure and a flexible C&C– it is not inferior to a typical malware.

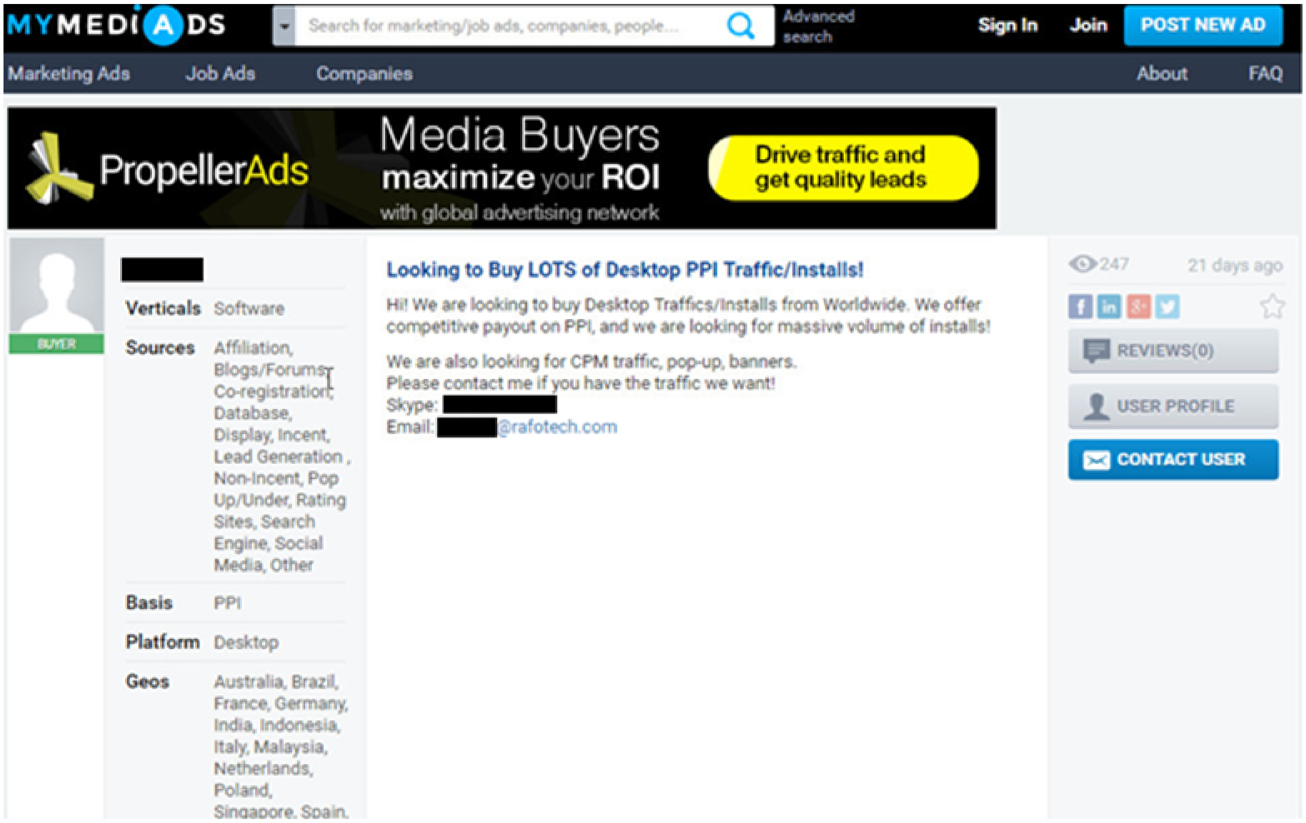
Many threat actors would like to have a fraction of Rafotech's power, as Fireball provides a critical backdoor, which can be further exploited.

GOING UNDER THE RADAR

While the distribution of Fireball is both malicious and illegitimate, it actually carries digital certificates imparting them a legitimate appearance. Confused? You should be.

Rafotech carefully walks along the edge of legitimacy, knowing that adware distribution is not considered a crime like malware distribution is. How is that? Many companies provide software or services for free, and make their profits by harvesting data or presenting advertisements. Once a client agrees to the installment of extra features or software to his/her computer, it is hard to claim malicious intent on behalf of the provider.

This gray zone led to the birth of a new kind of monetizing method – bundling. Bundling is when a wanted program installs another program alongside it, sometimes with a user's authorization and sometimes without. Rafotech uses bundling in high volume to spread Fireball.



[redacted]

Verticals	Software
Sources	Affiliation, Blogs/Forums, Co-registration, Database, Display, Incent, Lead Generation , Non-Incent, Pop Up/Under, Rating Sites, Search Engine, Social Media, Other
Basis	PPI
Platform	Desktop
Geos	Australia, Brazil, France, Germany, India, Indonesia, Italy, Malaysia, Netherlands, Poland, Singapore, Spain,

Looking to Buy LOTS of Desktop PPI Traffic/Installs!

