Flame (malware)

By Contributors to Wikimedia projects

Published: 2012-05-28 · Archived: 2026-04-05 17:57:42 UTC

From Wikipedia, the free encyclopedia

"Skywiper" redirects here. For the portable anti-drone device, see EDM4S.

Flame	
Malware details	
Aliases	Flamer, sKyWIper, Skywiper
Type	Malware
Author	Equation Group
Technical details	
Platform	Windows
Size	20 MB
Written in	C++, Lua

Flame,[a] also known as **Flamer**, **sKyWIper**,[b] and **Skywiper**,[2] is modular computer malware discovered in 2012[3][4] that attacks computers running the Microsoft Windows operating system.[5] The program is used for targeted cyber espionage in Middle Eastern countries.[1][5][6]

Its discovery was announced on 28 May 2012 by the MAHER Center of the Iranian National Computer Emergency Response Team (CERT),[5] Kaspersky Lab[6] and CrySyS Lab of the Budapest University of Technology and Economics.[1] The last of these stated in its report that Flame "is certainly the most sophisticated malware we encountered during our practice; arguably, it is the most complex malware ever found."[1] Flame can spread to other systems over a local area network (LAN). It can record audio, screenshots, keyboard activity and network traffic.[6] The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices.[7] This data, along with locally stored documents, is sent on to one of several command and control servers that are scattered around the world. The program then awaits further instructions from these servers.[6]

According to estimates by Kaspersky in May 2012, Flame had initially infected approximately 1,000 machines,[7] with victims including governmental organizations, educational institutions and private individuals.[6] At that time

65% of the infections happened in Iran, Israel, Palestine, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt,[3][6] with a "huge majority of targets" within Iran.[8] Flame has also been reported in Europe and North America.[9] Flame supports a "kill" command which wipes all traces of the malware from the computer. The initial infections of Flame stopped operating after its public exposure, and the "kill" command was sent.[10]

Flame is linked to the Equation Group by Kaspersky Lab. However, Costin Raiu, the director of Kaspersky Lab's global research and analysis team, believes the group only cooperates with the creators of Flame and Stuxnet from a position of superiority: "Equation Group are definitely the masters, and they are giving the others, maybe, bread crumbs. From time to time they are giving them some goodies to integrate into Stuxnet and Flame."[11]

Recent research has indicated that Flame is positioned to be remembered as one of the most significant and intricate cyber-espionage tools in history. Using a sophisticated strategy, Flame managed to penetrate numerous computers across the Middle East by falsifying an authentic Microsoft security certificate.[12]

In 2019, researchers Juan Andres Guerrero-Saade and Silas Cutler announced their discovery of the resurgence of Flame.[13][14] The attackers used 'timestomping' (changing timestamps and dates of files) to make the new samples look like they were created before the 'suicide' command. However, a compilation error included the real compilation date (c. 2014). The new version (dubbed 'Flame 2.0' by the researchers) includes new encryption and obfuscation mechanisms to hide its functionality.[15]

Flame (a.k.a. Da Flame) was identified in May 2012 by the MAHER Center of the Iranian National CERT, Kaspersky Lab and CrySyS Lab (Laboratory of Cryptography and System Security) of the Budapest University of Technology and Economics when Kaspersky Lab was asked by the United Nations International Telecommunication Union to investigate reports of a virus affecting Iranian Oil Ministry computers.[7] As Kaspersky Lab investigated, they discovered an MD5 hash and filename that appeared only on customer machines from Middle Eastern nations. After discovering more pieces, researchers dubbed the program "Flame" after one of the main modules inside the toolkit [FROG.DefaultAttacks.A-InstallFlame].[7]

According to Kaspersky, Flame had been operating in the wild since at least February 2010.[6] CrySyS Lab reported that the file name of the main component was observed as early as December 2007.[1] However, its creation date could not be determined directly, as the creation dates for the malware's modules are falsely set to dates as early as 1994.[7]

Computer experts consider it the cause of an attack in April 2012 that caused Iranian officials to disconnect their oil terminals from the Internet.[16] At the time the Iranian Students News Agency referred to the malware that caused the attack as "Wiper", a name given to it by the malware's creator.[17] However, Kaspersky Lab believes that Flame may be "a separate infection entirely" from the Wiper malware.[7] Due to the size and complexity of the program—described as "twenty times" more complicated than Stuxnet—the Lab stated that a full analysis could require as long as ten years.[7]

On 28 May, Iran's CERT announced that it had developed a detection program and a removal tool for Flame, and had been distributing these to "select organizations" for several weeks.[7] After Flame's exposure in news media, Symantec reported on 8 June that some Flame command and control (C&C) computers had sent a "suicide"

command to infected PCs to remove all traces of Flame.[10] All copies of the program and any related files were deleted.[18]

According to estimates by Kaspersky in May 2012, initially Flame had infected approximately 1,000 machines,[7] with victims including governmental organizations, educational institutions and private individuals.[6] At that time the countries most affected were Iran, Israel, the Palestinian Territories, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt.[3][6] A sample of the Flame malware is available at GitHub.

