enisa
European Network
and Information
Security Agency

The threat from Flamer

Flamer, a state of the art spying virus, reminds us of the weaknesses in our cyber defences.

The threat from Flamer

Flamer, according to technical analyses of various security teams, is a stealthy information stealer hitting hundreds of targeted PC users across the Middle East. Though, there is no direct threat for the vast majority of users, Flamer serves as an opportunity to learn about the threats we are facing and as a reminder to continue improving cyber security across Europe.

A week ago (end of May 2012) a number of security teams (the Iranian CERT, the Hungarian CERT, and Kaspersky) announced that they had discovered a new Trojan for Windows PCs, referred to as Flamer. According to antivirus companies, Flamer has infected a relatively small number of personal computers (100-1000) in the Middle East (see below the map of most infected countries, as reported by Kaspersky). The software architecture (modular, extensible, modifiable) shows that the attackers had planned to use this virus (platform) for a while.

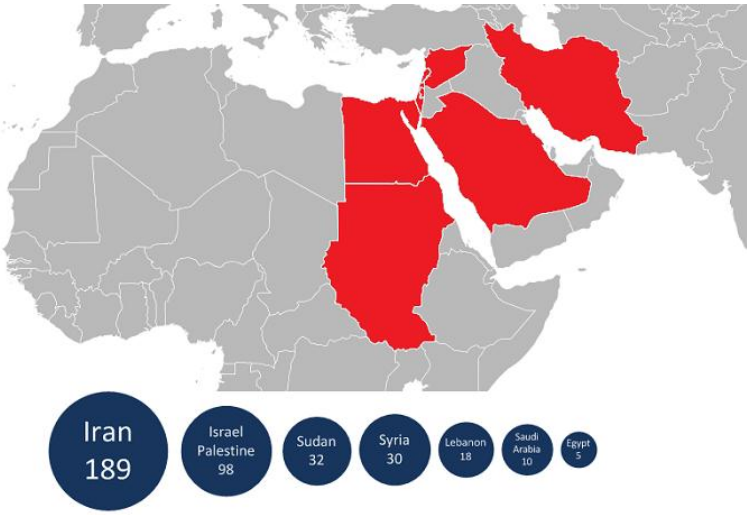

Figure 1: Map of the most infected countries

Flamer showcases a comprehensive set of spying tools and has tools for exfiltrating documents, tapping phone calls, online chats, internet browsing, Bluetooth scanning, and so on. It has been argued that Flamer is more complex and more sophisticated than Stuxnet and Duqu. Flamer exploits security weaknesses smartly to stay undetected. It has been argued that Flamer was hiding in plain sight, 20MB, looking like business software. Mika Hyponen from F-Secure, explained that Flamer had already been seen and filed back in 2010 and 2011, but that it was not recognised as a threat.

From an information security perspective we would like to highlight some key issues:

- **Attribution is difficult:** Media and experts are discussing and speculating about who is behind Flamer. We would like to stress that attribution of cyber attacks is difficult. It is relatively easy for attackers to hide traces, or to leave fake traces to divert attention to someone else. Considering the complexity and size of the Flamer code it may be assumed that the perpetrators have significant resources and are well organized. This could point to organized crime groups or national intelligence services. Flamer looks like an espionage tool (stealing documents, eavesdropping on phone calls, chats etc.) targeted at PC users in the Middle East, the perpetrator possibly has political interests.

- **Extensible virus platform:** The architecture of Flamer is highly modifiable and extensible in the sense that the attacker can easily change how it spreads and what it does. This kind of extensibility and modifiability is seen more and more often. A good example is Zeus which has been around since 2007 and is still infecting millions of PCs across the globe. Zeus is often described as a $1000 DIY virus kit, allowing even relative amateurs to quickly make a custom virus which is difficult to detect with consumer antivirus software. This set up is a way for attackers to continue to make use of their malware tools and infrastructure, beyond the moment of detection by antivirus companies or the patching of software vulnerabilities in computer systems.

- **State of the art:** Flamer uses some advanced techniques to hide and do its work. Flamer is packed with information stealing capabilities (it listens to microphones, other Bluetooth devices, takes screenshots from messaging programs, intercepts internet traffic, and more). While none of these features are particularly new, it is rare to see all these functions together in one virus. Flamer also exploits a well-known weakness in an old cryptographic hash function[1] to masquerade as a legitimate Windows update.

- **Targeted attack:** Flamer has been infecting PCs for up to two years. It appears that its spread and use has been targeted. This is part of a general trend in cyber-attacks, where attackers target specific small groups or individuals to get maximum impact and to avoid drawing attention from antivirus companies. Massive widespread virus attacks are becoming less effective and targeted attacks should be a top concern.

