ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms

By GReAT on August 8, 2016. 2:03 pm

PUBLICATIONS

APT CYBER ESPIONAGE NATION STATE SPONSORED ESPIONAGE PROJECTSAURON SPYWARE TARGETED ATTACKS

Download the full report (PDF)

Technical analysis

Indicators of compromise (IOC)

Download YARA rules

More information about ProjectSauron is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

Introduction:

Over the last few years, the number of “APT-related” incidents described in the media has grown significantly. For many of these, though, the designation “APT”, indicating an “Advanced Persistent Threat”, is usually an exaggeration. With some notable exceptions, few of the threat actors usually described in the media are advanced. These exceptions, which in our opinion represent the pinnacle of cyberespionage tools: the truly “advanced” threat actors out there, are Equation, Regin, Duqu or

Careto. Another such an exceptional espionage platform is "ProjectSauron", also known as "Strider".

What differentiates a truly advanced threat actor from a wannabe APT? Here are a few features that characterize the 'top' cyberespionage groups:

- The use of zero day exploits
- Unknown, never identified infection vectors
- Have compromised multiple government organizations in several countries
- Have successfully stolen information for many years before being discovered
- Have the ability to steal information from air gapped networks
- Support multiple covert exfiltration channels on various protocols
- Malware modules which can exist only in memory without touching the disk
- Unusual persistence techniques which sometime use undocumented OS features

"ProjectSauron" easily covers many of these points.

From discovery to detection:

When talking about long-standing cyber-espionage campaigns, many people wonder why it took so long to catch them. Perhaps one of the explanations is having the right tools for the right job. Trying to catch government or military grade malware requires specialized technologies and products. One such product is Kaspersky's AntiTargeted Attacks Platform, KATA (http://www.kaspersky.com/enterprise-security/anti-targeted-attack-platform). In September 2015, our anti-targeted attack technologies caught a previously unknown attack. The suspicious module was an executable library, loaded in the memory of a Windows domain controller (DC). The library was registered as a Windows password filter and had access to sensitive data in cleartext. Additional research revealed signs of massive activity from a new threat actor that we codenamed 'ProjectSauron', responsible for large-scale attacks against key governmental entities in several countries.

```
KBLOG_ROTATE_SECS = 10800
tmp_dir = os.getenv("WINDIR") .. "\\temp\\"
drive = "C:\\"
SAURON_KBLOG_KEY = "mISfx1q2Ef/QJPO4gi6DMKD51xeQ380knDrULcZyTF5vFNWb
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"
```

"SAURON" – internal name used in the LUA scripts

ProjectSauron comprises a top-of-the-top modular cyber-espionage platform in terms of technical sophistication, designed to enable long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods. Technical details show how attackers learned from other extremely advanced actors in order to avoid repeating their mistakes. For example, all artifacts are customized per given target, reducing their value as indicators of compromise for any other victim.

Some other key features of ProjectSauron:

- It is a modular platform designed to enable long-term cyber-espionage campaigns.
- All modules and network protocols use strong encryption algorithms, such as RC6, RC5, RC4, AES, Salsa20, etc.
- It uses a modified LUA scripting engine to implement the core platform and its plugins.
- There are upwards of 50 different plugin types.
- The actor behind ProjectSauron has a high interest in communication encryption software widely used by targeted governmental organizations. It steals encryption keys, configuration files, and IP addresses of the key infrastructure servers related to the encryption software.
- It is able to exfiltrate data from air-gapped networks by using specially-prepared USB storage drives where data is stored in an area invisible to the operation system.
- The platform makes extensive use of the DNS protocol for data exfiltration and real-time status reporting.
- The APT was operational as early as June 2011 and remained active until April 2016.
- The initial infection vector used to penetrate victim networks remains unknown.
- The attackers utilize legitimate software distribution channels for lateral movement within infected networks.

To help our readers better understand the ProjectSauron attack

platform, we've prepared an FAQ which brings together some of the most important points about this attacker and its tools. A brief technical report is also available, including IOCs and Yara rules.

Our colleagues from Symantec have also released their analysis on ProjectSauron / Strider. You can read it here: http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

ProjectSauron FAQ:

1. What is ProjectSauron?

ProjectSauron is the name for a top level modular cyber-espionage platform, designed to enable and manage long-term campaigns through stealthy survival mechanisms coupled with multiple exfiltration methods.

Technical details show how attackers learned from other extremely advanced actors in order to avoid repeating their mistakes. As such, all artifacts are customized per given target, reducing their value as indicators of compromise for any other victim.

