Operation TunnelSnake

APT REPORTS 06 MAY 2021 21 minute read

// AU

MA

Form netw

Window for their implants have high privileges in the system, allowing them to intercept and potentially tamper with core I/O operations conducted by the underlying OS, like reading or writing to files or processing incoming and outgoing network packets. The capability to blend into the fabric of the operating system itself, much like security products do, is the quality that earns rootkits their notoriety for stealth and evasion.

Having said that, the successful deployment and execution of a rootkit component in Windows has become a difficult task over the years. With Microsoft's introduction of Driver Signature Enforcement, it has become harder (though not impossible) to load and run new code in kernel space. Even then, other mechanisms such as Kernel Patch Protection (also known as PatchGuard) make it hard to tamper with the system, with every change in a core system structure potentially invoking the infamous Blue Screen of Death.

Consequently, the number of Windows rootkits in the wild has decreased dramatically, with the bulk of those still active often being leveraged in high profile APT attacks. One such example came to our attention during an investigation last year, in which we uncovered a formerly unknown Windows rootkit and its underlying cluster of activity. We observed this rootkit and other tools by the threat actor behind it being used as part of a campaign we dubbed 'TunnelSnake', conducted against several prominent organizations in Asia and Africa.

In this blog post we will focus on the following key findings that came up in our investigation:

- A newly discovered rootkit that we dub 'Moriya' is used by an unknown actor to deploy passive backdoors on public facing servers, facilitating the creation of a covert C&C communication channel through which they can be silently controlled;
- The rootkit was found on networks of regional diplomatic organizations in Asia and Africa, detected on several instances dating back to October 2019 and May 2020, where the infection persisted in the targeted networks for several months after each deployment of the malware;
- We observed an additional victim in South Asia, where the threat actor deployed a broad toolset for lateral movement along with the rootkit, including a tool that was formerly used by APT1. Based on the detection timestamps of that toolset, we assess that the attacker had a foothold in the network from as early as 2018;
- A couple of other tools that have significant code overlaps with Moriya were found as well. These contain a user mode version of the malware and another driver-based utility used to defe

We prov
More de
more de

Wha

Our inve
on a det
the malw
allows at
are mark
over whi

The root
kernel m
interest
by secur
initiating a connection to a server itself, avoids the need to incorporate a C&C address in the malware's binary or to maintain a steady C&C infrastructure. This hinders analysis and makes it difficult to trace the attacker's footprints.

The figure below illustrates the structure of the rootkit's components. They consist of a kernel mode driver and a user mode agent that deploys and controls it. In the following sections we will break down each of these components and describe how they operate to achieve the goal of tapping into the target's network communication and blending in its traffic.

Fig. 1. The architecture of the Moriya rootkit

User mode agent analysis

The user
mode co
commun
compror
be deplo
and relie
incoming

The first
targeted
named Ir
'Network
to the re
HKLM\S
invoked

Next, aft
system.
correspo
disk. In th
64-bit driver to the drivers directory in the system path, under the name MoriyaStreamWatchmen.sys, hence the rootkit's name.

Fig. 2. Code that writes the Moriya driver to disk

The agent uses a known technique whereby the VirtualBox driver (VBoxDrv.sys) is leveraged to bypass the Driver Signature Enforcement mechanism in Windows and load Moriya's unsigned driver. DSE is an integrity mechanism mandating that drivers are properly signed with digital signatures in order for them to be loaded, which was introduced for all versions of Windows starting from Vista 64-bit. The technique used to bypass it was seen in use by other threat actors like Turla, Lamberts and Equation.

Moriya's user mode agent bypasses this protection with the use of an open-source code[1] named DSEFIX v1.0. The user agent dumps an embedded VBoxDrv.sys image of version 1.6.2 to disk and loads it, which is then used by the aforementioned code to map Moriya's unsigned driver to kernel memory space and execute it from its entry point. These actions are made possible through IOCTLs implemented in VBoxDrv.sys that allow writing to kernel address space and executing code from it. Throughout this process, the bypass code is used to locate and modify a flag in kernel space named g_CiOptions, which controls the mode of enforcement.

After the unsigned driver is loaded, the agent registers a special keyword that is used as a magic value, which will be sought in the first bytes of every incoming packet passed on the covert channel. This allows the rootkit to filter marked packets and block them for any application on the system other than the user mode agent. The registration of the value is done through a special IOCTL with the code 0x222004 sent to the driver, where a typical magic string is pass12.

