Overview of The Flame

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

Overview of The Flame

The Flame (Da Flame) was discovered in 2012 in the Middle East Countries attacks computers running the Microsoft Windows operating system. According to (1), Flame has been operating since at least 2010. Its highly modular design allows Flame's controller to add additional components and capabilities. The Flame uses advanced compromise techniques and various known vulnerabilities to exploit and maintain access to the system.

According to (2), the Flame weighs 20 MB (all components sum up) which is big compared to other malware (Stuxnet only weighs hundreds of kilobytes). Flame is sophisticated because it can record audio, capture screen, and transmit visual data. Furthermore, it can steal information from the input boxes and password fields (even when they are hidden behind asterisks). Also, it can scan for locally visible Bluetooth devices if a Bluetooth adapter is attached to the local system.

How the Flame is Loaded onto Computers

According to (3), because the Flame is too big, it was loaded into the system in pieces. The first component is about 6 megabytes and contains half a dozen other compressed modules. Then it will decompress the other modules and install them in various places on the hard disk.

Kaspersky describes the Flame as a backdoor with a worm-like feature. Even though the initial point of entry of the Flame is unknown, it can spread through USB sticks or local networks (3).

Capabilities Future Versions of Flame

With the ability to self-contain, record, send and self-destruct all information of the infected devices (and other Bluetooth devices nearby) secretly. The Flame seems very advance in its structure and design. To make it a better design, we can make it lighter (a few GBs instead of

20), and make it self-contain against the most advanced anti-virus applications and strategies.

With all that in mind, the ‘Flame’ is considered the most dangerous and complex virus (in 2012).

It has proved it is sophisticated in cyber-warfare and a game changer in conventional wars.

References

Chapple, M., & Seidl, D. (2023). Chapter 1: Information as a Military Asset. In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 9–20). essay, Jones & Bartlett Learning. (1)

Wikipedia (n.d.). *Flame(malware).* Retrieved from https://en.wikipedia.org/wiki/Flame_%28malware%29

RT (2012). *'Flame' Virus explained: How it Works and Who's Behind it.* Retrieved from https://www.rt.com/news/flame-virus-cyber-war-536/ (2)

Newman, J., (2012). *The Flame Virus: Your FAQ Answered.* Retrieved from https://www.pcworld.com/article/464882/the_flame_virus_your_faqs_answered.html (3)