Task 6.2

* Advanced Persistent Threat:

An Advanced Persistent Threat (APT) is a target-oriented and advanced (as the name says) attack onto an IT-System. As of its advanced technology used, there is usually a greater „investor“ who delivers the needed resources for the attack which therefore suits his interests.

One example is the „Gauss“ trojan which is widespread in Libanon, Israel as well as Palestine. Gauss explicitly looks for credentials for specific bank accounts on the infected computer. Because of its similarities to Flame, another trojan which is likely developed by the secret service of Israel and the USA, Gauss is probably made by the same team/creator.

Gauss was first identified in September of 2011 by Kaspersky.

Himmelein, G. (2012 August, 09): Banking-Trojaner „Gauss“ vermutlich mit staatlichem Auftrag

URL: <http://www.heise.de/security/meldung/Banking-Trojaner-Gauss-vermutlich-mit-staatlichem-Auftrag-1664509.html> , last request 02.07.2016

- Spear phishing:

You could say „Spear phishing“ is a more precise but more effortful version of the well known phishing mails which are just spread to random receivers. The concept of Spear phishing is to target a specific person and design a email which is trustworthy to that person. This happens via so called „social engineering“. With more information about the target, the phishing mail can be made more realistic and more likely to be opened by the target.

One incident of spear phishing happened in June of 2015 at „Ubiquiti Networks Inc.“ an network tech company in the US. Employees were tricked by „spoofed email addresses and look-alike domains“ and therefore made direkt money transfers. Because of this attack the company lost 46.7 Million Dollar.

Brecht, D. (2016 January, 18): Spear Phishing: Real Life Examples

URL: <http://resources.infosecinstitute.com/spear-phishing-real-life-examples/>

last request 02.07.2016

* Exploit Kit:

An exploit kit is a toolkit which can run on a web server and is able to explore vulnerabilities found in the victims software applications and exploit these. The victim isn't aware of the exploit as he usually just visits a website which web server got hacked. From this website the victim is redirected to a web server where the exploit kit is running. After this redirect the exploit kit gathers information about the victims system and installed applications to determine the exploit to deliver to the victims system.

Cannes, J. (2013 February, 11): Tools of the Trade: Exploit Kits

URL: <https://blog.malwarebytes.com/cybercrime/2013/02/tools-of-the-trade-exploit-kits/>

last requested 02.07.2016

One infamous exploit kit is RIG. In 2015 the source code of RIG version 2.0 was leaked and therefore RIG was not longer in use. But there is already a new version (RIG 3.0) available in the crimeware scene. After analyzing two RIG-3.0-Servers experts from Trustwave reported that 1.25 million system were infected in just about 1.5 months.

Schmidt, J. (2015 August, 06): Exploit-Kit Rig: Verbrechen lohnt sich wieder

URL: <http://www.heise.de/newsticker/meldung/Exploit-Kit-Rig-Verbrechen-lohnt-sich-wieder-2772951.html>

last requested 02.07.2016

* Ransomware:

Ransomware is malware used to blackmail a target person or company. The Malware encrypts fragments or the whole target system and promises to make decryption possible after ransom money is payed. Usually the ransom is payed as bitcoins.

One example for Ransomware is the „Chimera“ malware. The Police of Bavaria officially gave warning of this Ransomware in 2015. In the official statement it is said that small to medium-size companies are favoured targets to this malware attack.

Police Bavaria (2015 December, 09): Chimera Schadsoftware legt Unternehmen und Behörden lahm

URL: <https://www.secupedia.info/aktuelles/chimera-schadsoftware-legt-unternehmen-und-behoerden-lahm-5246>

last request 02.07.2016