Except f
reverse
consists
port are
creating
for the r

In any ot
will be re
received
operatio
data fro

Upon an
using nar
channel
streams
function with the driver's handle.

All traffic passed on the channel is encoded with a simple encryption scheme. Every sent byte has its payload, following the magic string, XORed with the value 0x05 and then negated. Following the same logic, to decode the incoming traffic's payload, every byte of it should be first negated and then XORed with 0x05.

JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM
GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots
MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM
GReAT Ideas. Powered by SAS: threat actors advance on new fronts
IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM
GReAT Ideas. Powered by SAS: threat hunting and new techniques
DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER, BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT,

Fig. 4. Code used for packet encoding

Kernel mode driver analysis

The Moriya rootkit's driver component makes use of the Windows Filtering Platform (WFP) to facilitate the covert channel between the compromised host and the C&C server. WFP provides a kernel space API that allows driver code to intercept packets in transit and intervene in their processing by the Windows TCP/IP network stack. This makes it possible to write a driver that can filter out distinct packet streams, based on developer-chosen criteria, and designate them for consumption by a specific user mode application, as is the case in Moriya.

The driver fetches the distinct Moriya-related traffic using a filtering engine. This is the kernel mode mechanism used to inspect traffic according to rules that can be applied on various fields across several layers of a packet (namely data link, IP and transport), making it possible to handle matching packets with unique handlers. Such handlers are referred to as callout functions.

In the case of Moriya, the filtering engine is configured to intercept TCP packets, sent over IPv4 from a remote address. Each packet with these criteria will be inspected by a callout function that checks if its first six bytes correspond to the previously registered magic value, and if so, copies the packet contents into a special buffer that can be later read by the user mode ag
system,

To allow
in a glob
and is ta
When th
packet u
data and
FwpsStr

Fig. 5. Code that creates a new packet, designates it for the flow of the corresponding incoming TCP packet and injects data written from user space into it

As formerly mentioned, the driver registers several functions that are exposed to the user mode agent in order to interact with it:

- IRP_MJ_READ: used to allow the user mode agent to read the body of a Moriya TCP packet from a special buffer to which it is copied upon receipt. The function itself waits on an event that gets signaled once such a packet is obtained, thus turning the ReadFile function called by the user mode agent into a blocking operation that will wait until the packet is picked up by the driver.
- IRP_MJ_WRITE: injects user-crafted data into a newly created TCP packet that is sent as a response to an incoming Moriya packet from the server.

- **IRP_MJ_DEVICE_CONTROL**: used to register the keyword to check the beginning of every incoming TCP packet in order to identify Moriya-related traffic. The passed magic is anticipated to be six characters long.

Fig. 6. Code used for registering the packet magic value from the driver side

How were targeted servers initially infected?

Inspecting the systems targeted by the rootkit, we tried to understand how they got infected in the first place. As previously mentioned, Moriya was seen deployed mostly on public-facing servers within the victim organizations. In one case, we saw the attacker infect an organizational mail server with the China Chopper webshell, using it to map the victim's

network

a comma

others r

```
"cmd" /c
"cmd" /c
HKLM\SYS
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
"cmd" /c
...
```

In genera

through

IISSpy (c

deploye

prior to running the malware.

king in

olution

Transparent Tribe: Evolution analysis, part 1

Post exploitation toolset

During our investigation we found a target in South Asia that enabled us to get a glimpse into some of the other tools that we assess were in use by the same attacker. The toolset includes programs used to scan hosts in the local network, find new targets, perform lateral movement to spread to them and exfiltrate files. While most of the tools seem custom made and tailored for the attackers' activities, we could also observe some open-source malware frequently leveraged by Chinese-speaking actors. Following is an outline of these tools based on their purpose in the infection chain.

- **Network Discovery**: custom built programs used to scan the internal network and detect vulnerable services.
  - **HTTP scanner**: command-line tool, found under the name '8.tmp', which discovers web servers through banner grabbing. This is done by issuing a malformed HTTP packet to a given address, where no headers are included and the request is succeeded with multiple null bytes.

Fig. 7. Malformed packet generated by HTTP scanner

If the server responds, the output will be displayed in the console, as shown below.

