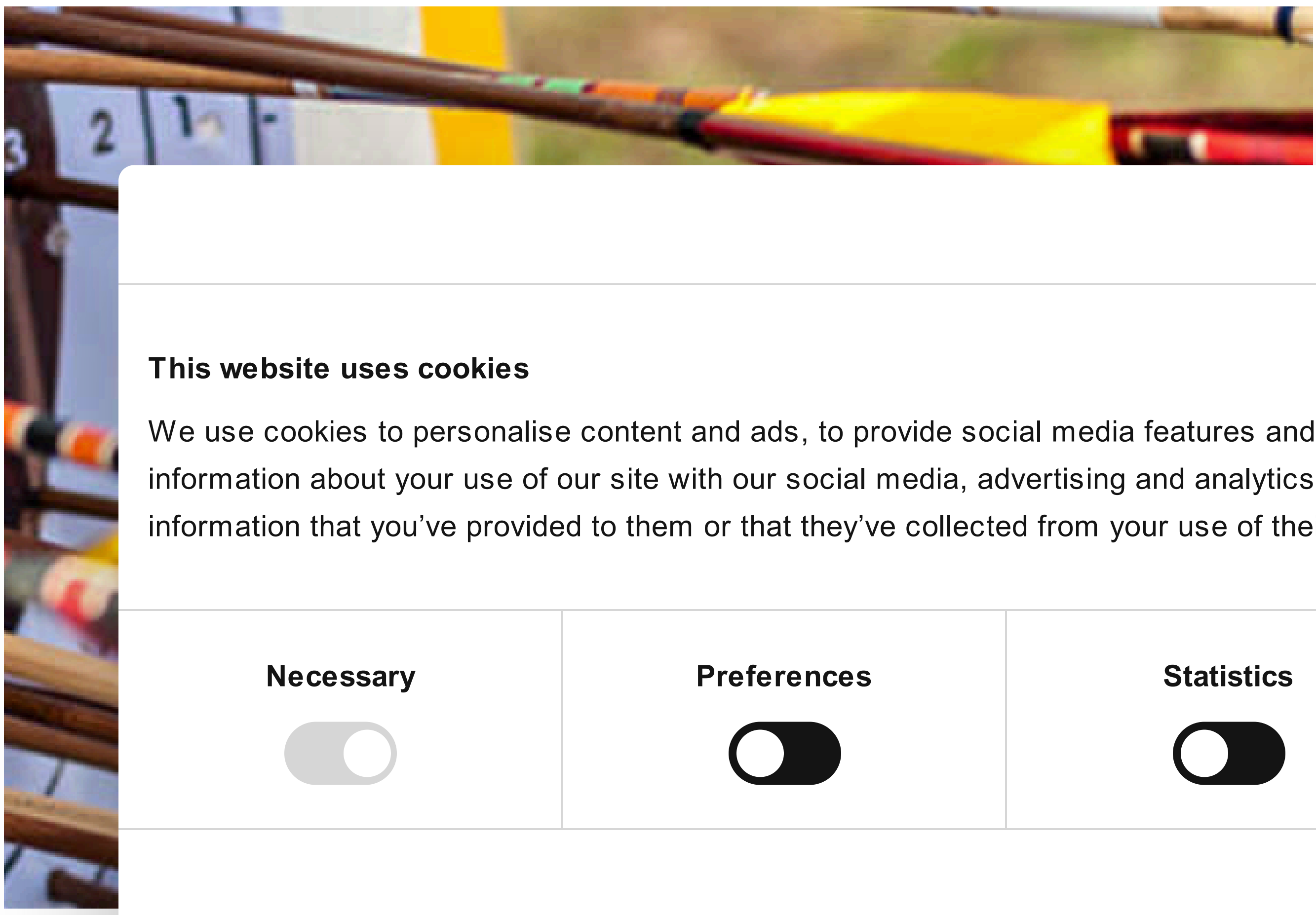
ProjectSauron: top level cyber-espionage platform covertly extracts encrypted government comms

APT REPORTS 08 AUG 2016 13 minute read



// AU

Expert GRE

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 exceptional espionage platform is "ProjectSauron", also known as "Strider".

