

Flame cyber virus linked to more malware: report

September 17 2012

```

IF NOT _params.STD THEN
  ASSERT(!loadstring(config.get("LIB.LIBS.STD"))){}
  IF NOT _params.table_ext THEN
    ASSERT(!loadstring(config.get("LIB.LIBS.table_ext"))){}
  IF NOT _LIB_FLAME_PROPS_LOADED_ THEN
    LIB_FLAME_PROPS_LOADED_ = true
    Flame_props = {}
    Flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    Flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NON_IF_SRES"
    Flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    Flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    Flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "SATON_INTERNET_CH"
    Flame_props.INTERNET_CHECK_KEY = "CONNECTION.TIME"
    Flame_props.SPS_CONFIG = "SATON.LEAK.BANDWIDTH_CALCULATOR.SPS_QUEUE"
    Flame_props.SPS_KEY = "SPS"
    Flame_props.PROXY_SERVER_KEY = "SATON.PROXY_DATA.PROXY_SERVER"
    Flame_props.getFlameId = function()
      IF config.HasKey(Flame_props.FLAME_ID_CONFIG_KEY) THEN
        local I_T_0 = config.get
        local I_T_1 = Flame_props.FLAME_ID_CONFIG_KEY
        return I_T_0(I_T_1)
      end
    end
    return nil
  end
end

```

A Flame computer virus program is pictured in this screen grab released by Russian security firm Kaspersky Lab. The Flame virus believed to be part of a cyberwarfare effort against Iran was developed as early as 2006 and is linked to at least three other malware programs, a new analysis said Monday.

The Flame virus believed to be part of a cyberwarfare effort against Iran was developed as early as 2006 and is linked to at least three other malware programs, a new analysis said Monday.

The report suggests that the effort to develop Flame, widely reported to be part of a US-Israeli effort to slow Iran's suspected [nuclear weapons](#) drive, has been going on longer than initially believed and has more components, including some not yet fully understood.

The report by the Russian [security firm](#) Kaspersky Lab with US-based

Symantec, Germany's computer emergency response team and the [International Telecommunication Union](#)'s cybersecurity arm showed that development of the Flame platform dates back to 2006.

An earlier analysis by Kaspersky had reported the code for Flame, which is likely related to Stuxnet and other viruses, was written in 2009.

Kaspersky said the latest analysis shows that "at least three other Flame-related malicious programs were created" but added that "their nature is currently unknown."

It added that "one of these Flame-related unknown malicious objects is currently operating in the wild."

A Kaspersky statement said development of Flame's Command and Control platform started "as early as December 2006" and was "disguised" to hide its true purpose.

A security blog post by Symantec said that Flame was designed in a way to delete any effort to find its source.

"The systems were configured to disable any unnecessary logging events and entries in the database were deleted at regular intervals," the posting said.

"Existing log files were securely deleted from the server on a regular basis. These steps were taken in order to hamper any investigation should the server be acquired by third parties."

Flame previously has been linked to Stuxnet, which was designed to attack [computer control systems](#) made by German industrial giant Siemens and commonly used to manage water supplies, [oil rigs](#), [power plants](#) and other [critical infrastructure](#).

Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there. The worm was crafted to recognize the system it was to attack.

Some reports say US and Israeli intelligence services collaborated to develop the computer worm to sabotage Iran's efforts to make a nuclear bomb.

(c) 2012 AFP

Citation: Flame cyber virus linked to more malware: report (2012, September 17) retrieved 25 April 2024 from <https://phys.org/news/2012-09-flame-cyber-virus-linked-malware.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.