- D
  h
  a

- **Lateral Movement**: tools used to spread to other hosts in the targeted networks.
  - **BOUNCER**: malware that was first described by Mandiant in their 2013[2] report on APT1. This tool is another passive backdoor that waits for incoming connections on a specific port and provides different features, as outlined below, that can be used to control a remote host and facilitate lateral movement from it.

```
0x01: Proxy Init Connection
                0x02: Proxy Send Packet
                0x03: Proxy Close Connection
                0x07: Execute Shellcode
                0x0A: Kill Bot
                0x0C: Reverse Shell CMD
                0x0D: Delete File
                0x0E: Execute local program
                0x0F: Enumerate Servers In Domain and save output in gw.dat
                0x10: Enumerate SQL Servers and save output in sql.dat
                0x12: Reverse Shell CreateProcess
                0x16: Upload File - Write Data
                0x17: Download File - Finish
                0x1E: Download File - Start
                0x1F: Upload File - Start
                0x2D: Enumerate Servers
                0x2E: Enumerate SQL Server
                0x2F: Enumerate Servers Verbose
                0x30: Enumerate Users
                0x32: Do nothing
```

The BOUNCER sample that we observed contained a string that indicates which command-line arguments it anticipates:

```
usage:%s   IP  port [proxip] [port] [key]
```

However, the backdoor is configured to accept only the port number on which it will listen.

We saw two versions of this backdoor, initiated by two different launchers. The first one is an executable file named nw.tmp that decrypts an embedded payload using the RC4 algorithm and injects it into a newly spawned svchost.exe process. The injected payload is similar to one described by Mandiant in 2013, which is yet another intermediate loader that decrypts and loads an embedded BOUNCER DLL. The last stage is started by invoking the DLL's dump export with the arguments passed via the command line.

The other version was stored with the name rasauto.dll in the system directory, impersonating the Windows Remote Access Auto Connection Manager library. Like the other version, it decrypts an embedded DLL using RC4, but this time uses no intermediate stage, instead directly calling the DLL's dump export without arguments. The decrypted library is a slightly modified BOUNCER variant that always listens on the hardcoded port 1437.

F

B
w
n

```
r
                rasauto.dll - stage 0 – loader 26-08-2013 09:37:08
                rasauto.dll - stage 1 - embedded BOUNCER backdoor - 26-08-2013 09:36:27
```

- **Custom PSExec**: the attacker deployed a tool to execute commands remotely on compromised machines. Like the original PSExec tool, this one consists of two components – a client named tmp and a service named pv.tmp. In order to use the tool, the attacker has to execute it via a command line with the parameters specified below.

```
Usage: psexec <hostname >   psserve_path  exefilename  ServerName[option]\n
```

The service component is a tiny program that uses the CreateProcessA API to start a program specified as an argument. The client component uses the Service Control Manager (SCM) API to create a service on the target machine. If the ServerName argument is not specified, the service will be named Server%c%c where %c is a random lower case character. The exefilename argument is then passed to the StartServiceA function in order to initiate the command execution.

Fig. 11. Code used to create and start the service on targeted host

It is worth noting that the program has some limitations. Compared with the original PSExec, it is not able to copy the service binary (i.e., pv.tmp, which has its path specified in the psserve_path argument) to a remote machine, but rather assumes it is already present on it. Besides, it cannot handle network credentials, limiting the ability to execute

c

th

- **Exfil**

  hosts

  - E

    in

    o

    h

Fig. 12. Earthworm help message

Termite provides additional features to download and upload files between the compromised hosts, as well as a way to spawn a remote shell to control the targeted machine.

Fig. 13. Termite help message

- **TRAN:** another tool that we detected under the filename tmp that was used to transfer
d
e
la
p
vi
p
G
c
c

IISSp

IISSpy is
telemetr
websites. It was detected on a machine in 2018, unrelated to any of the attacks in the current operation. This suggests the threat actor has been active since at least that year.

The malware, which comes as a DLL, achieves its goals by enumerating running IIS processes on the server (i.e., those that are executed from the image w3wp.exe), and injecting the malware's DLL into them to alter their behavior. The executed code in the IIS processes will then set inline hooks for several functions, most notably CreateFileW.