[1] MD5, despite numerous articles and warnings about the weaknesses of this hash function, is still widespread across both modern and legacy IT systems.

Weaknesses in our cyber defences

Flamer is generating a lot of media attention for two main reasons. Firstly, the Middle East is a politically tense region where new technologies are playing multiple roles which include the use of both small and large cyber-attacks. Secondly, experts are impressed by the sophistication of the virus. Flamer showcases the state of the art in malware techniques and also the extensive resources and skills some cyber attackers have.

Unless normal criminals find a way to hijack Flamer, most users will not have much to fear from it, as noted by BSI – and one could even argue that the threat from Flamer is exaggerated by the media. The number of infected PCs can after all be counted in the hundreds while millions of PCs of common users are being infected by very mundane cyber-attacks aimed at stealing money.

However, the threat from Flamer does illustrate important weaknesses in our cyber defences. While we have defence mechanisms for large-scale phishing and email scams, based on collective spam filters and anomaly detection, we are vulnerable to targeted phishing emails (see for example the spear-phishing attacks on global energy companies). Signature-based anti-virus products can protect a large number of consumers from common widespread viruses, but cannot keep sophisticated targeted attacks at bay, as Hyponen argued.

While targeted attacks may not be a big threat for ordinary consumers, and out of scope of consumer antivirus products, such threats do pose a real threat for critical infrastructure and critical services. An attack like Flamer could well be mounted on the EU's critical infrastructure and services. Flamer should serve as a reminder to continue to improve the resilience of critical infrastructure and services, not only to weather physical disasters or system failures, but also to withstand and respond to cyber-attackers with advanced skills and vast resources.

This starts with the identification and analysis of emerging trends and threats. Information about successful attacks, when disclosed to the public, makes us more aware of how vulnerable we are to cyber attacks on our IT systems, but there is not enough information about all the incidents. ENISA has previously highlighted that we need to move from a situation in which we make decisions reacting to attacks to a situation in which we make decision informed by better information about threats. ENISA is working with Member States to start gathering better information about threat, for example through assisting in the implementation of Article 13 of the Telecom reform.

Secondly, when attacks do happen, it is important that there are effective response capabilities in place. ENISA is working with Computer Emergency Response Teams (CERTs) across Europe to handle cyber incidents. On a large scale, ENISA is working to improve the national, Pan-European and Trans-Atlantic contingency and crisis coordination capabilities, for example by facilitating exercises such as the second Pan-European cyber exercise, Cyber Europe 2012, which will be conducted in the autumn.

The EU Member States, ENISA and the EU are collaborating to address cyber security in general – for example, many EU countries have developed cyber security strategies and are focussing on the protection of critical information infrastructure and services. The EU CIIP action plan and the upcoming European Strategy for Internet Security are key initiatives to improve collaboration on cyber security issues and to improve cyber security across the EU, and in particular the EU's critical information infrastructure.

Annex: Further information about Flamer

A number of security teams have published technical analysis of Flamer, aka Skywiper:

- Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East
- SKyWIper: A complex malware for targeted attacks
- Cyber Espionage Reaches New Levels with Flamer
- http://arstechnica.com/security/2012/06/flame-wields-rare-collision-crypto-attack/
- http://arstechnica.com/security/2012/06/flame-malware-was-signed-by-rogue-microsoft-certificate/
- http://blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx?Redirected=true
- http://www.symantec.com/connect/blogs/w32flamer-enormous-data-collection
- http://blogs.mcafee.com/mcafee-labs/spreading-the-flame-skywiper-employs-windows-update

References from several CERT teams around Europe

- http://www.cert.at/services/blog/20120531174118-234.html
- http://www.cert.fi/tietoturvanyt/2012/05/ttn201205291651.html
- http://www.cert.si/obvestila/obvestilo/article/ze-tretji-kiber-udarec-iranu.html
- https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=3092%3Ael-codigo-malicioso-flame-considerado-uno-de-los-mas-sofisticados&catid=5&Itemid=197&lang=en
- http://www.cert.se/publikationer/namnvart/flames-en-industriell-dammsugare-som-samlar-upp-kaenslig-information

References from antivirus companies

- http://www.symantec.com/security_response/writeup.jsp?docid=2012-053007-0702-99&om_rssid=sr-mixed30days
- http://blogs.mcafee.com/mcafee-labs/jumping-in-to-the-flames-of-skywiper
- http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=1195098
- http://www.f-secure.com/weblog/archives/00002371.html
- http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat
- http://www.mcafee.com/us/about/skywiper.aspx