Usually APT campaigns have a geographical nexus, aimed at extracting information within a specific region or from a given industry. That usually results in several infections in countries within that region, or in the targeted industry around the world. 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.

The name, ProjectSauron reflects the fact that the code authors refer to 'Sauron' in the LUA scripts.

2. Who are the victims?

Using our telemetry, we found more than 30 infected organizations in Russia, Iran, Rwanda and possibly in Italian-speaking countries as well. Many more organizations and geographies are likely to be affected.

The attacked organizations are key entities that provide core

state functions:

- Government
- Scientific research centers
- Military
- Telecommunication providers
- Finance

3. Have you notified victims?

As usual, Kaspersky Lab actively collaborates with industry partners, CERTs and law enforcement agencies to notify victims and help to mitigate the threat. We also rely on public awareness to spread information about it. If you need more information about this actor, please contact intelreports@kaspersky.com.

4. For how long have the attackers been active?

Forensic analysis indicates that the APT has been operational since at least June 2011 and was still active in 2016. Although it appears to have largely ceased, there is a chance that it is still active on computer systems that are not covered by Kaspersky Lab solutions.

5. Did the attackers use interesting or advanced techniques?

The attackers used multiple interesting and unusual techniques, including:

- Data exfiltration and real-time status reporting using DNS requests.
- Implant deployment using legitimate software update scripts.
- Data exfiltration from air-gapped networks through the use of specially prepared USB storage drives where the stolen data is stored in the area unused by standard tools of the operating system.
- Using a modified LUA scripting engine to implement the core platform and its plugins. The use of LUA components in malware is very rare – it was previously spotted in the Flame and Animal Farm attacks.

6. How did you discover this malware?

In September 2015, Kaspersky Lab's Anti-Targeted Attack Platform discovered anomalous network traffic in a client organization's network. Analysis of this incident led to the discovery of 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.

7. How does ProjectSauron operate?

ProjectSauron usually registers its persistence module on domain controllers as a Windows LSA (Local Security Authority) password filter. This feature is typically used by system administrators to enforce password policies and validate new passwords to match specific requirements, such as length and complexity. 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.

In cases where domain controllers lack direct Internet access, the attackers install additional implants on other local servers which have both local network and Internet access and may pass through significant amount of network traffic, i.e. proxy-servers, web-servers, or software update servers. After that, these intermediary servers are used by ProjectSauron as internal proxy nodes for silent and inconspicuous data exfiltration, blending in with high volumes of legitimate traffic.

Once installed, the main ProjectSauron modules start working as 'sleeper cells', displaying no activity of their own and waiting for 'wake-up' commands in the incoming network traffic. This method of operation ensures ProjectSauron's extended persistence on the servers of targeted organizations.

8. What kind of implants does ProjectSauron use?

Most of ProjectSauron's core implants are designed to work as backdoors, downloading new modules or running commands from the attacker purely in memory. The only way to capture these modules is by making a full memory dump of the infected systems.

Almost all of ProjectSauron's core implants are unique, have different file names and sizes, and are individually built for each target. Each module's timestamp, both in the file system and in its own headers, is tailored to the environment on which it is installed.

Secondary ProjectSauron modules are designed to perform specific functions like stealing documents, recording keystrokes, and stealing encryption keys from both infected computers and attached USB sticks.

ProjectSauron implements a modular architecture using its own virtual file system to store additional modules (plugins) and a modified LUA interpreter to execute internal scripts. There are upwards of 50 different plugin types.

9. What is the initial infection vector?

To date, the initial infection vector used by ProjectSauron to penetrate victim networks remains unknown.

10. How were the ProjectSauron implants deployed within the target network?

In several cases, ProjectSauron modules were deployed through the modification of scripts used by system administrators to centrally deploy legitimate software updates within the network.

In essence, the attackers injected a command to start the malware by modifying existing software deployment scripts. The injected malware is a tiny module that works as a simple downloader.

Once started under a network administrator account, this small downloader connects to a hard-coded internal or external IP address and downloads the bigger ProjectSauron payload from there.

In cases where the ProjectSauron persistence container is stored on disk in EXE file format, it disguises the files with legitimate software file names.

11. What C&C infrastructure did the attackers use?

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.

We collected 28 domains linked to 11 IPs located in the United States and several European countries that might be connected to ProjectSauron campaigns. Even the diversity of ISPs selected for ProjectSauron operations makes it clear that the actor did everything possible to avoid creating patterns.

