

Forum:[Hack Forums](#)

Thread: [Did I successfully remove this?](#)

theDuke - March 13, 2016, 7:37 pm

I received an email to my business email that looks like a typical email for me.

It read there is an attached invoice and it's in .doc format.

I opened it and it said that Microsoft office has protected the content.

I scanned the file with Avast and it said that a threat was detected. I removed it and deleted the file.

The email read;

This email is being sent in order to inform you that a new invoice has been generated for your account. Please see the attached file.

and it was from laureenebylt@rambler.ru

Now Avast is reporting this:

Now, I am wondering if I am infected, and what is the proper way to clean this?

Thanks for your help.

I would also like to do a full checkup if I could.

9/11 - March 13, 2016, 7:44 pm

Scan your computer with Malwarebytes.

theDuke - March 13, 2016, 7:58 pm

(Mar 13, 2016 07:44 PM)Donald J. Drumpf Wrote: [\[CITE\]](#) Scan your computer with Malwarebytes. Just did, thanks.

Showed 22 threats and I removed them all and re-scanned. Nothing detected now. How can I be sure I am fully clean now?

9/11 - March 13, 2016, 8:01 pm

(Mar 13, 2016 07:58 PM)VersaceKing Wrote: [\[CITE\]](#) Just did, thanks.

Showed 22 threats and I removed them all and re-scanned. Nothing detected now. How can I be sure I am fully clean now?

If your mouse starts moving randomly then you're fucked.

Starki - March 13, 2016, 8:01 pm

(Mar 13, 2016 07:58 PM)VersaceKing Wrote: [\[CITE\]](#) Just did, thanks.

Showed 22 threats and I removed them all and re-scanned. Nothing detected now. How can I be sure I am fully clean now?

Firstly what were the threats that was found, attach the log if you can. Too fully assure you are clean, doing a FRST scan of your system will probably be appropriate.

?Synapse - March 13, 2016, 8:02 pm

(Mar 13, 2016 08:01 PM)Donald J. Drumpf Wrote: [\[CITE\]](#) If your mouse starts moving randomly them you're fucked.

I don't think a RATTter would make it so obvious, they'd either wait til your AFK or use remote desktop.

9/11 - March 13, 2016, 8:03 pm

(Mar 13, 2016 08:02 PM)?Synapse Wrote: [\[CITE\]](#) I don't think a RATTter would make it so obvious, they'd either wait til your AFK or use remote desktop.

Ehh you never know.

theDuke - March 13, 2016, 8:05 pm

(Mar 13, 2016 08:01 PM)Jam Jar Wrote: [\[CITE\]](#) Firstly what were the threats that was found, attach the log if you can. Too fully assure you are clean, doing a FRST scan of your system will probably be appropriate.

Code Malwarebytes Anti-Malware
www.malwarebytes.org

Scan Date: 3/13/2016

Scan Time: 7:45 PM

Logfile:

Administrator: Yes

Version: 2.2.0.1024

Malware Database: v2016.03.14.01

Rootkit Database: v2016.03.12.01

License: Free

Malware Protection: Disabled

Malicious Website Protection: Disabled

Self-protection: Disabled

OS: Windows 10

CPU: x64

File System: NTFS

User: --

Scan Type: Threat Scan

Result: Completed

Objects Scanned: 356690

Time Elapsed: 5 min, 34 sec

Memory: Enabled

Startup: Enabled

Filesystem: Enabled

Archives: Enabled

Rootkits: Disabled

Heuristics: Enabled

PUP: Enabled

PUM: Enabled

Processes: 0

(No malicious items detected)

Modules: 0

(No malicious items detected)

Registry Keys: 3

PUP.Optional.MyBrowser, HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{CEB36A40-1884-422D-B1CB-E61EF7A88BD}, Delete-on-Reboot, [f2b7780fc1d87eb8e54d097aed17d42c],
PUP.Optional.MyBrowser, HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{ED0579FB-3D79-4400-ADC4-3AE0BA759CEB}, Delete-on-Reboot, [e0c9fe89cecb15211d142360768ec739],
PUP.Optional.ProductSetup, HKU\S-1-5-21-1044105832-515205811-4118248317-1002\SOFTWARE\PRODUCTSETUP, Quarantined, [189165226c2d7fb76e075ac4c83cbe42],