The corresponding CreateFileW hook function checks if the filename argument contains the directory '\MORIYA\' or '\moriya\' in its path, and if so, infers that the attacker has sent a specially crafted HTTP request to the web server. In this request, the Moriya path in the URL is followed by an encoded command. After the command is decoded and processed, it is passed via a mailslot (\\.\mailslot\slot) to a separate thread, while signaling an event called Global\CommandEvent.

Fig. 15. Code of the CreateFileW hook function that looks for the 'MORIYA' \ 'moriya' directory in a request path

Should the currently handled file contain the Moriya path, the very same hook function will generate a special file on the web server to which command execution output will be written. This file's path is created by finding the position of the '\MORIYA\' or '\moriya\' strings in the inspected filename argument, and replacing it with the string '\IISINFO.HTM'. This will then be appended to the command data passed on the mailslot, following a ' > ' character.

The other thread waiting on the command event mentioned above is in charge of processing attacker data fetched from the mailslot. Any such command will be read and parsed to find the ' > ' character and the file path that follows it, in this case the one corresponding to 'IISINFO.HTML'. After executing the command via cmd.exe, the output will be written to the file in this path, allowing the attacker to read it by issuing a corresponding HTTP request where the URL path leads to this file on the server.

Other functions that are hooked in the IIS process are CreateProcessAsUserW and CreateProcessW. These are used to detect if the current process spawns a new server instance, which will in turn be injected with the malware's DLL. Apart from this, IISSpy will also create a monitoring thread that will periodically look for newly created httpd.exe processes, corresponding to the Apache server. If detected, the malware will be injected to them as well.

Althoug
that IISS
connect

- The c
in exa
conn
the IC
- Both
text l

Fi

- In bo
OutputDebugString API function. An example of such a string used in identical code in the two variants is shown below.

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

Fig.

- Both
servi
More

Fig. 18. Comparison of Install export function CFGs between IISSpy and Moriya

The ProcessKiller rootkit vs. security products

Another interesting artefact found in our telemetry that could be tied to the developers of Moriya is a malware named ProcessKiller. As its name suggests, it is intended to eliminate execution of processes, with the use of a kernel mode driver. Ultimately, this tool is used to shut down and block initiation of AV processes from kernel space, thus allowing other attack tools to run without being detected.

This malware operates through the following stages:

- An attacker calls the malware's DLL from an export named Kill, passing it a list of process names it would like to shut down and block as a command-line argument.
- The malware writes a driver that is embedded as a resource within it, impersonating a Kaspersky driver under the path %SYSTEM%\drivers\kavp.sys.
- There is an attempt to load the driver using the Service Control Manager. However, since it is not signed and loading is prone to fail on Windows versions above Vista 64-bit, the malware uses the same DSEFix code to bypass Digital Signature Enforcement as witnessed in Moriya's user mode agent.
- The malware parses the process names passed as arguments and creates a vector of 'blacklisted processes' out of them.
- For each process in the list, the malware detects its PID and issues it through an IOCTL with code 0x22200C to the driver which is in charge of shutting it down from kernel space. The shutc
PsLo
- The I
drive
boot
PsSe
creat
the p
STAT
failed
- At th
- If the
code

Once ag

- Distir

Fig. 19. Unique debug message that appears in ProcessKiller and Moriya

- Filename of the same structure, i.e., Moriya's agent is internally named 'MoriyaServiceX64.dll', and ProcessKiller's DLL is named 'ProcessKillerX64.dll'
- Usage of the exact same DSEFix code to load an unsigned driver.

What do we know about the threat actor?

Unfortunately, we are not able to attribute the attack to any particular known actor, but based on the TTPs used throughout the campaign, we suppose it is a Chinese-speaking one. We base this on the fact that the targeted entities were attacked in the past by Chinese-speaking actors, and are generally located in countries that are usually targeted by such an actor profile. Moreover, the tools leveraged by the attackers, such as China Chopper, BOUNCER, Termite and

Earthworm, are an additional indicator supporting our hypothesis as they have previously been used in campaigns attributed to well-known Chinese-speaking groups.

Who were the targets?

