1. An example of a host-based intrusion detection tool is the tripwire program. This is a file integrity checking tool that scans files and directories on the system on a regular basis and notifies the administrator of any changes. It uses a protected database of cryptographic checksums for each file checked and compares this value with that recomputed on each file as it is scanned. It must be configured with a list of files and directories to check and what changes, if any, are permissible to each. It can allow, for example, log files to have new entries appended, but not for existing entries to be changed. What are the advantages and disadvantages of using such a tool? Consider the problem of determining which files should only change rarely, which files may change more often and how, and which change frequently and hence cannot be checked. Consider the amount of work in both the configuration of the program and on the system, administrator monitoring the responses generated.

The advantages of using such tool is system can easily catch and identify the changed files or directories.

The disadvantages of using such tool is that during normal operation, it is normal to have changes with files and directories. The tool may not be able to examine if it is normal or being attacked but sending notes to the administrator. Administrator may receive numerous notifications and hard to find the unexpected changes.

The user information, privileges should only change rarely

The documentation files should be change more often as users may use them for normal operation.

2. The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run D (P), the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program: Program CV := {. . . main-program := {if D(CV) then goto next: else infect-executable; } next: } In the preceding program, infect-executable is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.

No, D cannot correctly decide whether CV is a virus. From the description, we knows that CV is a virus which will duplicate itself during operation. D(CV) should return true as CV is a virus, but the program go to next instead of infect-executable. On the other hand, if D(CV) is false, it will infect-executable which gives wrong condition of the statement.

As correctness, if D(CV) then infect-executable: else go to next;

3. Consider the following fragment: legitimate code if data is Friday the 13th; crash_computer(); legitimate code What type of malware is this?

This is logic bomb as when it execute, it will destroy the target. When the date is Friday the 13th, it will execute the function crash_computer() which will damage the computer operation.

4. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

No, you should not plug in and examine the USB stick in your working computer as you always don't know what is in there and it is safe for not doing that.

Executable virus, macro virus, Trojan Horse, and worms can be transport by USB stick.

For mitigate the threats, you can use strong up-to-date anti-virus software to scan the stick, use VM ware to check the USB. But try not to run it in working space.

5. Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book". Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? What types of malware might it be?

You could be suspicious that the game wants these types of permissions by using your address book sending malicious code from you to your friends and get them affected. It could be Trojan Horse collects personal information of contacts to attackers and they can use this information to achieve their goals. It may causes loss of data and system damage.

Nowadays, every company collects user's information and store in their database, and sell them to somewhere else to gain more money. You cannot guarantee you will be exposed information to attackers or not. It is possible that the game contains Trojan Horse and steal your contacts information and sending malicious code. If you are using a new smartphone, it might be okay if you download the game and play it since you don't have a contact. You can always check your phones later for anti-virus.

6. List the types of attacks on a personal computer that each of a (host-based) personal firewall, and anti-virus software, can help you protect against. Which of these countermeasures would help block the spread of macro viruses spread using email attachments? Which would block the use of backdoors on the system?

Trojan, Virus, Worms, Spyware, Keylogger, Adware, Backdoor, Wabbits, Exploit, Botnet, Dialer, Dropper, Fake AV, Phishing, Cookies, Bluesnarfing, Bluejacking, DDoS, Boot Sector Virus, Browser Hijackers, Virus Document, Mousetrapping, Obfuscated Spam, Pharming, Crimeware, and SQL Injection.

For countermeasures, DS authentication will help the email attachments as it is not from the trusted user, up-to-date anti-virus application can help find the macro viruses. Do not open snit-virus alerted mails.

For blocking backdoors, firewall and anti-virus application can help with the backdoors.

7. Research and list any three malwares that occurred in 2019. If possible, classify them as virus, worm or Trojan. Provide technical details of how the attack occurred, what vulnerability was exploited, what was the impact of the attack. Briefly provide countermeasures that could have possibly prevented these attacks. Provide proper references and citations.

Emotet

https://blog.malwarebytes.com/cybercrime/2019/03/emotet-revisited-this-pervasive-persistent-threat-is-still-a-danger-to-businesses/

Emotet started out in 2014 as an information-stealing banking Trojan that scoured sensitive financial information from infected systems (which is the reason why Malwarebytes detects some components as Spyware.Emotet). However, over time Emotet and its business model evolved, switching from a singular threat leveled at specific targets to a botnet that distributes multiple malware payloads to industry verticals ranging from governments to schools.

impact

"Emotet continues to be among the most costly and destructive malware affecting SLTT governments. Its worm-like features result in rapidly spreading network-wide infection, which are difficult to combat. Emotet infections have cost SLTT governments up to $1 million per incident to remediate."