Table of Contents

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
products
Septem
The susp
controlle
sensitive
threat a
key gove

"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. Wha

ProjectS
enable a
multiple

Technica
avoid rep
their valu

Usually A
specific
within th
seems t
intelligen
area.

The nam
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

GREAT WEBINARS

13 MAY 2021, 1:00PM
GReAT Ideas. Balalaika Edition
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM
GReAT Ideas. Green Tea Edition
JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU,

:
IoT

MELEV

: threat

BAB,

: threat

BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT, FABIO ASSOLINI

3. Hav

As usual
enforce
awarene
contact

4. For

Forensic
still activ
active o

5. Did t

The atta

- Data
- 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
modules
these m

Almost a
are indiv
own hea

Seconda
docume
and atta

ProjectS
additiona
are upwa

9. Wha

To date,
remains

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?

FROM THE SAME AUTHORS

Grandoreiro, the global trojan with grandiose goals

Stealer here, stealer there, stealers everywhere!

Exotic SambaSpy is now dancing with Italian users

n Latin

ew
s on
ions in

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 U
reservin
maliciou
that wor
filesyste

This met
unknown
genuine

13. Do

Some of
Howeve
network

Also, we
or softw

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
Edition x

To date,

18. We

ProjectS
encrypti
organiza

In a numb
custom
accessin
the attac
location

Also, one
for the t
of the co
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*.t
mp;*.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 n

20. Ha
Projec

Attributi
in variou
smoke a
When de
attributio

21. Is t

We think
can only

22. Wh

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.

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of the SideWinder APT group

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities

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 c
- Runn
- Use c
- Use c
- Malw

Flame:

- Lua-
- Secu
- Attac

Equation

- Usag
- Virtu
- 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 back
on syste
analysts
them in c
unnotice

We have
attacker
patterns
the orga

More inf
Reportin

APT

PROJE

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

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Email *

Comment

PATRICK
Posted on August 8, 2016. 6:28 pm

I left a similar comment on Facebook, but I thought I'd point it out here as well: The scripting language's name is Lua, not LUA. Here's what they have to say about it:

"Lua" (pronounced LOO-ah) means "Moon" in Portuguese. As such, it is neither an acronym nor an abbreviation, but a noun. More specifically, "Lua" is a name, the name of the Earth's moon and the name of the language. Like most names, it should be written in lower case with an initial capital, that is, "Lua". Please do not write it as "LUA", which is both ugly and confusing, because then it becomes an acronym with different meanings for different people. So, please, write "Lua" right!

Reply

NOLAN BERRY
Posted on August 9, 2016. 5:03 pm

I gave a talk this week at DefCon Skytalks on more advanced DNS Exfil and C&C interesting to see this come up so soon.

Reply

SHACHAR2
Posted on August 10, 2016. 11:18 am

can't wait for the documentary about the project
in 50 years time…

Reply

IGOR
Posted on March 14, 2018. 5:12 pm

LUA is a

Reply

// LA

SAS

The Cry APT: Inv

BORIS LARIN

nouls

es of

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR
04 SEP 2024, 5:00PM 60 MIN
Inside the Dark Web: exploring the human side of cybercriminals
ANNA PAVLOVSKAYA

TECHNOLOGIES AND SERVICES
13 AUG 2024, 5:00PM 60 MIN
The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise
OLEG GOROBETS, ALEXANDER LISKIN

CYBERTHREAT TALKS
16 JUL 2024, 5:00PM 60 MIN
Cybersecurity's human factor – more than an unpatched vulnerability
OLEG GOROBETS

TRAININGS AND WORKSHOPS
09 JUL 2024, 4:00PM 60 MIN
Building and prioritizing detection engineering backlogs with MITRE ATT&CK
ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

// SU
MAILS

The hott

cribe

Cookiebot by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
●	○	○	○

Show details >

kasp

Industrial threats
Web threats
Vulnerabilities and exploits
All threats

Security technologies
Research
Publications
All categories

Encyclopedia
Threats descriptions
KSB 2023

Privacy Policy | License Agreement | Cookies