INFOSEC 101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

June 06,2014 Release #269

–Begin Transmission–

Fake Antivirus Malware

What is it?

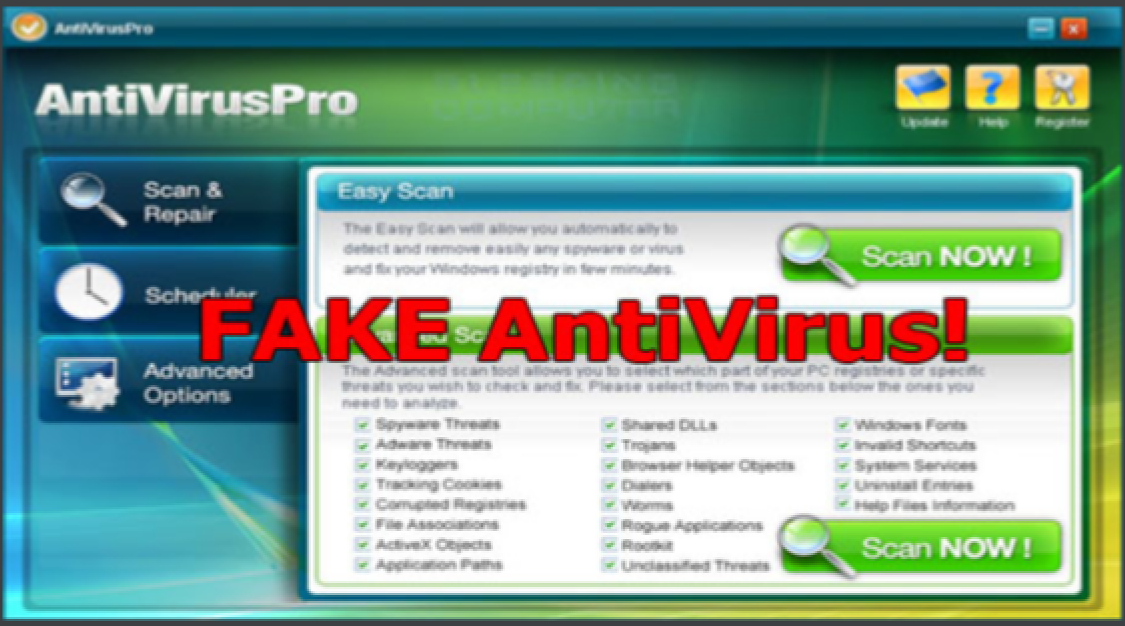
Fake antivirus malware reports non-existent threats in order to scare the user into installing malicious software and/or paying for unnecessary product registration and cleanup.

Fake antivirus malware is commonly known as scareware. Typically it is installed through malicious websites and takes the form of fake online scans. Frequently they also attempt to poison the results of popular search engines so that users access the malicious distribution sites when conducting a search.

ANTIVIRUS
Why pay when you can get free protection?
You get what you pay for.

Fake antivirus malware is financially motivated and is a big earner for cybercriminals. The large profits provide significant resources for investment into creation and distribution of fake antivirus. Hacking gangs are very good at rapidly producing professional-looking bogus websites that pose as legitimate security vendors.

How to spot one?



AntiVirusPro

AntiVirusPro

Update Help Register

Scan & Repair

Scheduler

Advanced Options

Easy Scan

The Easy Scan will allow you automatically to detect and remove easily any spyware or virus and fix your Windows registry in few minutes.

Scan NOW !

FAKE AntiVirus!

The Advanced scan tool allows you to select which part of your PC registries or specific threats you wish to check and fix. Please select from the sections below the ones you need to analyze.

☑ Spyware Threats
☑ Adware Threats
☑ Keyloggers
☑ Tracking Cookies
☑ Corrupted Registries
☑ File Associations
☑ ActiveX Objects
☑ Application Paths
☑ Shared DLLs
☑ Trojans
☑ Browser Helper Objects
☑ Dialers
☑ Worms
☑ Rogue Applications
☑ Rootkit
☑ Unclassified Threats
☑ Windows Fonts
☑ Invalid Shortcuts
☑ System Services
☑ Uninstall Entries
☑ Help Files Information

Scan NOW !

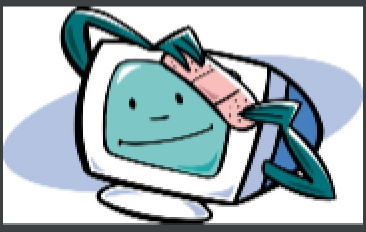
1 An antivirus program that installs itself then proceeds to "scan" the PC without user intervention is unlikely to be real.

2 Antivirus software today tries hard not to bother users.

3 If you are constantly reminded that you have to activate the product, it's probably fake.

4 It asks for payment in order to "clean" the system.

How to prevent



✓ Using up-to-date, legitimate antivirus or endpoint security software

✓ User Awareness.

✓ Avoid clicking on suspicious links or accessing malicious websites.

–End Transmission–

Information Security: It's a Shared Responsibility

REFERENCES

http://www.sophos.com/en-us/threat-center/threat-analyses/threatsaurus/a-to-z-of-threats/f/fake-antivirus-malware.aspx

http://blog.trendmicro.com/trendlabs-security-intelligence/fakeav-101-how-to-tell-if-your-antivirus-is-fake/

–End Transmission–

Document Code: 2014ICT_15SECA023