Hi! We are looking to buy Desktop Traffics/Installs from Worldwide. We offer competitive payout on PPI, and we are looking for massive volume of installs!

We are also looking for CPM traffic, pop-up, banners.
Please contact me if you have the traffic we want!
Skype: [redacted]
Email: [redacted]@rafotech.com

Figure 4: Bundling in Action

Figure 4: Bundling in Action

According to our analysis, Rafotech's distribution methods appear to be illegitimate and don't follow the criteria which would allow these actions to be considered naïve or legal. The malware and the fake search engines don't carry indicators connecting them to Rafotech, they cannot be uninstalled by an ordinary user, and they conceal their true nature.

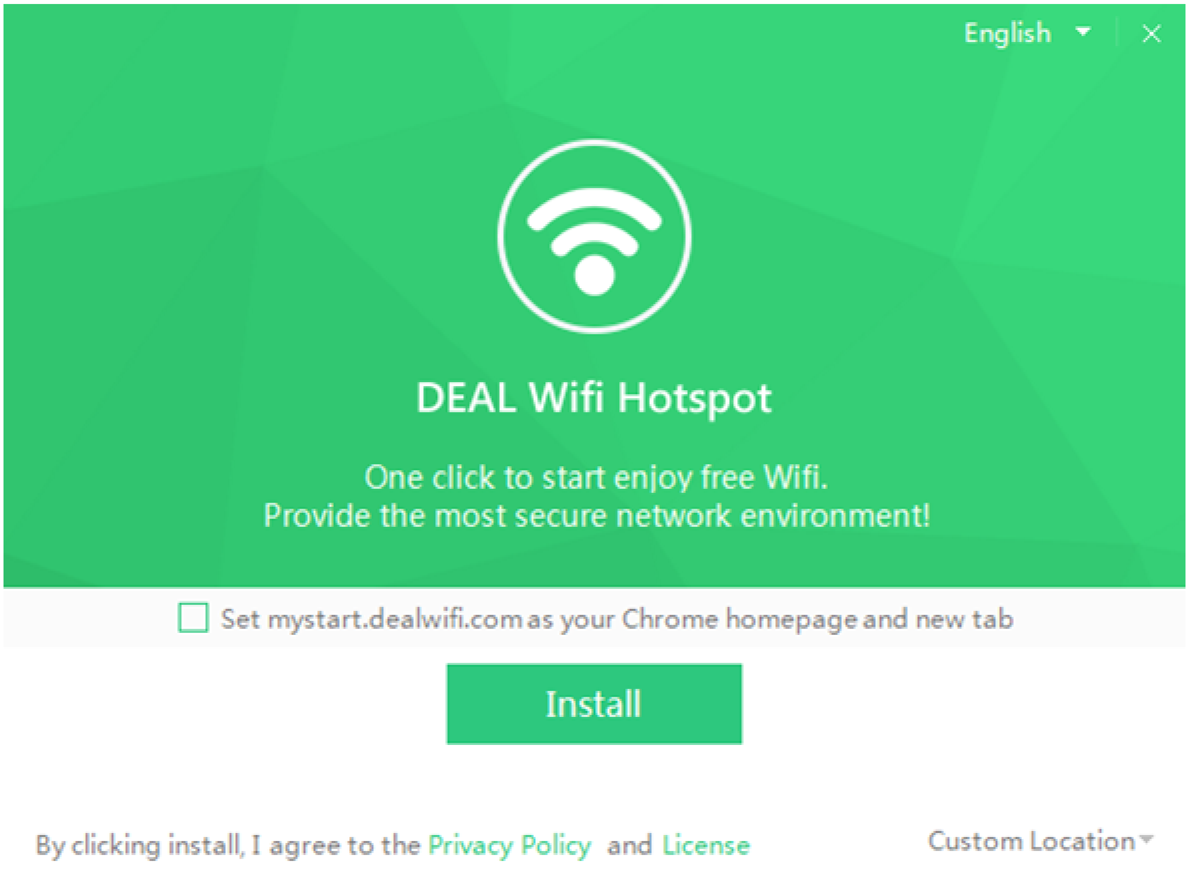
So how do they carry digital certificates? One possibility is that issuers make their living from providing certificates, and small issuers with flexible ethics can enjoy the lack of clarity in the adware world's legality to approve software such as Rafotech's browser-hijackers.
THE INFECTION MODEL

As with other types of malware, there are many ways for Fireball to spread. We suspect that two popular vectors are bundling the malware to other Rafotech products – Deal Wifi and Mustang Browser – as well as bundling via other freeware distributors: products such as “Soso Desktop”, “FVP Imageviewer” and others.

