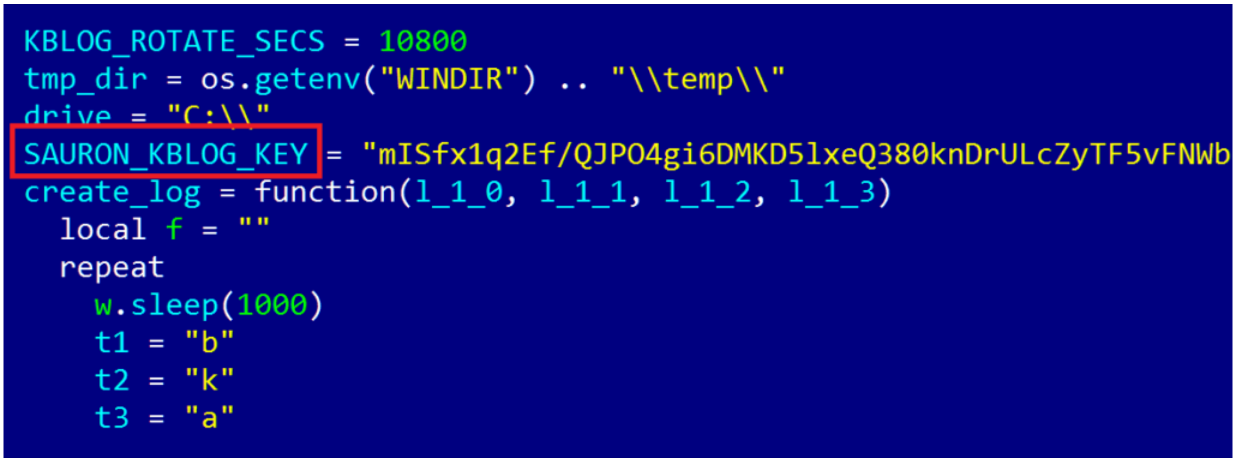
ProjectSuaron: Kaspersky Lab researchers describe espionage platform

August 10 2016, by Nancy Owano



```
KBLOG_ROTATE_SECS = 10800
tmp_dir = os.getenv("WINDIR") .. "\\temp\\"
drive = "C:\\"
SAURON_KBLOG_KEY = "mISfx1q2Ef/QJPO4gi6DMKD5lxeQ380knDrULcZyTF5vFNWb
create_log = function(l_1_0, l_1_1, l_1_2, l_1_3)
  local f = ""
  repeat
    w.sleep(1000)
    t1 = "b"
    t2 = "k"
    t3 = "a"
```

ProjectSauron is a sobering discovery of a type of malware that has been around for years and is regarded as a top level cyber-espionage platform.

Security experts find that the ProjectSauron is using an advanced piece of malware, said *Daily Mail*, called Remsec.

The snoopers have been doing their thing since 2011. A Kaspersky Lab report dated Tuesday (Version 1.02) carries a full discussion of what is going on.

Back story: In September last year, Kaspersky Lab's Anti-Targeted Attack Platform discovered anomalous network traffic in a government organization network.

Looking into this, they discovered "a strange executable program library loaded into the memory of the domain controller server. The library was registered as a Windows password filter and had access to sensitive data such as administrative passwords in cleartext. Additional research revealed signs of activity of a previously unknown threat actor, responsible for largescale attacks against key governmental entities."

Symantec, meanwhile, said there were selected targets in Russia, China, Sweden, and Belgium.

Symantec found evidence of infections in 36 computers across seven separate organizations. The group's targets were in places that included Russia, China, Sweden, and Belgium.

Kaspersky Lab said they found more than 30 infected organizations providing such functions as government, scientific research, telecommunications, military and finance.

The malware focus is intelligence-gathering.

Stealthy is a fitting description, and the snooping has been going on since 2011. The name of the malware is dubbed 'ProjectSauron' and the name, said the Kaspersky Lab report, reflects the fact that the code authors refer to 'Sauron' in the configuration files.

Kaspersky said "Usually APT [Advanced Persistent Threat] campaigns have a geographical nexus, aimed at extracting information within a specific region or from a given industry... Interestingly, ProjectSauron seems to be dedicated to just a couple of countries, focused on collecting high value intelligence by compromising almost all key entities it could possibly reach within the target area."

Symantec noted observations on Remsec.

"Remsec contains a number of stealth features that help it to avoid detection. Several of its components are in the form of executable blobs (Binary Large Objects), which are more difficult for traditional antivirus software to detect, according to Symantec. The security watchers there said that "'In addition to this, much of the malware's functionality is deployed over the network, meaning it resides only in a computer's memory and is never stored on disk."

Symantec posted its blog about this on August 7, saying targets have been mainly organizations and individuals that would be of interest to a nation state's intelligence services. Symantec in its blog said that Remsec "opens a back door on an infected computer, can log keystrokes, and steal files."

Who are the perpetrators? Difficult to answer. Kaspersky Lab said that "Attribution is hard and reliable attribution is rarely possible in cyberspace. Even with confidence in various indicators and apparent attacker mistakes, there is a greater likelihood that these can all be smoke and mirrors created by an attacker with a greater vantage point and vast resources. When dealing with the most advanced threat actors, as is the case with ProjectSauron, attribution becomes an unsolvable problem."

Citation: ProjectSuaron: Kaspersky Lab researchers describe espionage platform (2016, August 10) retrieved 5 May 2024 from https://techxplore.com/news/2016-08-projectsuaron-kaspersky-lab-espionage-platform.html