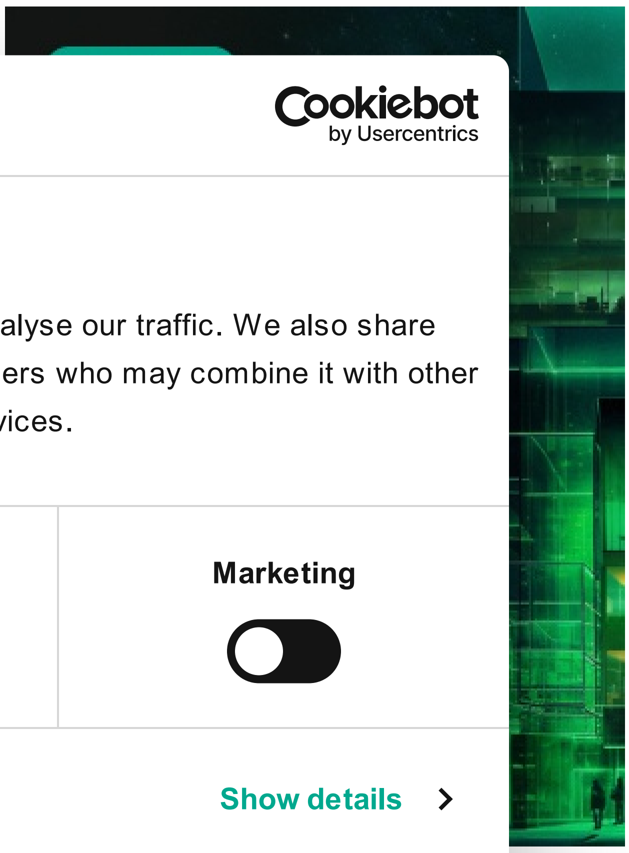
Based on our telemetry the attacks were highly targeted and delivered to less than 10 victims around the world. The most prominent victims are two large regional diplomatic organizations in South-East Asia and Africa, while all the others were victims in South Asia.

Conclusion

The TunnelSnake campaign demonstrates the activity of a sophisticated actor that invests significant resources in designing an evasive toolset and infiltrating networks of high-profile organizations. By leveraging Windows drivers, covert communications channels and proprietary malware, the group behind it maintains a considerable level of stealth. That said, some of its TTPs, like the usage of a commodity webshell and open-source legacy code for loading unsigned drivers, may get detected and in fact were flagged by our product, giving us visibility into the group's operation.

Still, with activity dating back to at least 2018, the threat actor behind this campaign has shown that it is
conduct
area of i
continue
and upda

For more
at: intelr
To learn
check ou



IOCs

48307C22	
A2C4EE8	
5F0F1B0A	
C1159FE3193E8B5206006B4C9AFBFE62	ProcessKiller
DA627AFEE096CDE0B680D39BD5081C41	ProcessKiller Driver – 32-bit
07CF58ABD6CE92D96CFC5ABC5F6CBC9A	ProcessKiller Driver – 64-bit
9A8F39EBCC580AA56D6DDAF5804EAE61	pv.tmp (Custom PSExec Server)
39C361ABB74F9A338EA42A083E6C7DF8	pc.tmp (Custom PsExec Client)
DE3FB65461EE8A68A3C7D490CDAC296D	tran.tmp (Exfiltration tool)
EAC0E57A22936D4C777AA121F799FEE6	client.exe (Utility embedded in tran.tmp)
D745174F5B0EB41D9F764B22A5ECD357	rasauto.dll (Bouncer Loader)
595E43CDF0EDCAA31525D7AAD87B7BE4	8.tmp (HTTP)Scanner
9D75B50727A8E732DB0ADE7E270A7395	ep.tmp DCOM Scanner
3A4E1F3F7E1BAAB8B02F3A8EE20F98C9	nw.tmp Bouncer Loader
47F2D06713DAD556F535E523B777C682	Termite

45A5D9053BC90ED657FA90DE0B775E8F	Earthworm

[1] Today a copy of the original code can be found here: http://www.m5home.com/bbs/thread-8043-1-1.html

[2] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

APT · MALWARE DESCRIPTIONS · MALWARE TECHNOLOGIES · ROOTKITS · TARGETED ATTACKS

Operation TunnelSnake

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

Type your comment here

Name *

Com

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 >

// LA

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

Grandoreiro, the global trojan with grandiose goals

GREAT

Stealer here, stealer there, stealers everywhere!

GREAT

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// 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.

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

**EastWi
attacks
Russia**

Kaspers
campaig
using Cl
APT27 t

// SU
MAILS

The hott

cribe

Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023

Privacy Policy | License Agreement | Cookies

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 ›