FFF: Flame&Family Friends - Gamesec speech

When Stuxnet was discovered in 2010, everyone wondered if it was one of a kind, or, if there are others like it out there. We suspected there were others, but we had no proof. Every single anti-malware company in the world scoured their collections for samples similar to Stuxnet - without success.

The theory was confirmed in September 2011, when the Duqu malware was discovered and announced by the Hungarian CrySyS lab and Symantec. Duqu is a spy trojan, created on top of the same platform as Stuxnet - which we are now calling the “Tilded” platform, because of the preference of its authors for using filenames started with “~d”.

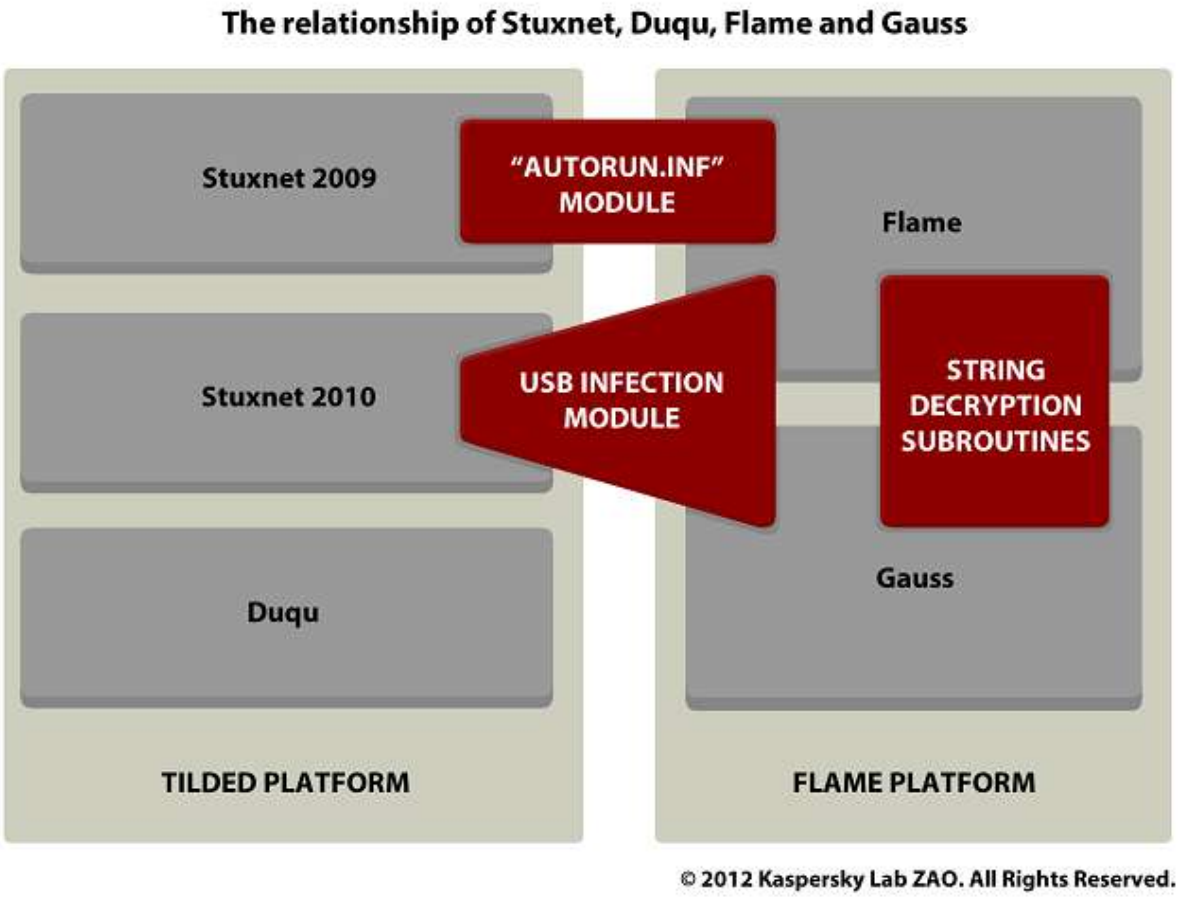
For sure, Duqu and Stuxnet raised the stakes for cyberwar -- but with the discovery of Flame in May 2012, new bars have been raised. The Flame cyber-espionage worm came to the attention of the experts at Kaspersky Lab after the United Nation’s International Telecommunication Union asked for help finding an unknown piece of malware nicknamed Wiper. While searching for Wiper, Kaspersky Lab discovered Worm.Win32.Flame.

Flame is a sophisticated attack toolkit that is a lot more complex than Duqu. It is a backdoor, a Trojan, and has worm-like features, allowing it to replicate in a local network and on removable media if it is commanded so by its controller.

For instance, to replicate in local networks, Flame uses a unique “God mode” technique, which has long been feared and talked about -- hijacking Windows Update connections and presenting itself as a legitimate, Microsoft-signed update to the victim. To pull off this trick, the Flame operators performed an extraordinary collision attack on MD5, which currently remains unknown.

Once a system is infected, Flame begins a complex set of operations, including sniffing the network traffic, taking screenshots, recording audio conversations and intercepting keyboard strokes. All this data is available to the operators through the link to Flame’s command-and-control servers. Later, the operators can choose to upload further modules, which extend Flame’s functionality. We have so far seen about 20 modules and the purpose of some of these is still being investigated.

Once again, the security industry wondered - Stuxnet, Duqu, Flame - are these all, or there are more military-grade malware out there? With the recent discovery of Gauss, we can confirm yet another spy trojan created in the same 'factory' as Flame, Duqu and Stuxnet. We are only seeing just a small picture of all the nation-state sponsored malware attacks that are crawling in the wild.



Talking points:

- A close look at Flame's operation, modules and architecture
- The Flame C2 servers
- Links with Stuxnet, Duqu and Gauss
- Sinkholing Flame
- Working with CERTs and other non-profit orgs
- Sharing information in a timely manner
- Lessons learned

Finally, we will talk about the future of cyber-weapons and the challenges and dangers they pose to civilians, researchers, anti-malware companies and nation-states.