Lab Report 19

1. Assessment Sheet
2. **When you are notified that a user’s workstation or system is acting strange and log files indicate system compromise, what is the first thing you should do to the workstation or system and why?**

When we found abnormal things happening in a user’s workstation, we should inform IT implementation department and ask them to isolate the individual machine for instance, disconnect the Internet. In this process, we cannot power off the machine directly because, some sensitive data might not saving properly before we restart the workstation and the files’ integrity cannot be guaranteed.

1. **When an antivirus program identifies a virus and quarantines this file, has the malware been eradicated?**

Actually, antivirus program doesn’t remove the infected file directly from the operating system; instead, it will isolate this file in to a particular position where the virus cannot take effect. The purpose of doing this is that anti-virus program provides an opportunity with end user if they want restore a file rather than truly delete that file.

1. **What is the SANS Institute’s six-step incident handling process?**

In the SANS Institute’s incident handlings reports, it says that we have the following six phases for incident handlings process.

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lesson Learned
7. **What is the risk of starting to contain an incident prior to completing the identification process?**

If we haven’t completed the identification process before taking action, we might make mistakes, which probably allow the real harmful incidents keep in deep. From another aspect, if we take action on a wrong object, it is a great waste for system recourses. So, to sum up, security practitioners should classify those incidents and identify the root causes of those incidents clearly in ahead, so that we can avoid making mistakes when responding.

1. **Why is it a good idea to have a security policy that defines the incident response process in your organization?**

We know that policy is an organization-wide rules and any violation of a policy will be punished by the organization. And at the same time, defining the incident response process is a very important thing because once a serious incident happens if we don’t have a pre-defined countermeasure. It will cause chaos of the organization. As a consequence, the company might not be able recover its business within an expected periods. So, the company might suffer much more huge losses.

1. **The post-mortem “lesson learned” step is the last in the incident response process. Why is this the most important step in the process?**

The lesson learned in this phase can help us refine the future incident response plan.

1. Challenge Questions

**Description:** **creating a plan for receiving and re-introducing the field team’s computers back into the company network. Briefly describe your plan for ensuring that any infected machines do not impact the corporate network. What should you consider when creating your plan? What lessons learned could be incorporated in the future?**

Answer:

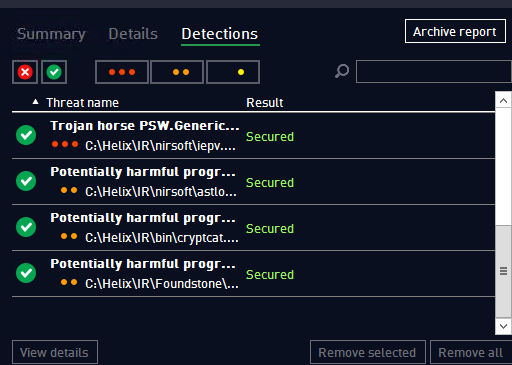
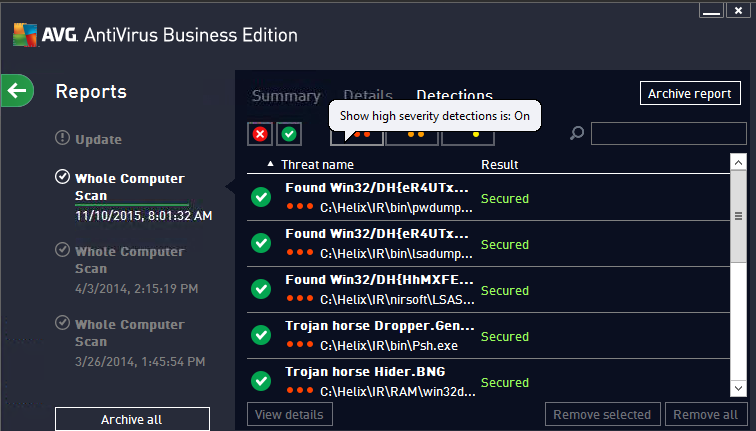
Because the computers of field team were infected and at the same time we need to re-introduce these computers to our own network system, so the primary thing is to back up all the data of infected computer. And then we should isolate these computers and perform a virus scanning for each computer. Before the scanning, we need to update the signature database of the anti-virus tools.

After the scanning, we need to change our firewall setting of our corporate network system which should restrict the access from those infected systems.

