Essay on trojan virus

Business, Company

Trojan Virus

A Trojan virus is a malware that performs malicious functions under the pretext of a desired action, and it can harm the computer or compromise security.

At present, inventors of Trojans continue to release new variants, in order to see the virus remains ahead of detection and retain its continual grip on computers with the malware. Sinowal Trojan is among the most recent Trojans. Sinowal poses solemn threats to every person with an internet connection since it works secretly through a common infection scheme called drive-by downloads (Shiels, 2008). Internet users obtain the infection without recognition when they open a website that contains the Sinowal malicious code. The reason as to why Sinowal poses serious threat is because the Trojan can exist in a computer system for a long time, collecting and storing information. Several financial institutions in UK, Poland, US and Australia have reported cases of credit and debit cards being compromised by this malware. Security firms advise PC owners to scan their systems for malicious software, regularly, and update their anti-virus programs, frequently. In addition to using security soft ware, users are advised to shun from clicking items on networks with high traffic including social networks.

Also, a new Trojan virus is threatening systems of Apple Mac. Users of Apple Mac have been cautioned that a new Trojan virus can infect their PCs and steal secret codes of services like online banking, Papal and Google. The new virus is said to be a dangerous strain of Flashback, which is a Trojan virus that became discovered last year. The malware seeks to take secret control of Macs through different methods. The malware capitalizes on Java vulnerabilities a software language usually employed by websites to convey interactive aspects, and necessitates no intervention from the user to thrive. In case, Java is not set up, or all its security areas are updated, the new modification, Flashback G, tries to ploy users into installing it through presenting a sham security certificate that seems as if it comes from Apple. Mostly, users get tricked, as they click on “ continue” without knowing that they are installing malicious software in their systems. Users of Mac who have earlier versions of OS X, may be at be at a higher risk of obtaining the new Trojan, since Java was integrated as a component of the installation parcel. Besides, the Trojan gets transmitted through infected web pages, which makes it too easy to obtain this infection. Once a user opens an infected web page, the malware compromises the system through downloading and installing it covertly, devoid of the user’s conscious. However, if the system is secured, it may be hard for the Trojan to find its way. The new Trojan is extremely sophisticated as it can scan networks and obtain passwords and usernames, which it stores and conveys to cyber criminals. According to estimates, almost 600, 000 Macs are infected by the new variant of Trojan, which is a strain of Flashback.

Trojan Mitigation

New threats of Trojan viruses can be mitigated through different ways, depending on the nature of the attack.

Mitigating Reconnaissance Trojan Attacks

First, a professional in network security can notice when a reconnaissance attack is ongoing through structured alarms that become activated when certain bounds like the amount of ICMP requests in each second become surpassed.

A range of tools and technologies can be employed to monitor this action and produce an alarm. For instance, the Adaptive Security Appliance (ASA) of Cisco can be used to monitor intrusion, through a detached gadget. Moreover, authentication may be executed, in order to guarantee proper access. Encryption may, also, be used, so as, to make packet sniffer attacks ineffective (Bidgoli, 2006). Use of anti-sniffer apparatus to discover packet sniffer attacks and controlled infrastructure can, also, help in detecting reconnaissance attack. Lastly, employing IPS and firewall and can restrict the quantity of data that can be revealed with a port scanner.

Mitigating DOS Trojan Attacks

Lastly, DOS Attacks can easily be established by the network security. A network consumption graph demonstrating unusual actions could designate a DoS attack. However, mitigating DoS attacks need vigilant diagnostics, preparation, and collaboration from Internet Service Providers (ISPs), in order to establish when a DoS attack is happening. The entire process must, also, be supported by policies on network security. Other mitigation procedures for DOS attacks include use of the antispoofing technologies, establishment of Intrusion prevention systems (IPS) and firewalls as well as, use of traffic policing (Bhaiji, 2008).

Mitigating Access Trojan Attacks

A professional in network security can detect any access attacks through evaluating bandwidth utilization, logs and procedure loads. The policy on network security ought to spell out that logs become formally maintained, for every server and network device. A network security professional can establish whether an unusual amount of failed login attempts has happened, through reviewing logs. Other procedures for mitigating access attacks include ensuring that there is a strong password security, use of cryptography and using application patches and operating systems.

In conclusion, it is possible to mitigate new threats of Trojan Virus, although such mitigation requires competent network security policies and personnel.

References

Bhaiji, Y. (2008). Network security technologies and solutions. Indianapolis, IN: Cisco Press.

Bidgoli, H. (2006). Handbook of information security. Hoboken, N. J.: John Wiley.

Shiels, M. (2008, October 31). Trojan virus steals banking info. BBC News. Retrieved from http://news. bbc. co. uk/2/hi/7701227. stm.