The spyware that the Britisch and American secret forces used to break in to belgacom was called Regin. It is one of the most complex viruses ever seen.

+ propagation through USB so random node in the graph or a certain node Trageted attack

+ We want to focus on APT’s

An APT is a targeted cyberattack that will keep trying to break into the targeted system. It will try to stay unnoticed for as long as possible. Bruce Schneier describes an APT as something different and stronger than a conventional hacker:

“A conventional hacker or criminal isn’t interested in any particular target. He wants a thousand credit card numbers for fraud, or to break into an account and turn it into a zombie, or whatever. Security against this sort of attacker is relative; as long as you’re more secure than almost everyone else, the attackers will go after other people, not you. An APT is different; it’s an attacker who – for whatever reason – wants to attack you. Against this sort of attacker, the absolute level of your security is what’s important. It doesn’t matter how secure you are compared to your peers; all that matters is whether you’re secure enough to keep him out.” - [Bruce Schneier: APT is a Useful Buzzword.](http://www.schneier.com/blog/archives/2011/11/advanced_persis.html)

An APT is the abbreviation of an Advanced Persistent Attack.

Advanced: ..

Persistent: …

Attack: ..

Soorten APT’s

Regin, Equation, Flame, Stuxnet

Stuxnet: over 100.000 – 300.000 targets

First known example: 2007. Discovery in June 2010. Inactive since 2012

Type Worm. Way of Propagation was through USB drives, LAN spreading and File infection. The **purpose was Cybersabotage. The worm exploited four separate zero-day vulnerabilities. It helped to hide the malware in the system and on infected USB devices to support rootkit functionality.**

Equation: over 500 to 1000 targets

First known example 2002, type complex cyberattack platform, discovery 2014, status ongoing

Propagation: Exploits, USB drives, self replication, physical media, cd roms

Purpose Cyberespionage, data theft, surveillance.

Special features: ability to infect hard drive firmware. Use of interdiction technique to infect victims

Regin

First known sample: 2003, discovery 2012, status active. Type: Trojan, rootkit, complex cyberplatform. Number of targets 11-100. Way of propagation:unknown. Cyberespionage. Remote control.

* Regin – the first cyber-attack platform known to penetrate and monitor GSM networks in addition to other “standard” spying tasks.
* One particular Regin module is capable of monitoring GSM base station controllers, collecting data about GSM cells and the network infrastructure.
* The Regin platform uses an incredibly complex communication method between infected networks and command and control servers, allowing remote control and data transmission by stealth.
* Specific Regin targets include individuals involved in advanced mathematical/cryptographical research

<https://apt.securelist.com/#secondPage/attack=12>

STATUS:Inactive since 2012

TYPE:Complex cyberattack platform

DISCOVERY:May 2012

TARGETED PLATFORMS:Windows

FIRST KNOWN SAMPLE:2007

NUMBER OF TARGETS:500-1,000

THE WAY  
OF PROPAGATION

* USB drives
* LAN spreading

PURPOSE/  
FUNCTIONS

* Cyberespionage

SPECIAL  
FEATURES

* A complex attack toolkit with worm-like features
* An uncharacteristically large program for malware at 20 megabytes. Flame is about 20 times larger than Stuxnet, comprising many different attack and cyberespionage features
* It was signed with a fraudulent certificate purportedly from the Microsoft Enforced Licensing Intermediate PCA certificate authority.
* It is written partly in the Lua scripting language, which is uncommon in malware

Intrusion kill chain uitleggen en waar ge kunt verdedigen. Kill chains give us a guideline but recent APT go far beyond this kill chain so not the only focus.

Conclusion:

We focussen ons op APT’s die zich via een combinatie van usb sticks en exploits, social engineering gaan verplaatsen.

In de kill chain willen we ze tegenhouden op derde moment proberen tegen te houden.