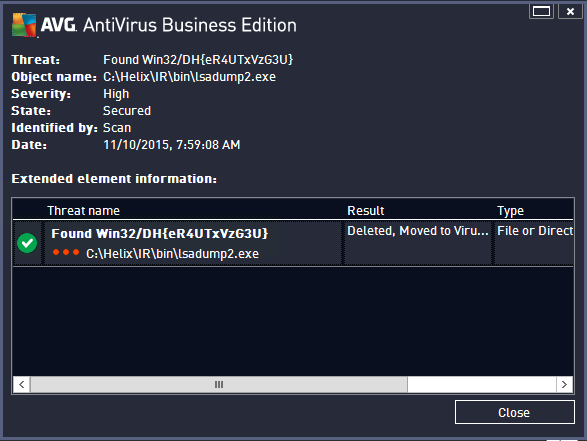
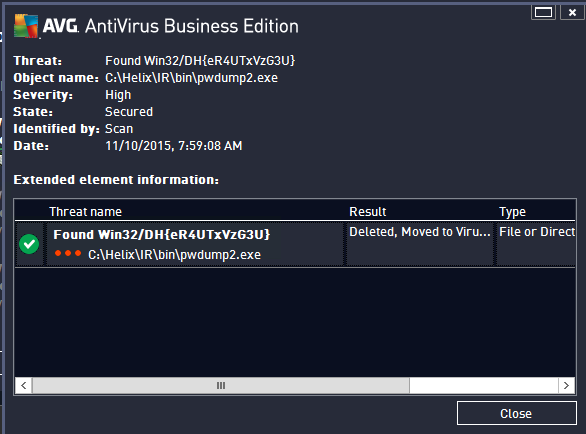
When I am creating a plan, the most important thing I consider is that the security of the data which means that we need backup these compete data first because when the virus scanning start, some files might be deleted with a mistake of anti-virus tools. In addition, isolation is another aspect that I considered most because isolation can stop the spreading of viruses, which help us prevent the further damages to our entire network systems. We have to control the viruses into a controllable scope so that we can deal with it quickly and effectively.

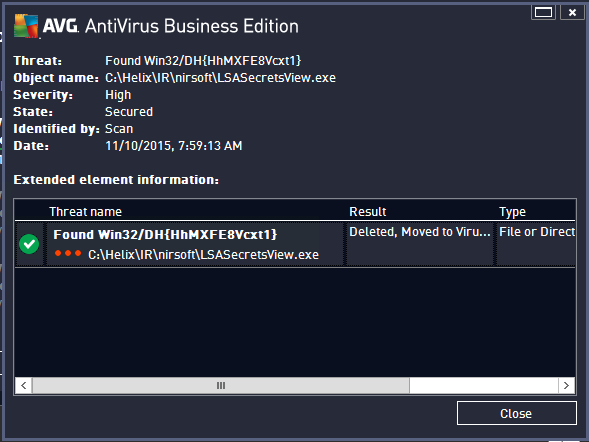
The lesson we learned from this incident is that we have to strengthen security of single computers, especially for those computers which are brought from outside. We need implement host-based prevention for those computers so that we can try our best to avoid the enlargement of the bad consequences.

1. Report Screenshot
2. Detections summary of AVG



1. Threats details
2. Found win32/DH{eR4UTxVzG3U} and Found Win32/DH{HhMXFe8Vcxt1}

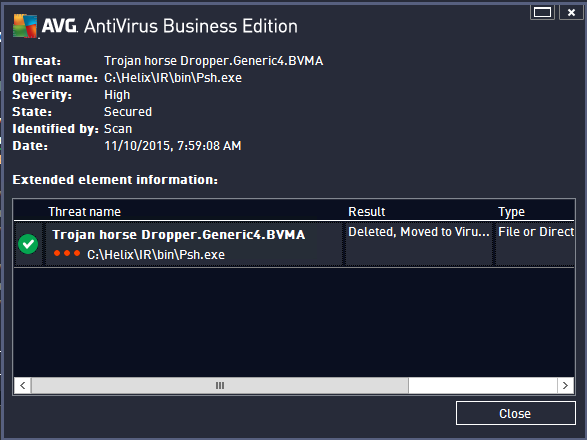




Answer:

In order to remove Win/DH virus, we need first top Win32/DH services and then we need remove this program in control panel > add/remove programs > choose Win32/DH > uninstall. After doing this, we need to remove the registry information from Windows registry in order to make it is removed cleanly.

