INNOVATIVE SOLUTIONS
Your Business. Secured!

"Fireball" Malware attacks over **250 million** computers worldwide. **Discover how IS can keep you secured!**

EXECUTIVE SUMMARY

Effects of **WannaCry** ransomware haven't been completely faded away and security researchers have already discovered another emerging malware that has impacted over 250 million personal computers. This is a Chinese adware named as **"Fireball"**.

This software is mainly intended to take over the user's web browser and generate fake clicks and traffic to ultimately generate ad revenue to a Chinese marketing firm called Rafotech.

The Fireball malware is capable of carrying out a wide range of actions on the victim devices:

- Fireball can gain control of the browser of any infected computer.
- It has malware-downloading capability that executes any code on the user machines.
- It influences the traffic with internet of affected PC to boost the ad-revenue.
- It is capable of installing plugins and changing configurations.
- It violates user privacy by spying on them.

When installed in the infected PC:

- It takes control of the default search engine and replaces it with a fake one.
- It provides the attacker with the ability to divert all search queries to forged search engine.
- It collects personal information of the victim and tracks its web usage pattern.
- It comes with legit software which has a digital certificate making it difficult for regular users to uninstall it.
- It has the ability to execute any kind of code which makes the malware extremely dangerous.

User Checklist:

- Users should check their default home page and default search engine in the browsers.
- Users should review the extensions and plugins of their browsers and try to modify the search engine.
- If you are unable to change the settings, then there is a chance that your system has been compromised.

Tel +966 11 293 1501 **Fax** +966 11 293 3758
Email info@is.com.sa **Web** www.is.com.sa

Command and Control servers and Indicators of Compromise to investigate the PC have been mentioned in **Appendix A and Appendix B** respectively.

Our MSS provides our clients with the ability to block known and unknown malicious files by only allowing the approved files and application to execute. This ensures that even legitimate files will not be able to run until assessed by our security experts. Using advanced technologies for Managed Endpoint Protection, our MSS team can block File Names, File Paths, Digital signatures and Hashes.

Some of our Managed Security Services features includes:

- 24x7 Pro-active defense for every endpoint in your environment from known and unknown threats.
- Stop zero-day threats by allowing only approved list of software and applications to be executed.
- Stop malicious software by blocking known viruses, Trojan, applications exploits and custom/targeted attacks.
- Monitor and control access to the Windows registry and specific processes.
- Monitor and control file integrity to prevent or report access to critical, non-executable system configuration files.

APPENDIX A: MALICIOUS DOMAINS		APPENDIX B: MALICIOUS HASHES
attirerpage[.]com	hohosearch[.]com	FAB40A7BDE5250A6BC8644F4D6B9C28F
s2s[.]rafotech[.]com	yessearches[.]com	69FFDF99149D19BE7DC1C52F33AAA651
trotux[.]com	d3l4qa0kmel7is[.]cloudfront[.]net	B56D1D35D46630335E03AF9ADD84B488
startpageing123[.]com	d5ou3dytze6uf[.]cloudfront[.]net	2579DF066D38A15BE8142954A2633E7F
funcionapage[.]com	d1vh0xkmncek4z[.]cloudfront[.]net	8C61A6937963507DC87D8BF00385C0BC
universalsearches[.]com	d26r15y2ken1t9[.]cloudfront[.]net	7ADB7F56E81456F3B421C01AB19B1900
thewebanswers[.]com	d11eq81k50lwgi[.]cloudfront[.]net	84DCB96BDD84389D4449F13EAC750986
nicesearches[.]com	ddyv8sl7ewq1w[.]cloudfront[.]net	5BCE955CF12AF3417F055DADC0212920
youndoo[.]com	d3i1asoswufp5k[.]cloudfront[.]net	2B307E28CE531157611825EB0854C15F
giqepofa[.]com	dc44qjwal3p07[.]cloudfront[.]net	7B2868FAA915A7FC6E2D7CC5A965B1E7
mustang-browser[.]com	dv2m1uumnsgtu[.]cloudfront[.]net	66E4D7C44D23ABF72069E745E6B617ED
forestbrowser[.]com	d1mxvenloqrqmu[.]cloudfront[.]net	
luckysearch123[.]com	dfrs12kz9qye2[.]cloudfront[.]net	
ooxxsearch[.]com	dgkytklfjrqkb[.]cloudfront[.]net	
search2000s[.]com	dgkytklfjrqkb[.]cloudfront[.]net/main/trmz[.]exe	

Tel +966 11 293 1501 **Fax** +966 11 293 3758
Email info@is.com.sa **Web** www.is.com.sa