

## Joyce Nicola

---

**From:** Vince Orton [vorton@pacstates.com]  
**Sent:** Thursday, October 08, 2009 11:26 AM  
**To:** Joyce Leibelt  
**Subject:** PC Forensic Report

Joyce -

This will serve as an informal report for the desktop computer you submitted for forensic analysis.

1) The original drive was imaged to DVD media to preserve the original state of the machine. This was not a full forensic image (sector-by-sector), but rather a more condensed image of active sectors (far less data to archive). Based upon discussions with you, this was deemed more appropriate. \*\* You will receive the Forensic DVD system image.

2) The original drive was imaged again to an external drive to be used for scanning and analysis.

3) Subsequent analysis was performed on the copied drive only. The original drive remains exactly as it was when we received the desktop computer. \*\* You will receive your system back exactly as provided to PacStates for analysis.

4) The copied drive was analyzed for spyware, adware, worms, trojans, and virus infections.

5) Using a Windows-based scanning tool, the drive showed no infections. However, several directory trees and files could not be accessed indicating that the tools were not able to complete a 100% analysis. Normally this isn't considered unusual, but given the nature and ingenuity of the suspected attack, we felt that further research was warranted.

6) We built a Linux-based system to repeat selected scans and analysis on the theory that Linux would bypass possible Windows-based protocols to protect and/or hide files. Selected scans were repeated with the copied drive using the Linux system.

7) Two instances of Trojan.Zbot-5918 were reported:

-----  
Found 2 possible viruses (66201 files scanned).  
C:/WINDOWS/SYSTEM32/sdra64.exe Trojan.Zbot-5918  
C:/WINDOWS/Temp/14.tmp Trojan.Zbot-5918  
-----

8) A search for Trojan.Zbot-5918 returns the following information:

a) Trojan.Zbot has variations:

Trojan-Spy:W32/ZBot.HS  
Trojan-Spy:W32/Zbot.KZ  
(and others)

b) Attempts to steal online banking login-information and other sensitive data from the infected computer.

c) ZBot variants target online banking. Banks in multiple countries have been targeted. Various languages have been used in spam pushing the installation.

d) ZBot variants use modular components (configuration and commands) downloaded from the Internet after installation. The components are encrypted and hinder full analysis as the ZBot requires an online connection and all components to determine full functionality.

e) Browser activity is monitored for multiple ".fi", ".ch", ".de", ".nl"

and ".com" bank URL addresses. Logging online banking information is the primary payload of Trojan-Spy:W32/Zbot variants.

f) ZBot.HS attempts to hide using stealth techniques.

g) Attack vector variations are likely, but the Trojan.Zbot appears to commonly infect through spam, using social engineering to trick the user into clicking a link, which downloads the trojan and results in the infection.

h) More information:

[http://www.f-secure.com/v-descs/trojan-spy\\_w32\\_zbot\\_hs.shtml](http://www.f-secure.com/v-descs/trojan-spy_w32_zbot_hs.shtml)

9) CONCLUSION: It is highly likely that this computer's infection resulted in unauthorized bank account access since that is its observed behavior.

10) RECOMMENDATION: Completely erase and reinstall all software on this desktop computer, including the O/S and business applications. Use the DVD image to retrieve any existing data files that are required - do not boot up this computer while connected to your company's network.

\*\*\*\*\*

That's it. I can produce a more complete and detailed report, but I don't think GenLabs will benefit from further analysis or detail beyond the above conclusion and recommendation.

Thanks,  
-Vince

--

Vince Orton - Pacific States Systems Company 909-297-5880 Office 951-201-3730 Cell  
888-281-3606 Fax  
vince.orton Skype