List of code names for various families of modules in Flame's source code and their possible purpose[1]

Name	Description
Flame	Modules that perform attack functions
Boost	Information gathering modules
Flask	A type of attack module
Jimmy	A type of attack module
Munch	Installation and propagation modules
Snack	Local propagation modules
Spotter	Scanning modules
Transport	Replication modules
Euphoria	File leaking modules
Headache	Attack parameters or properties

Flame is an uncharacteristically large program for malware at 20 megabytes. It is written partly in the Lua scripting language with compiled C++ code linked in, and allows other attack modules to be loaded after initial infection.[6][19] The malware uses five different encryption methods and an SQLite database to store structured information.[1] The method used to inject code into various processes is stealthy, in that the malware modules do not appear in a listing of the modules loaded into a process and malware memory pages are protected with READ, WRITE and EXECUTE permissions that make them inaccessible by user-mode applications.[1] The internal code has few similarities with other malware, but exploits two of the same security vulnerabilities used previously by Stuxnet to infect systems.[c][1] The malware determines what antivirus software is installed, then customises its own behaviour (for example, by changing the filename extensions it uses) to reduce the probability of detection by that software.[1] Additional indicators of compromise include mutex and registry activity, such as installation of a fake audio driver which the malware uses to maintain persistence on the compromised system.[19]

Flame is not designed to deactivate automatically, but supports a "kill" function that makes it eliminate all traces of its files and operation from a system on receipt of a module from its controllers.[7]

Flame was signed with a fraudulent certificate purportedly from the Microsoft Enforced Licensing Intermediate PCA certificate authority.[20] The malware authors identified a Microsoft Terminal Server Licensing Service certificate that inadvertently was enabled for code signing and that still used the weak MD5 hashing algorithm, then produced a counterfeit copy of the certificate that they used to sign some components of the malware to make them appear to have originated from Microsoft.[20] A successful collision attack against a certificate was previously demonstrated in 2008,[21] but Flame implemented a new variation of the chosen-prefix collision attack.[22]

Property	Value

Like the previously known cyber weapons Stuxnet and Duqu, it is employed in a targeted manner and can evade current security software through rootkit functionality. Once a system is infected, Flame can spread to other systems over a local network or via USB stick. It can record audio, screenshots, keyboard activity and network traffic.[6] The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth enabled devices.[7] This data, along with locally stored documents, is sent on to one of several command and control servers that are scattered around the world. The program then awaits further instructions from these servers.[6]

Unlike Stuxnet, which was designed to sabotage an industrial process, Flame appears to have been written purely for espionage.[23] It does not appear to target a particular industry, but rather is "a complete attack toolkit designed for general cyber-espionage purposes".[24]

Using a technique known as sinkholing, Kaspersky demonstrated that "a huge majority of targets" were within Iran, with the attackers particularly seeking AutoCAD drawings, PDFs, and text files.[8] Computing experts said that the program appeared to be gathering technical diagrams for intelligence purposes.[8]

A network of 80 servers across Asia, Europe and North America has been used to access the infected machines remotely.[25]

On 19 June 2012, *The Washington Post* published an article claiming that Flame was jointly developed by the U.S. National Security Agency, CIA and Israel's military at least five years prior. The project was said to be part of a classified effort code-named Olympic Games, which was intended to collect intelligence in preparation for a cyber-sabotage campaign aimed at slowing Iranian nuclear efforts.[26]

According to Kaspersky's chief malware expert, "the geography of the targets and also the complexity of the threat leaves no doubt about it being a nation-state that sponsored the research that went into it."[3] Kaspersky initially said that the malware bears no resemblance to Stuxnet, although it may have been a parallel project commissioned by the same attackers.[27] After analysing the code further, Kaspersky later said that there is a strong relationship between Flame and Stuxnet; the early version of Stuxnet contained code to propagate via USB drives that is nearly identical to a Flame module that exploits the same zero-day vulnerability.[28]