1. Trojan horse Dropper.Generic4.BVMA



Answer:

1. Backup PC data
2. Stop Random.exe process
3. Delete the following file

%AppData%\[random].exe  
%ProgramFiles%\LP\[random].tmp  
%ProgramFiles%\LP\[random].exe  
%Windows%\system32\[random].exe

1. Delete the following registry entries.

NT\CurrentVersion\Winlogon\”Shell”=”[SET OF RANDOM CHARACTERS].exe”

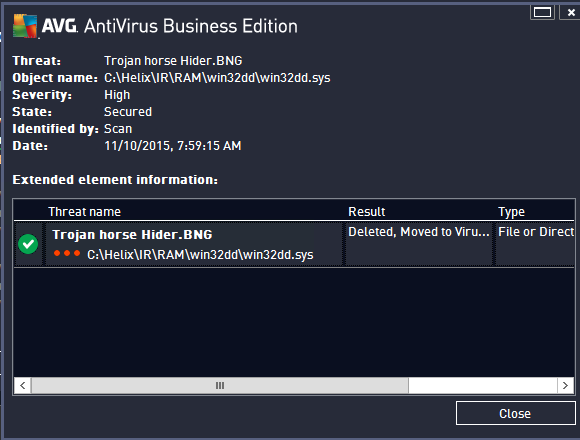
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Shared Tools\MsConfig\startupfolder\[random names]

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Shared Tools\MsCongif\startupreg\[random names]

Reference:

Mock, S. (2013, 2 6). *How to Remove Trojan horse dropper.generic4.bvma*. Retrieved 11 16, 2015, from blogspot.com: http://removevirustool.blogspot.com/2013/02/how-to-remove-trojan-horse.html

1. Trojan horse Hider.BNG



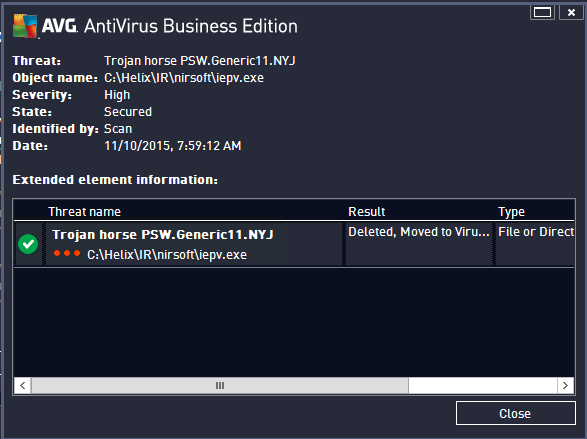
Answer:

1. Reboot workstation to safe model
2. Run anti-virus tools

Reference:

Brewer, T. (2013, 1 29). How to Remove Trojan Horse Hider.MPR Permanently? Retrieved 11 16, 2015, from Anvisoft: http://www.anvisoft.com/resources/how-to-remove-trojan-horse-hider-mpr-permanently/

1. Trojan horse PSW.Generic11.



Answer:

1. Reboot our infected machine into safe model
2. Kill the following processes

%AppData%\[RANDOM CHARACTERS]\[RANDOM CHARACTERS].exe

1. Remove the files and folders

%Desktopdir%\Trojan PSW.Generic11.NYJ.lnk

%Programs%\Trojan PSW.Generic11.NYJ\Trojan PSW.Generic11.NYJ.lnk

1. Remove the following entries of windows registry

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Trojan PSW.Generic11.NYJ\DisplayIcon %AppData%\[RANDOM CHARACTERS]\[RANDOM CHARACTERS].exe,0

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Trojan PSW.Generic11.NYJ

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Trojan PSW.Generic11.NYJ\UninstallString “%AppData%[RANDOM CHARACTERS][RANDOM CHARACTERS].exe” -u

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\[RANDOM CHARACTERS] %AppData%\[RANDOM CHARACTERS]\[RANDOM CHARACTERS].exe