Prevention
Obviously, it's preferable for businesses to avoid Emotet infections in the first place, as remediation is often costly and time-consuming. Here are some things you can do to prevent getting infected with Emotet:

- **Educate users**: Make sure end users are aware of the dangers of Emotet and know how to recognize malspam—its primary infection vector. Train users on how to detect phishing attempts, especially those that are spoofed or more sophisticated than, say, the Nigerian Prince.
- **Update software regularly**: Applying the latest updates and patches reduces the chances of Emotet infections spreading laterally through networks via EternalBlue vulnerabilities. If not already implemented, consider automating those updates.
- **Limit administrative shares:** to the absolute minimum for Emotet damage control.
- **Use safe passwords:** Yes, it really is that important to use unique, strong passwords for each online account. Investigate, adopt, and role out a single password manager for all of the organization's users.
- **Back up files**: Some variants of Emotet also download ransomware, which can hold now-encrypted files hostage, rendering them useless unless a ransom is paid. Since we and the FBI recommend never paying the ransom—as it simply finances future attacks and paints a target on an organization's back—having recent and easy-to-deploy backups is always a good idea.

botnet

https://blog.radware.com/security/botnets/2019/10/scan-exploit-control/

In general, a botnet is a network of compromised devices that have become infected with malware, allowing an attacker to control the devices. BotHerders control these infected devices through covert channels, issuing commands to the devices to perform malicious activities such as launching distributed denial of service (DDoS) attacks, sending malicious spam or information theft.

When it comes to botnet's that launch denial of service attacks, Mirai and its variants still dominate the landscape. Mirai was discovered in 2016 by MalwareMustDie and originally targeted SSH and Telnet protocols by exploiting defaults or hardcoded credentials. Mirai, its variants and other botnets have evolved over the last three years and now leverages multiple exploits that target both residential and enterprise devices.

impact

The Ecuadorian government claims it suffered 40 million cyber-attacks a day as a result of its action to evict Julian Assange.

Finland suffered a Distributed Denial of Service attack targeting Parliamentary Election results services used by the government to communicate the outcome of the elections with the general population.

AESDDoS Botnet exploited the Atlassian Confluence Server via CVE-2019-3396. The botnet was also seen exploiting an API misconfiguration found in Docker Engine-Community.

Prevention

- Network baselining: Network performance and activity should be monitored so that irregular network behavior is apparent.
- Software patches: All software should be kept up-to-date with security patches.
- Vigilance: Users should be trained to refrain from activity that puts them at risk of bot infections or other malware. This includes opening emails or messages, downloading attachments, or clicking links from untrusted or unfamiliar sources.
- Anti-Botnet tools: Anti-botnet tools provide botnet detection to augment preventative efforts by finding and blocking bot viruses before infection occurs. Most programs also offer features such as scanning for bot infections and botnet removal as well. Firewalls and antivirus software typically include basic tools for botnet detection, prevention, and removal. Tools like Network Intrusion Detection Systems (NIDS), rootkit detection packages, network sniffers, and specialized anti-bot programs can be used to provide more sophisticated botnet detection/prevention/removal.

Ransomware

https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019

Ransomware is a type of malware that encrypts the files on a user's device or a network's storage devices.

Ransomware is most typically distributed through spam email attacks. The spam email will have an attachment disguised as a legitimate file or will include a URL link in the body of the email. If the former method is used, the ransomware program is activated as soon as the attachment is opened and within seconds, starts to encrypt files on the device. If the attack vector is a link, upon clicking it the user is taken to a web page where the ransomware is delivered to the device unbeknownst to the user. The malicious programs or sites often use exploit kits to detect if there are security vulnerabilities in the device's operating system or applications that can be used to deliver and activate the ransomware.

Impact

The U.S. was hit by a barrage of ransomware attacks in 2019 that impacted at least 948 government agencies, educational establishments and health-care providers at a potential cost in excess of $7.5 billion,

Prevention

Backups are critical. Use a backup system that allows multiple iterations of the backups to be saved, in case a copy of the backups includes encrypted or infected files. Routinely test backups for data integrity and to ensure it is operational.

Restrict Internet access. Use a proxy server for Internet access and consider ad-blocking software. Restrict access to common ransomware entry points, such as personal email accounts and social networking websites.

apply the principles of least privilege and network segmentation. Categorize and separate data based on organizational value and where possible, implement virtual environments and the physical and logical separation of networks and data. Apply the principle of least privilege.

Keep all systems patched, including all hardware, including mobile devices, operating systems, software, and applications, including cloud locations and content management systems (CMS), patched and up-to-date. Use a centralized patch management system if possible. Implement application white-listing and software restriction policies (SRP) to prevent the execution of programs in common ransomware locations, such as temporary folders.