Iran's CERT described the malware's encryption as having "a special pattern which you only see coming from Israel".[29] *The Daily Telegraph* reported that due to Flame's apparent targets—which included Iran, Syria, and the

West Bank—Israel became "many commentators' prime suspect". Other commentators named the U.S. as possible perpetrators.[27] Richard Silverstein, a commentator critical of Israeli policies, claimed that he had confirmed with a "senior Israeli source" that the malware was created by Israeli computer experts.[27] *The Jerusalem Post* wrote that Israel's Vice Prime Minister Moshe Ya'alon appeared to have hinted that his government was responsible,[27] but an Israeli spokesperson later denied that this had been implied.[30] Unnamed Israeli security officials suggested that the infected machines found in Israel may imply that the virus could be traced to the U.S. or other Western nations.[31] The U.S. has officially denied responsibility.[32]

A leaked NSA document mentions that dealing with Iran's discovery of FLAME is an NSA and GCHQ jointly-worked event.[33]

- Cybercrime
- Cyberwarfare
- Cyber security standards
- Cyberterrorism
- Digital privacy
- Operation High Roller

1. ^ "Flame" is one of the strings found in the code, a common name for attacks, most likely by exploits[1]
2. ^ The name "sKyWIper" is derived from the letters "KWI" which are used as a partial filename by the malware[1]
3. ^ MS10-061 and MS10-046

1. ^ Jump up to: **a** **b** **c** **d** **e** **f** **g** **h** **i** **j** **k** *"sKyWIper: A Complex Malware for Targeted Attacks"* (PDF). *Budapest University of Technology and Economics*. *28 May 2012. Archived from the original (PDF) on 28 May 2012. Retrieved 29 May 2012.*
2. ^ *"Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East"*. *Symantec. Archived from the original on 31 May 2012. Retrieved 30 May 2012.*
3. ^ Jump up to: **a** **b** **c** **d** *Lee, Dave (28 May 2012). "Flame: Massive Cyber-Attack Discovered, Researchers Say". BBC News. Archived from the original on 30 May 2012. Retrieved 29 May 2012.*
4. ^ *McElroy, Damien; Williams, Christopher (28 May 2012). "Flame: World's Most Complex Computer Virus Exposed". The Daily Telegraph. Archived from the original on 30 May 2012. Retrieved 29 May 2012.*
5. ^ Jump up to: **a** **b** **c** *"Identification of a New Targeted Cyber-Attack". Iran Computer Emergency Response Team. 28 May 2012. Archived from the original on 29 May 2012. Retrieved 29 May 2012.*
6. ^ Jump up to: **a** **b** **c** **d** **e** **f** **g** **h** **i** **j** **k** **l** *Gostev, Alexander (28 May 2012). "The Flame: Questions and Answers". Securelist. Archived from the original on 30 May 2012. Retrieved 16 March 2021.*
7. ^ Jump up to: **a** **b** **c** **d** **e** **f** **g** **h** **i** **j** **k** *Zetter, Kim (28 May 2012). "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers". Wired. Archived from the original on 30 May 2012. Retrieved 29 May 2012.*
8. ^ Jump up to: **a** **b** **c** *Lee, Dave (4 June 2012). "Flame: Attackers 'sought confidential Iran data'". BBC News. Archived from the original on 4 June 2012. Retrieved 4 June 2012.*