Registry Values: 4

PUP.Optional.MyBrowser, HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{CEB36A40-1884-422D-B1CB-E61EF7A88BD}|Path, \IBUpd, Delete-on-Reboot, [f2b7780fc1d87eb8e54d097aed17d42c]
PUP.Optional.MyBrowser, HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\SCHEDULE\TASKCACHE\TASKS\{ED0579FB-3D79-4400-ADC4-3AE0BA759CEB}|Path, \IBUpd2, Delete-on-Reboot, [e0c9fe89cecb15211d142360768ec739]
Trojan.Neurevt, HKU\S-1-5-21-1044105832-515205811-4118248317-1002\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN|Windows Font Preloader Service, "C:\ProgramData\Windows Font Preloader Service\c3i71gy5q3c37.exe", Quarantined, [04a581063d5c4aec879a254f937135cb]
PUP.Optional.ProductSetup, HKU\S-1-5-21-1044105832-515205811-4118248317-1002\SOFTWARE\PRODUCTSETUP|tb, 0N0U0L1F, Quarantined, [189165226c2d7fb76e075ac4c83cbe42]

Registry Data: 0

(No malicious items detected)

Folders: 1

PUP.Optional.SpringFiles, C:\ProgramData\Microsoft\Windows\Start Menu\SpringFiles, Quarantined, [beebc1c66f2ab581338a0a07fb080df3],

Files: 14

Trojan.Agent, C:\ProgramData\Nimoru\GizmoSE, Quarantined, [e0c9eb9c46536acc91c2bf5bd32e1ce4],
Backdoor.Bot, C:\ProgramData\Nimoru\LicenseSE, Quarantined, [f8b1e6a1d1c82b0bdf086adf28daa55b],
PUP.Optional.AdLoad, C:\Users\--\AppData\Local\Temp\1WAEv0jyww.exe, Quarantined, [9e0bd4b39ffa41f50e72ebfc748d02fe],
Trojan.Agent.H, C:\Users\--\AppData\Local\Temp\is-C48SR.tmp\precomp042.exe, Quarantined, [c1e892f51b7e83b3b7aa50e858aafb05],
PUP.Optional.OpenCandy, C:\Users\--\Downloads\CheatEngine65.exe, Quarantined, [397031560b8e3ef89dd738ab3fc228d8],
Trojan.Agent, C:\Users\--\AppData\Roaming\383844.exe, Quarantined, [7d2c1e69455476c02de3f1c9d033d729],
PUP.Optional.eShopComp, C:\Users\--\AppData\Local\Google\Chrome\User Data\Default\Local Storage\http_pstatic.eshopcomp.com_0.localstorage, Quarantined, [29806027f3a6ee48fe38730619eb0ff1],
PUP.Optional.eShopComp, C:\Users\--\AppData\Local\Google\Chrome\User Data\Default\Local

Storage\http_pstatic.eshopcomp.com_0.localstorage-journal, Quarantined,
[b1f8ff88badfd264ff3788f109fb41bf],
PUP.Optional.CrossRider, C:\Users\--\AppData\Local\Google\Chrome\User Data\Default\Local
Storage\https_d19tqk5t6qcjac.cloudfront.net_0.localstorage, Quarantined,
[4762a7e08f0a71c5cec51b618d779070],
PUP.Optional.CrossRider, C:\Users\--\AppData\Local\Google\Chrome\User Data\Default\Local
Storage\https_d19tqk5t6qcjac.cloudfront.net_0.localstorage-journal, Quarantined,
[34751077bddc38fe454e0b719c68d729],
PUP.Optional.HDApp, C:\Users\--\AppData\Local\Google\Chrome\User Data\Default\Local
Storage\https_hdapp1008-a.akamaihd.net_0.localstorage, Quarantined,
[16932a5dabee66d061402954d331a35d],
PUP.Optional.HDApp, C:\Users\--\AppData\Local\Google\Chrome\User Data\Default\Local
Storage\https_hdapp1008-a.akamaihd.net_0.localstorage-journal, Quarantined,
[b3f69cebb9e0b87eebb67c01af55c53b],
Trojan.Neurevt, C:\ProgramData\Windows Font Preloader Service\c3i71gy5q3c37.exe,
Delete-on-Reboot, [04a581063d5c4aec879a254f937135cb],
PUP.Optional.SpringFiles, C:\ProgramData\Microsoft\Windows\Start
Menu\SpringFiles\SpringFiles.lnk, Quarantined, [beebc1c66f2ab581338a0a07fb080df3],

Physical Sectors: 0
(No malicious items detected)

(end)
Thanks, I'll look into that.