12. Does ProjectSauron target isolated (air-gapped) networks?

Yes. We registered a few cases where ProjectSauron successfully penetrated air-gapped networks.

The ProjectSauron toolkit contains a special module designed to move data from air-gapped networks to Internet-connected systems. To achieve this, removable USB devices are used. Once networked systems are compromised, the attackers wait for a USB drive to be attached to the infected machine.

These USBs are specially formatted to reduce the size of the partition on the USB disk, reserving an amount of hidden data (several hundred megabytes) at the end of the disk for malicious purposes. This reserved space is used to create a new custom-encrypted partition that won't be recognized by a common OS, such as Windows. The partition has its own semi-filesystem (or virtual file system, VFS) with two core directories: 'In' and 'Out'.

This method also bypasses many DLP products, since software that disables the plugging of unknown USB devices based on DeviceID wouldn't prevent an attack or data leakage, because a genuine recognized USB drive was used.

13. Does ProjectSauron target critical

infrastructure?

Some of the entities infected by ProjectSauron can be classified as critical infrastructure. However, we haven't registered ProjectSauron infections inside industrial control system networks that have SCADA systems in place.

Also, we have not yet seen a ProjectSauron module targeting any specific industrial hardware or software.

14. Did ProjectSauron use any special communication methods?

For network communication, the ProjectSauron toolkit has extensive abilities, leveraging the stack of the most commonly used protocols: ICMP, UDP, TCP, DNS, SMTP and HTTP.

One of the ProjectSauron plugins is the DNS data exfiltration tool. 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.

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.

15. What is the most sophisticated feature of the ProjectSauron APT?

In general, the ProjectSauron platform is very advanced and reaches the level of complexity of Regin, Equation and similar threat actors we have reported on in the past. Some of the most interesting things in the ProjectSauron platform include:

- Multiple exfiltration mechanisms, including piggybacking on known protocols.
- Bypassing air-gaps using hidden data partitions on USB sticks.
- Hijacking Windows LSA to control network domain servers.
- Implementing an extended LUA engine to write custom malicious scripts to control the entire malware platform with a

high-level language.

16. Are the attackers using any zero-day vulnerabilities?

To date we have not found any 0-day exploits associated with ProjectSauron.

However, 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.

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.

17. Is this a Windows-only threat? What versions of Windows are targeted?

ProjectSauron works on all modern Microsoft Windows operating systems – both x64 and x86. We have witnessed infections running on Windows XP x86 as well as Windows 2012 R2 Server Edition x64.

To date, we haven't found a non-Windows version of ProjectSauron.

18. Were the attackers hunting for specific information?

ProjectSauron actively searches for information related to rather uncommon, custom network encryption software. This client-server software is widely adopted by many of the target organizations to secure communications, voice, email, and document exchange.

In a number of the cases we analyzed, ProjectSauron deployed malicious modules inside the custom network encryption's software directory, disguised under similar filenames and accessing the data placed beside its own executable. Some of extracted LUA scripts show that the attackers have a high interest in the software components, keys, configuration files, and the

location of servers that relay encrypted messages between the nodes.

Also, one of the embedded ProjectSauron configurations contains a special unique identifier for the targeted network encryption software's server within its virtual network. The behavior of the component that searches for the server IP address is unusual. After getting the IP, the ProjectSauron component tries to communicate with the remote server using its own (ProjectSauron) protocol as if it was yet another C&C server. This suggests that some communication servers running the mentioned network encryption software could also be infected with ProjectSauron.

19. What exactly is being stolen from the targeted machines?

The ProjectSauron modules we found are able to steal documents, record keystrokes and steal encryption keys from infected computers and attached USB sticks.

The fragment of configuration block below, extracted from ProjectSauron, shows the kind of information and file extensions the attackers were looking for:

```
.*account.*|.*acct.*|.*domain.*|.*login.*|.*member.*|.*user.*|.*name|.*email|.*_id|id|uid|mn|mailaddress|.*nick.*|alias|codice|uin|sign-in|strCodUtente|.*pass.*|.*pw|pw.*|additional_info|.*secret.*|.*segreto.*

[^\$]$

^.*\.(doc|xls|pdf)$
```

```
*.txt;*.doc;*.docx;*.ppt;*.pptx;*.xls;*.xlsx;*.vsd;*.wab;*.pdf;*.dst;*.ppk;*.rsa;*.rar;*.one;*.rtf;~WPL*.tmp;*.FTS;*.rpt;*.conf;*.cfg;*.pk2;*.nct;*.key;*.psw
```

Interestingly, while most of the words and extensions above are in the English language, several of them point to Italian, such as:

'codice', 'strCodUtente' and 'segreto'.