9. ^ *Murphy, Samantha (5 June 2012). "Meet Flame, the Nastiest Computer Malware Yet". Mashable.com. Archived from the original on 8 June 2012. Retrieved 8 June 2012.*
10. ^ Jump up to: ***a*** ***b*** *"Flame malware makers send 'suicide' code". BBC News. 8 June 2012. Archived from the original on 24 August 2012. Retrieved 8 June 2012.*
11. ^ *Kaspersky Labs Global Research & Analysis Team (16 February 2015). "Equation: The Death Star of Malware Galaxy". SecureList. Archived from the original on 17 February 2015,* Costin Raiu (director of Kaspersky Lab's global research and analysis team): "It seems to me Equation Group are the ones with the coolest toys. Every now and then they share them with the Stuxnet group and the Flame group, but they are originally available only to the Equation Group people. Equation Group are definitely the masters, and they are giving the others, maybe, bread crumbs. From time to time they are giving them some goodies to integrate into Stuxnet and Flame."
12. ^ *Munro, Kate (1 October 2012). "Deconstructing Flame: the limitations of traditional defences". Computer Fraud & Security.* ***2012*** *(10): 8–11. doi:10.1016/S1361-3723(12)70102-1. ISSN 1361-3723.*
13. ^ *Zetter, Kim (9 April 2019). "Researchers Uncover New Version of the Infamous Flame Malware". Vice.com. Vice Media. Retrieved 6 August 2020.*
14. ^ *Chronicle Security (12 April 2019). "Who is GOSSIPGIRL?". Medium. Archived from the original on 22 July 2020. Retrieved 15 July 2020.*
15. ^ *Guerrero-Saade, Juan Andres; Cutler, Silas (9 April 2019). Flame 2.0: Risen from the Ashes (PDF) (Report). Chronicle Security. Archived (PDF) from the original on 1 June 2023. Retrieved 17 May 2024.*
16. ^ *Hopkins, Nick (28 May 2012). "Computer Worm That Hit Iran Oil Terminals 'Is Most Complex Yet'". The Guardian. Archived from the original on 31 May 2012. Retrieved 29 May 2012.*
17. ^ *Erdbrink, Thomas (23 April 2012). "Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet". The New York Times. Archived from the original on 31 May 2012. Retrieved 29 May 2012.*
18. ^ *"Flame". www.radware.com. Retrieved 25 September 2024.*
19. ^ Jump up to: ***a*** ***b*** *Kindlund, Darien (30 May 2012). "Flamer/sKyWIper Malware: Analysis". FireEye. Archived from the original on 2 June 2012. Retrieved 31 May 2012.*
20. ^ Jump up to: ***a*** ***b*** *"Microsoft releases Security Advisory 2718704". Microsoft. 3 June 2012. Archived from the original on 7 June 2012. Retrieved 4 June 2012.*
21. ^ *Sotirov, Alexander; Stevens, Marc; Appelbaum, Jacob; Lenstra, Arjen; Molnar, David; Osvik, Dag Arne; de Weger, Benne (30 December 2008). MD5 considered harmful today: creating a rogue CA certificate. 25th Annual Chaos Communication Congress in Berlin. Archived from the original on 25 March 2017. Retrieved 4 June 2011.*
22. ^ *Stevens, Marc (7 June 2012). "CWI Cryptanalist Discovers New Cryptographic Attack Variant in Flame Spy Malware". Centrum Wiskunde & Informatica. Archived from the original on 28 February 2017. Retrieved 9 June 2012.*
23. ^ *Cohen, Reuven (28 May 2012). "New Massive Cyber-Attack an 'Industrial Vacuum Cleaner for Sensitive Information'". Forbes. Archived from the original on 31 May 2012. Retrieved 29 May 2012.*
24. ^ *Albanesius, Chloe (28 May 2012). "Massive 'Flame' Malware Stealing Data Across Middle East". PC Magazine. Archived from the original on 30 May 2012. Retrieved 29 May 2012.*
25. ^ *"Flame virus: Five facts to know". The Times of India. Reuters. 29 May 2012. Retrieved 30 May 2012.* `{{cite news}}` : CS1 maint: deprecated archival service (link)

26. ^ *Nakashima, Ellen (19 June 2012). "U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say". The Washington Post. Archived from the original on 18 July 2012. Retrieved 20 June 2012.*
27. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** *"Flame Virus: Who is Behind the World's Most Complicated Espionage Software?". The Daily Telegraph. 29 May 2012. Archived from the original on 31 May 2012. Retrieved 29 May 2012.*
28. ^ *"Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected". Kaspersky Lab. 11 June 2012. Archived from the original on 16 November 2021. Retrieved 13 June 2012.*
29. ^ *Erdbrink, Thomas (29 May 2012). "Iran Confirms Attack by Virus That Collects Information". The New York Times. Archived from the original on 6 June 2012. Retrieved 30 May 2012.*
30. ^ *Tsukayama, Hayley (31 May 2012). "Flame cyberweapon written using gamer code, report says". The Washington Post. Archived from the original on 2 June 2012. Retrieved 31 May 2012.*
31. ^ *Dareini, Ali Akbar; Murphy, Dan; Satter, Raphael; Federman, Josef (30 May 2012). "Iran: 'Flame' virus fight began with oil attack". Yahoo! News. Associated Press.*
32. ^ *"Flame: Israel rejects link to malware cyber-attack". BBC News. 31 May 2012. Archived from the original on 5 June 2014. Retrieved 3 June 2012.*
33. ^ *"Visit Précis: Sir Iain Lobban, KCMG, CB; Director, Government Communications Headquarters (GCHQ) 30 April 2013 – 1 May 2013" (PDF). Archived (PDF) from the original on 2 May 2014. Retrieved 1 May 2014.*