It’s important to remember that when a user installs freeware, additional malware isn’t necessarily dropped at the same time. If you download a suspicious freeware and nothing happens on the spot, it doesn’t necessarily mean that something isn’t happening behind the scenes.

Furthermore, it is likely that Rafotech is using additional distribution methods, such as spreading freeware under fake names, spam, or even buying installs from threat actors.

As with everything in the internet, remember that there are no free lunches. When you download freeware, or use cost-free services (streaming and downloads, for example), the service provider is making profit somehow. If it’s not from you or from advertisements, it will come from somewhere else.



One click to start enjoy free Wifi.
Provide the most secure network environment!

□ Set mystart.dealwifi.com as your Chrome homepage and new tab

By clicking install, I agree to the Privacy Policy and License

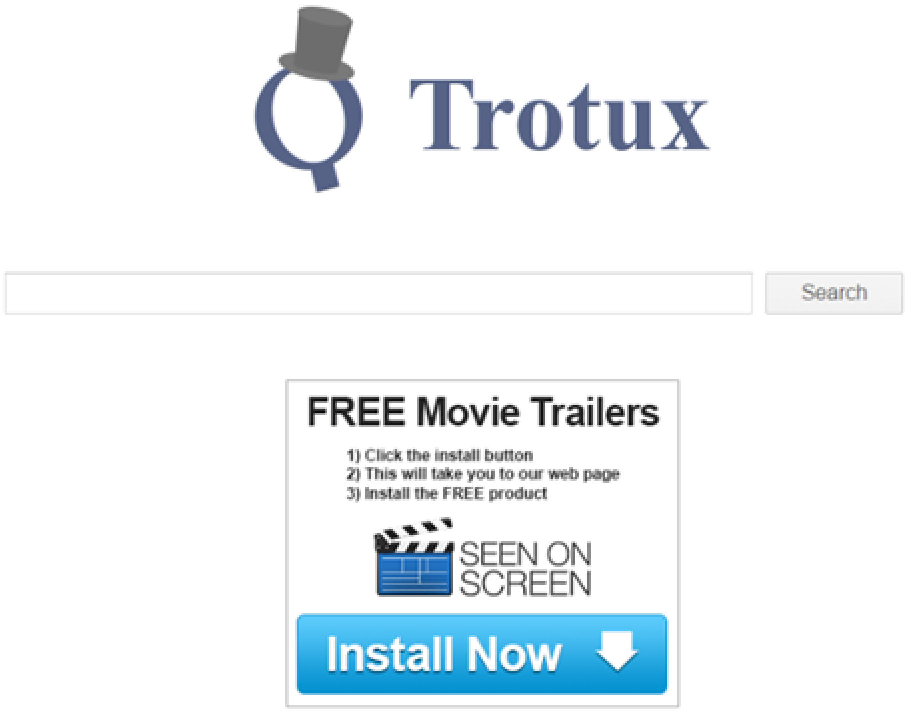
Figure 5: Deal Wifi Installation Screen

Figure 5: Deal Wifi Installation Screen

HOW CAN I KNOW IF I AM INFECTED?

To check if you're infected, first open your web browser. Was your home-page set by you? Are you able to modify it? Are you familiar with your default search engine and can modify that as well? Do you remember installing all of your browser extensions?

If the answer to any of these questions is "NO", this is a sign that you're infected with adware. You can also use a recommended adware scanner, just to be extra cautious.



1) Click the install button
2) This will take you to our web page
3) Install the FREE product

Figure 6: trotux.com; a Fake Search Engine Run by Rafotech

THE RED BUTTON IN THE WRONG HANDS

It doesn't take much to imagine a scenario in which Rafotech decides to harvest sensitive information from all of its infected machines, and sell this data to threat groups or business rivals. Banking and credit card credentials, medical files, patents and business plans can all be widely exposed and abused by threat actors for various purposes. Based on our estimated infection rate, in such a scenario, one out of five corporations worldwide will be susceptible to a major breach. Severe damage can be caused to key organizations, from major service providers to critical infrastructure operators to medical institutions. The potential loss is indescribable, and repairing the damage caused by such massive data leakage (if even possible) could take years.

Rafotech holds the power to initiate a global catastrophe and it is not alone. During our research we've tracked down additional browser-hijackers that, to our understanding, were developed by other companies. One such company is ELEX Technology, an Internet Services company also based in Beijing produces products similar to those of Rafotech.

Several findings lead us to suspect that the two companies are related, and may be collaborating in the distribution of browser-hijackers or in trading customers' traffic. For example, an adware developed by ELEX, named YAC ("Yet Another Cleaner") is suspected to be connected to Rafotech's operation, dropping its browser-hijackers.

