MUST READ The US military is still sending un-encrypted emails

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence |
Laws and regulations | Malware | Mobile | Security | Social Networks | Reports |
SA Team | EXTENDED COOKIE POLICY | Contact me |
elligence Laws
NDED COOKIE POLIC

third time

September 25, 2015 By Pierluigi Paganini

Michael Horowitz from Computerworld discovered an application called “Lenovo Customer Feedback Program 64,” which is used to gather customers feedback data.

Once, two, three … this is the third time that security experts discover a spyware pre-installed on

Lenovo laptops and workstations, and also in this case without the knowledge of its millions of users.

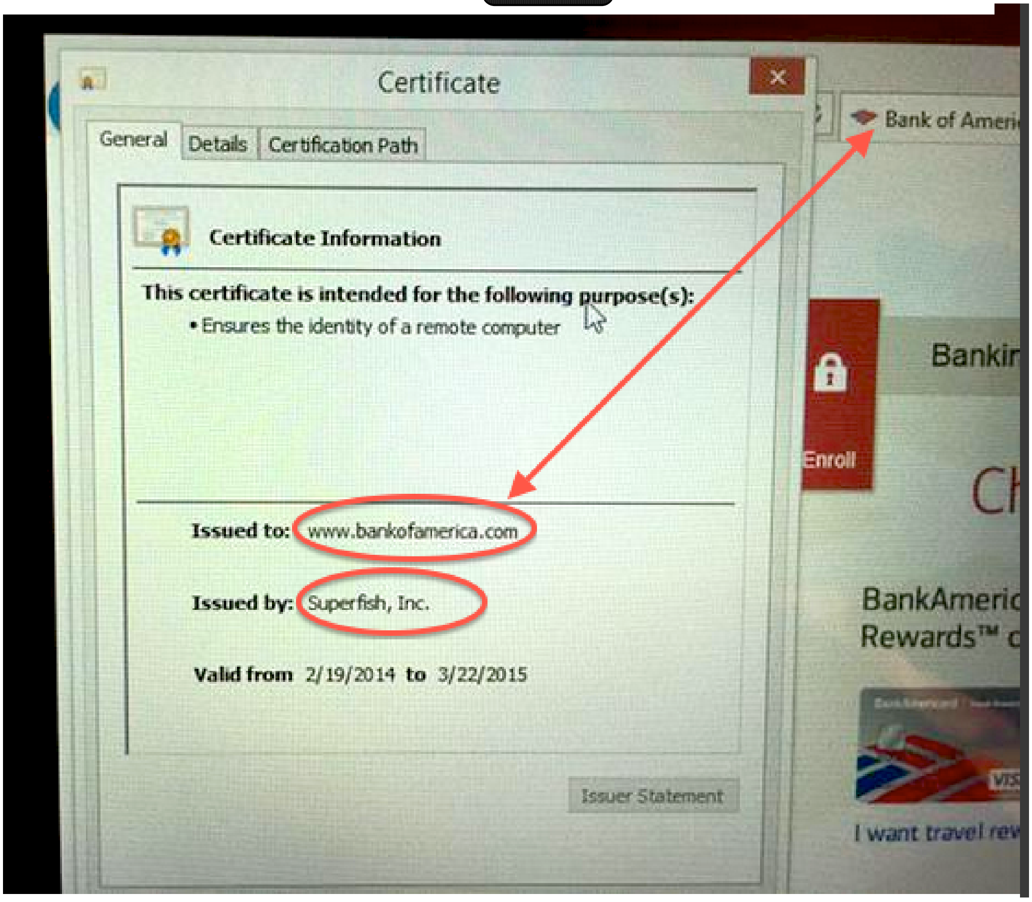
The IT giant was already accused in the past for selling some refurbished laptop models with pr installed application that were collecting users' data for commercial purposes. Earlier this year, security experts reported Lenovo was selling laptops pre-installed with Superfish spyware that anyway could be exploited by attackers to spy on the end-users.

SuperFish is considered by many antivirus companies as a potentially unwanted program, adwa or a trojan. The "Superfish" malware was installed on laptops sold by Lenovo until January 2015 was able to steal web traffic using fake, self-signed, root certificates to inject advertisements int sessions. Lenovo removed Superfish after numerous users reported the embarrassing discove on its forums by claiming to be victims of attacks.

"A blatant man-in-the-middle attack malware breaking privacy laws. I have requested return of laptop and refund as I find it unbelievable that … Lenovo would facilitate such applications pre bundled with new laptops," the user wrote on the Lenovo forums.