Keywords / filenames targeted by ProjectSauron data theft modules:

Italian keyword	Translation
Codice	code
CodUtente	Usercode
Segreto	Secret

This suggests the attackers had prepared to attack Italian-speaking targets as well. However, we are not aware of any Italian victims of ProjectSauron at the moment.

20. Have you observed any artifacts indicating who is behind the ProjectSauron APT?

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 are 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.

21. Is this a nation-state sponsored attack?

We think an operation of such complexity, aimed at stealing confidential and secret information, can only be executed with support from a nation-state.

22. What would ProjectSauron have cost to set up and run?

Kaspersky Lab has no exact data on this, but estimates that the development and operation of ProjectSauron is likely to have required several specialist teams and a budget probably running into millions of dollars.

23. How does the ProjectSauron platform compare to other top-level threat actors?

The actor behind ProjectSauron is very advanced, comparable only to the top-of-the-top in terms of sophistication: alongside Duqu, Flame, Equation, and Regin. Whether related or unrelated to these advanced actors, the ProjectSauron attackers have definitely learned from them.

As a reminder, here are some features of other APT attackers which we discovered that the ProjectSauron attackers had carefully learned from or emulated:

Duqu:

- Use of intranet C&Cs (where compromised target servers may act as independent C&Cs)
- Running only in memory (persistence on a few gateway hosts only)
- Use of different encryption methods per victim
- Use of named pipes for LAN communication
- Malware distribution through legitimate software deployment channels

Flame:

- LUA-embedded code
- Secure file deletion (through data wiping)
- Attacking air-gapped systems via removable devices

Equation and Regin:

- Usage of RC5/RC6 encryption
- Virtual Filesystems (VFS)
- Attacking air-gapped systems via removable devices
- Hidden data storage on removable devices

These other actors also showed what made them vulnerable to potential exposure, and ProjectSauron did its best to address these issues:

- Vulnerable or persistent C&C locations
- ISP name, IP, domain, and tools reuse across different campaigns

- Crypto-algorithm reuse (as well as encryption keys)
- Forensic footprint on disk
- Timestamps in various components
- Large volumes of exfiltrated data, alarming unknown protocols or message formats

In addition, it appears that the attackers took special care with what we consider as indicators of compromise and implemented a unique pattern for each and every target they attacked, so that the same indicators would have little value for anyone else. This is a summary of the ProjectSauron strategy as we see it. The attackers clearly understand that we as researchers are always looking for patterns. Remove the patterns and the operation will be harder to discover. We are aware of more than 30 organizations attacked, but we are sure that this is just a tiny tip of the iceberg.

24. Do Kaspersky Lab products detect all variants of this malware?

All Kaspersky Lab products detect ProjectSauron samples as HEUR:Trojan.Multi.Remsec.gen

25. Are there Indicators of Compromise (IOCs) to help victims identify the intrusion?

ProjectSauron's tactics are designed to avoid creating patterns. Implants and infrastructure are customized for each individual target and never re-used – so the standard security approach of publishing and checking for the same basic indicators of compromise (IOC) is of little use.

However, structural code similarities are inevitable, especially for non-compressed and non-encrypted code. This opens up the possibility of recognizing known code in some cases.

That's why, alongside the formal IOCs, we have added relevant YARA rules. While the IOCs have been listed mainly to give examples of what they look like, the YARA rules are likely to be of greater use and could detect real traces of ProjectSauron.

For background: YARA is a tool for uncovering malicious files or patterns of suspicious activity on systems or networks that share

similarities. YARA rules—basically search strings—help analysts to find, group, and categorize related malware samples and draw connections between them in order to build malware families and uncover groups of attacks that might otherwise go unnoticed.

We have prepared our YARA rules based on tiny similarities and oddities that stood out in the attackers' techniques. These rules can be used to scan networks and systems for the same patterns of code. If some of these oddities appear during such a scan, there is a chance that the organizations has been hit by the same actor.

More information about ProjectSauron is available to customers of Kaspersky Intelligence Reporting Service. Contact: intelreports@kaspersky.com

Related Articles

THE DROPPING ELEPHANT – AGGRESSIVE CYBER-ESPIONAGE IN

OPERATION DAYBREAK

CVE-2016-4171 – ADOBE FLASH ZERO-DAY USED IN TARGETED ATTACKS