CONCLUSION

In this research we've described Rafotech's browser-hijackers operation – possibly the largest infection operation in history. We believe that although this is not a typical malware attack campaign, it has the potential to cause irreversible damage to its victims as well as worldwide internet users, and therefore it must be blocked by security companies.

The full distribution of Fireball is not yet known, but it is clear that it presents a great threat to the global cyber ecosystem. With a quarter billion infected machines and a grip in one of every five corporate networks, Rafotech's activities make it an immense threat.

HOW DO I REMOVE THE MALWARE, ONCE INFECTED?

To remove almost any adware, follow these simple steps:

1. Uninstall the adware by removing the application from the Programs and Features list in the Windows Control Panel.

For Mac OS users:

1. Use the Finder to locate the Applications
2. Drag the suspicious file to the Trash.
3. Empty the Trash.

Note – A usable program is not always installed on the machine and therefore may not be found on the program list.

1. Scan and clean your machine, using:

- Anti-Malware software
- Adware cleaner software

1. Remove malicious Add-ons, extensions or plug-ins from your browser:

On Google Chrome:
a. Click the Chrome menu icon and select Tools > Extensions.

b. Locate and select any suspicious Add-ons.

c. Click the trash can icon to delete.

On Internet Explorer:
a. Click the Setting icon and select Manage Add-ons.

b. Locate and remove any malicious Add-ons.

On Mozilla Firefox:
a. Click the Firefox menu icon and go to the Tools tab.

b. Select Add-ons > Extensions.

A new window opens.

c. Remove any suspicious Add-ons.

d. Go to the Add-ons manager > Plugins.

e. Locate and disable any malicious plugins.

On Safari:
a. Make sure the browser is active.

b. Click the Safari tab and select preferences.

A new window opens.

c. Select the Extensions tab.

d. Locate and uninstall any suspicious extensions.

1. Restore your internet browser to its default settings:

On Google Chrome:
a. Click the Chrome menu icon, and select Settings.

b. In the On startup section, click Set Pages.

c. Delete the malicious pages from the Startup pages list.

d. Find the Show Home button option and select Change.

e. In the Open this page field, delete the malicious search engine page.

f. In the Search section, select Manage search engines.

g. Select the malicious search engine page and remove from the list.

On Internet Explorer:
a. Select the Tools tab and then select Internet Options.

A new window opens.

b. In the Advanced tab, select Reset.

c. Check the Delete personal settings box.

d. Click the Reset button.

On Mozilla Firefox:
a. Enable the browser Menu Bar by clicking the blank space near the page tabs.

b. Click the Help tab, and go to Troubleshooting information.

A new window opens.

c. Select Reset Firefox.

On Safari:
a. Select the Safari tab and then select Preferences.

A new window opens.

b. In the Privacy tab, the Manage Website Data… button.

A new window opens.

c. Click the Remove All button.

INDICATORS OF COMPROMISE

C&C addresses

- attirerpage[.]com
- s2s[.]rafotech[.]com
- trotux[.]com
- startpageing123[.]com
- funcionapage[.]com
- universalsearches[.]com
- thewebanswers[.]com
- nicesearches[.]com
- youndoo[.]com
- giqepofa[.]com
- mustang-browser[.]com

- forestbrowser[.]com
- luckysearch123[.]com
- ooxxsearch[.]com
- search2000s[.]com
- walasearch[.]com
- hohosearch[.]com
- yessearches[.]com
- d3l4qa0kmel7is[.]cloudfront[.]net
- d5ou3dytze6uf[.]cloudfront[.]net
- d1vh0xkmncek4z[.]cloudfront[.]net
- d26r15y2ken1t9[.]cloudfront[.]net
- d11eq81k50lwgi[.]cloudfront[.]net
- ddyv8sl7ewq1w[.]cloudfront[.]net
- d3i1asoswufp5k[.]cloudfront[.]net
- dc44qjwal3p07[.]cloudfront[.]net
- dv2m1uumnsgtu[.]cloudfront[.]net
- d1mxvenloqrqmu[.]cloudfront[.]net
- dfrs12kz9qye2[.]cloudfront[.]net
- dgkytklfjrqkb[.]cloudfront[.]net
- dgkytklfjrqkb[.]cloudfront[.]net/main/trmz[.]exe

File Hashes

- FAB40A7BDE5250A6BC8644F4D6B9C28F
- 69FFDF99149D19BE7DC1C52F33AAA651
- B56D1D35D46630335E03AF9ADD84B488
- 8C61A6937963507DC87D8BF00385C0BC
- 7ADB7F56E81456F3B421C01AB19B1900
- 84DCB96BDD84389D4449F13EAC75098
- 2B307E28CE531157611825EB0854C15F
- 7B2868FAA915A7FC6E2D7CC5A965B1E