"I just bought a Lenovo G50 Notebook. And as you might guess it's also "infected" with PUP (a SuperFish Software (that's the one which displays ads on webpages)). So, now i try to clean up a brand new device. Sounds a bit absurd. What do you think?" said another user.

erading a



Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

• Ensures the identity of a remote computer

Issued to: www.bankofamerica.com

Issued by: Superfish, Inc.

Valid from 2/19/2014 to 3/22/2015

Issuer Statement

MORE S

Naikon
Chinese
Accordin
Naikon A
the China
it throug

A similar circumstance is happened again this summer, in August security experts discovered that the company was installing unwanted and unremovable rootkit software on certain Lenovo laptop model and desktop PCs.

The controversial feature is called "***Lenovo Service Engine***" (LSE), it is a function implemented in the firmware of computers sold by Lenovo.

According to the security experts, if Windows is installed on the computer, the LSE automatically downloads and installs Lenovo software. The operations start during bootstrap before the Microsoft operating system is launched, overwriting some of the Windows operating system files.

The Lenovo Service Engine injects software that updates, drivers, and firmware onto a Windows machine even if users completely reinstall the OS and remove pre-installed software.

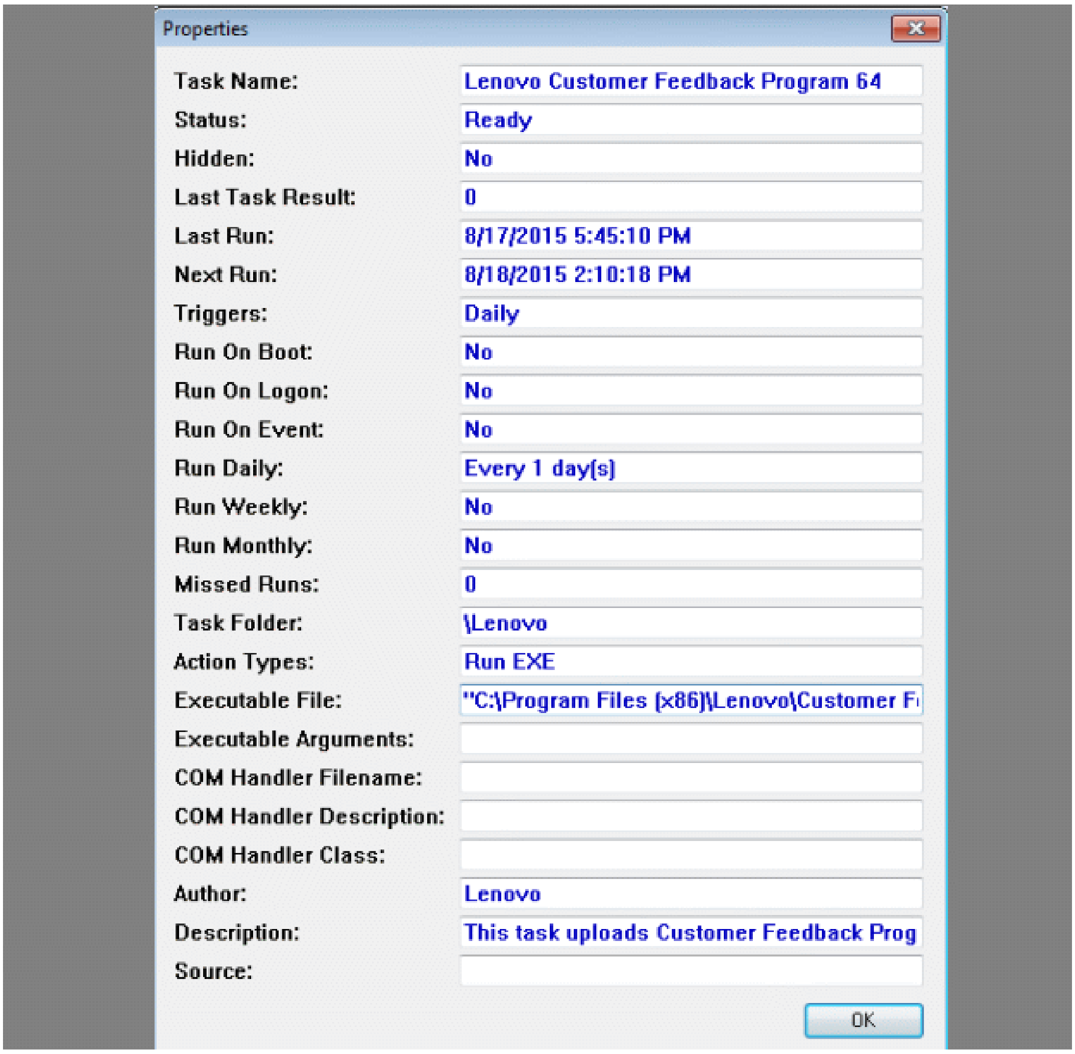
On various forums, users speculated the existence of a Lenovo "bootkit" impossible to remove.

