ProjectSauron APT On Par With Equation, Flame, Duqu

By Michael Mimoso

Published: 2016-08-08 · Archived: 2026-04-06 01:54:32 UTC

ProjectSauron, an APT attack platform, has been used since 2011 to target critical government, financial and communications organizations in a number of countries.

A state-sponsored APT platform on par with Equation, Flame and Duqu has been used since 2011 to spy on government agencies and other critical industries.

Known as ProjectSauron, or Strider, the platform has all the earmarks of advanced attackers who covet stealth, and rely on a mix of zero-day exploits and refined coding to exfiltrate sensitive data, even from air-gapped machines.

Researchers at Kaspersky Lab and Symantec today published separate reports on ProjectSauron, and said large-scale attacks have targeted government agencies, telecommunications firms, financial organizations, military and research centers in Russia, Iran, Rwanda, China, Sweden, Belgium and Italy. Campaigns were still active this year, said researchers at Kaspersky Lab.

While researchers still do not know how the attackers are infiltrating these critical networks, much of their activity on compromised networks has been uncovered.

The attack platform, for example, is modular framework called Remsec that once deployed allows for lateral movement, data theft and the injection of more attack code. To complicate detection and attribution, the attackers customize artifacts used in campaigns to each target, making them less useful as indicators of compromise, Kaspersky Lab said.

The platform, meanwhile, uses a Lua scripting engine to deploy the core platform and its 50 different plugins; a reference to Sauron, the evil villain in *Lord of the Rings* was found in a Lua module. Another hallmark of ProjectSauron is its use of strong encryption algorithms, specifically RC6, RC5, Salsa20 and others.

```
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"
```

“The actor behind ProjectSauron has a high interest in communication encryption software widely used by targeted governmental organizations,” Kaspersky Lab said in its report. “It steals encryption keys, configuration files, and IP addresses of the key infrastructure servers related to the encryption software.”

For persistence, a backdoor module is registered on domain controllers as a Windows Local Security Authority password filter, which is normally used to enforce password policies.

“This way, the ProjectSauron passive backdoor module starts every time any network or local user (including an administrator) logs in or changes a password, and promptly harvests the password in plaintext,” Kaspersky Lab said in its report.

Most of the implants used in the attacks work as backdoors that either install new modules or run commands. Each implant is unique, the Kaspersky Lab report said, with unique file names and sizes and missions such as stealing documents, logging keystrokes or stealing encryption keys from local and attached disks.

Kaspersky Lab said it found 28 command and control domains linked to 11 IP addresses in the United States and a number of European countries. Local CERTs and law enforcement have been notified of the attacks, Kaspersky Lab said.

“The ProjectSauron actor is extremely well prepared when it comes to operational security. Running an expensive cyberespionage campaign like ProjectSauron requires vast domain and server infrastructure uniquely assigned to each victim organization and never reused again. This makes traditional network-based indicators of compromise almost useless because they won’t be reused in any other organization, Kaspersky Lab said in its report. “Even the diversity of ISPs selected for ProjectSauron operations makes it clear that the actor did everything possible to avoid creating patterns.”

The researchers also discovered a module that moves data from air-gapped machines via a removable USB that reserves space on an encrypted partition with its own virtual file system and two directories called “In” and “Out.”

“Once networked systems are compromised, the attackers wait for a USB drive to be attached to the infected machine,” Kaspersky Lab said in its report.

To move data off compromised networks, the attackers use common protocols such as HTTP, TCP, SMTP and others. A plugin was also found that uses DNS to exfiltrate stolen data.

“To avoid generic detection of DNS tunnels at network level, the attackers use it in low-bandwidth mode, which is why it is used solely to exfiltrate target system metadata,” Kaspersky Lab said in its report. “Another interesting feature in ProjectSauron malware that leverages the DNS protocol is the real-time reporting of the operation progress to a remote server. Once an operational milestone is achieved, ProjectSauron issues a DNS-request to a special subdomain unique to each target.”

As for zero-day exploits, none have been discovered, Kaspersky Lab said in its report, but the means by which the attackers are moving data from air-gapped machines indicates there has to be one.

“When penetrating isolated systems, the creation of the encrypted storage area in the USB does not in itself enable attackers to get control of the air-gapped machines. There has to be another component such as a 0day exploit

placed on the main partition of the USB drive," Kaspersky Lab said in its report. "So far we have not found any 0-day exploit embedded in the body of the malware we analyzed, and we believe it was probably deployed in rare, hard-to-catch instances."