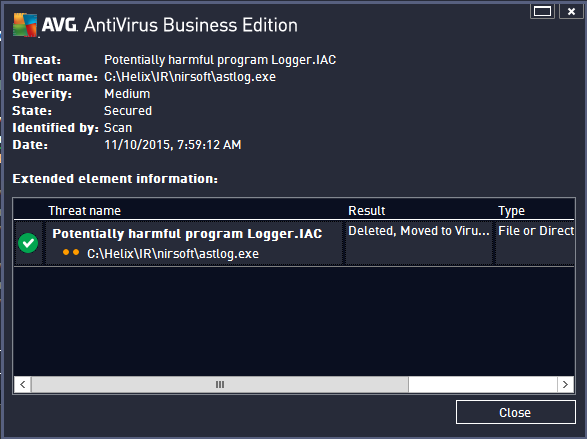
HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Trojan PSW.Generic11.NYJ\ShortcutPath “%AppData%\[RANDOM CHARACTERS]\[RANDOM CHARACTERS].exe” -u

HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Trojan PSW.Generic11.NYJ\DisplayName Trojan PSW.Generic11.NYJ

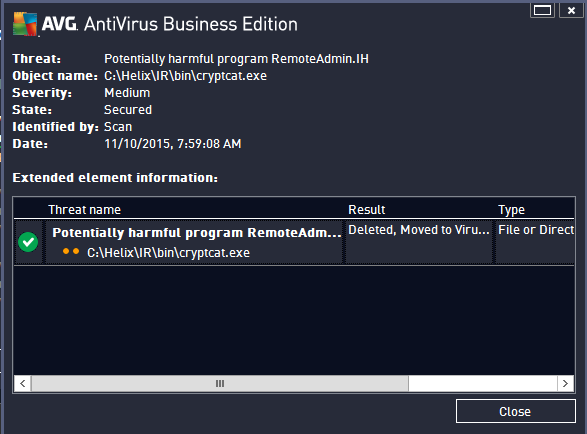
Reference:

Parker, J. (2003, 7 6). How to Remove Trojan PSW.Generic11.NYJ ? Retrieved 11 16, 2015, from SpywareRemovers: http://spywareremovers.com/how-to-remove-trojan-psw-generic11-NYJ

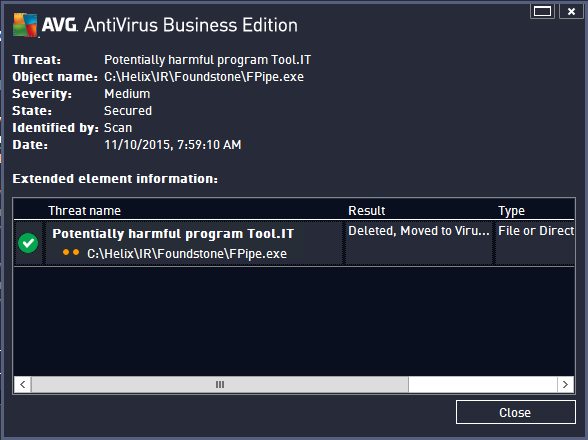
1. Potentially harmful program Logger.IAC



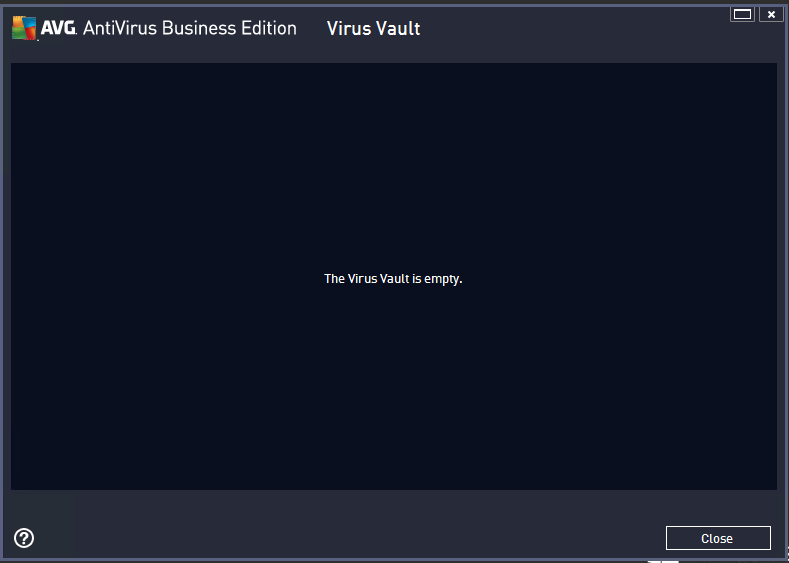
1. Potentially harmful program RemoteAdmin.IH



1. Potentially harmful program Tool.IT



1. Empty Virus Vault



1. Security incident report

1. Other additional supporting text/image content