According to the company, its service doesn't collect user data neither personally identifying information, but sends back some basic information, including the system model, date, region, and system ID.

News of the day is that Lenovo is embedding tracking software into its laptops and workstations, models affected are Lenovo ThinkPad, ThinkCentre, and ThinkStation series.

Michael Horowitz from Computerworld has discovered a disputable software, called "**Lenovo Customer Feedback Program 64**," which is used by Lenovo to gather customers' feedback data.

> *"The task that gave me pause is called "Lenovo Customer Feedback Program 64". It was running daily. According to the description in the task scheduler: "This task uploads Customer Feedback Program data to Lenovo." wrote Horowitz.*



Task Name:	Lenovo Customer Feedback Program 64
Status:	Ready
Hidden:	No
Last Task Result:	0
Last Run:	8/17/2015 5:45:10 PM
Next Run:	8/18/2015 2:10:18 PM
Triggers:	Daily
Run On Boot:	No
Run On Logon:	No
Run On Event:	No
Run Daily:	Every 1 day(s)
Run Weekly:	No
Run Monthly:	No
Missed Runs:	0
Task Folder:	\Lenovo
Action Types:	Run EXE
Executable File:	"C:\Program Files (x86)\Lenovo\Customer F
Executable Arguments:	
COM Handler Filename:	
COM Handler Description:	
COM Handler Class:	
Author:	Lenovo
Description:	This task uploads Customer Feedback Prog
Source:	

Horowitz clarified that Lenovo has explicitly referred the software in its EULA.

"The [EULA] document says that it can be found in the

```
C:\windows\system32\oobe\info
```

folder. The folder contains 39 files. Which is the EULA? It doesn't say.

Apparently, the reason I only ran across one of the two phone-home EXEs is that the Lenovo Experience Improvement system un-installs itself after 90 days. The document mentions that it can also be manually un-installed from the Control Panel "Programs and Features" where it is listed as "Lenovo Experience Improvement".

Lenovo repeatedly mentions, in document HT102023, that the data they collect is not "personally identifiable information". They also state that the only apps for which they collect data are their own. And, Lenovo.TVT.CustomerFeedback.Agent.exe gets a clean bill of health at Virus Total where it was first seen in May of 2014." continues Horowitz.

According to Horowitz the application includes also these other files:

- Lenovo.TVT.CustomerFeedback.Agent.exe.config

- Lenovo.TVT.CustomerFeedback.InnovApps.dll
- Lenovo.TVT.CustomerFeedback.OmnitureSiteCatalyst.dll

Omniture is an online marketing and Web analytics company, Horowitz speculate that it is included to monitor users' online activities.

"So, while there may not be extra ads on ThinkPads, there is some monitoring and tracking. On the one hand this is surprising because the machines were refurbished and sold by IBM. On the other hand, considering Lenovo's recent history, it's not surprising at all."

Users that want to remove the Lenovo Customer Feedback Program 64 application need to follow this procedure:

- Know your System Type (whether it's a 32-bit or 64-bit version of Windows)
- Download TaskSchedulerView
- Now, search your Lenovo PCs for Lenovo Customer Feedback Program 64
- Disable Lenovo Customer Feedback Program 64 daily task from running
- Additionally, you can also rename the "C:\Program Files (x86)\Lenovo"

Pierluigi Paganini

(Security Affairs – Lenovo, malicious application)

Share it please ...

Share this:

Email | Twitter 46 | Print | LinkedIn 43 | Facebook 27 | More

Lenovo | marketing | pre-installed malware | spyware | Superfish | unwanted program | web monitoring

Breaking News | Digital ID | Hacking | Malware

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE
Naikon APT Group backed by the Chinese PLA Unit 78020

NEXT ARTICLE
The US military is still sending un-encrypted emails

YOU MIGHT ALSO LIKE

Xkeyscore: the secret Germany’s deal with the NSA

Yet malicious software found on Lenovo PCs

August 13, 2015 By Pierluigi Paganini

August 28, 2015 By Pierluigi Paganini