TLP:WHITE

# THE CYBERCRIMINAL GROUP SILENCE

1.0

17/07/2020


TLP:WHITE

# Sommaire

**1 Silence's main target group: banks** . . . . . **3**

**2 Tactics, techniques and procedures (TTPs)** . . . . . **4**
2.1 Compromises . . . . . 4
2.2 Deployment . . . . . 4
2.3 Attack execution . . . . . 5
2.3.1 Access to the ATM management software . . . . . 5
2.3.2 Accessing the card processing system . . . . . 7

**3 Links between Silence and TA505** . . . . . **8**

**4 Conclusion** . . . . . **8**

**5 Bibliographie** . . . . . **9**

# 1 Silence's main target group: banks

Silence[1] is a group of allegedly Russian-speaking, independent cybercriminals that has been on the scene since 2016. Initially it mostly targeted banks in CIS countries (such as Russia, Belarus, Moldova, Armenia and Kazakhstan) as well as Ukraine, but has since extended its reach to some thirty countries across Europe (Germany, Switzerland, the UK and Austria among them), Asia (including Israel, Turkey, Taiwan, Malaysia and South Korea) and Africa (e.g. Ghana and Kenya) [1].

According to Group-IB [1, 2], IP addresses located in France reportedly communicated with Silence's command-and-control (C2) infrastructure in 2019, something that had apparently already happened in 2016 and 2017.

| IP | Provider | Country | Program | Year |
|---|---|---|---|---|
| 5.39.30.110 | OVH | France | Silence.Downloader | 09-2016 |
| 54.36.191.97 | OVH | France | Silence.Downloader | 10-2017 |
| 164.132.228.29 | OVH | France | Silence.Downloader | 06-2017 |
| 137.74.224.142 | OVH | France | Silence.Downloader | 08-2017 |
| 92.222.68.32 | OVH | France | Silence.Downloader | 04-2017 |
| 139.99.156.100 | OVH | France | Exploit | 10-2017 |
| 149.56.131.140 | OVH | France | Meterpreter | 08/10-2017 |
| 51.255.200.161 | OVH | France | Exploit CVE-2017-0199 | 06-2017 |
| 109.13.212.72 | SFR SA | France | pakovelli@mail.com | 08-2017 |

The IP address 5.39.30.110 (OVH) was used as a Silence.Downloader C2 server in September 2016. This IP address was resolved between August 2012 and June 2019 by the domain name « `cours-a-domicile.fr` ». However, a DNS resolution observed over such a long period of time may be a sign that the domain name has been "abandoned". What's more, were Silence to use the C2 for targeted phishing, this could indicate a targeting of French-speaking structures. Accordingly, the fact that nothing of the sort has come to the attention of the National Cybersecurity Agency of France (ANSSI) does not mean France could not be, or has not already been, a target.

One of the ways in which this cybercriminal group derives its income is through automated teller machines (ATMs), although this is not their only activity, as they adapt their tools to the compromised environment. Indeed, whereas Silence used tools developed by other cybercriminals[2] during their first attacks, the tools and malware they now leverage have mainly been developed by its members (Silence, Atmosphere, Farse and Cleaner[3]) [2, 1].

What typically happens once the victim's IS has been compromised is that Silence's C2 server deploys a payload containing several modules and enabling the threat actors:

- either to increase the withdrawal limits at ATMs as well as the overdraft limits of customer cards via an intrusion into the bank's payment card processing system;
- or to gain control of the bank's ATMs via an intrusion into its ATM management program.

In both cases, simultaneous withdrawals are carried out by mules[4].

In 2016, Silence also tried, on two occasions, to issue fraudulent transfers from the Russian inter-bank transfer system AWS CBR (Russian equivalent of Swift) [2].

In all, from June 2016 to June 2019, Silence is believed to have stolen around USD 4.2m from banks [1].

Silence appeared to be particularly active through 2019 and therefore warrants close attention. From September 2018 to August 2019 for example, Group-IB has already detected 16 campaigns run by Silence [1], and identified at least 7 successful campaigns:

- in May 2018 and February 2019, Silence attacked two Indian banks;

[1] FireEye names TEMP.TruthTeller which it considers to be part of Silence's activity. For Crowdstrike, Silence refers to Whisper Spider.
[2] For example, they had used the third party-developed backdoor Kikothac before designing their own backdoor, Silence.MainModule.
[3] This tool is used to delete logs of the threat actors' remote connection with the victim's IS.
[4] Individual who transfers illegally acquired funds via different bank accounts in different countries.

- in February 2019, it stole around USD 400,000 from the Russian bank Omsk IT Bank;
- in May 2019, it stole around USD 3m from the Bangladeshi bank Dutch-Bangla Bank;
- in June 2019, it attacked Russian banks;
- in July 2019, it attacked banks in Chile, Costa Rica, Bulgaria and Ghana.

# 2 Tactics, techniques and procedures (TTPs)

## 2.1 Compromises

Silence targets its victims through phishing emails masquerading as financial institutions. Sometimes, the emails come from legitimate addresses of employees at the institutions whose IS has already been compromised [3], lending them even more credibility.

These emails contain a malicious attachment:

- either in the form of a Word document containing a macro or exploit;
- or in the form of a ZIP or RAR file containing a CHM file[5];
- or in the form of a document exploiting CVE-2017-0199[6] and CVE-2017-11882[7] which downloads and runs an HTA file containing a VBScript;
- or in the form of a .LNK file[8].

As a preparatory stage, Silence is also known to send out thousands of emails on a global scale in a bid to update its database of active email addresses of its targets and expand its attack geography. These emails contain an image or link but no malicious payload [1]. Group-IB thus identified three such campaigns targeting Russia, former Soviet countries, Asia, Europe and New Zealand in 2018.

## 2.2 Deployment

By clicking on the malicious attachment, the victim launches the automatic installation within the information system (IS) of the remote administration tool Truebot (or Silence.Downloader). By communicating with the C2, this malware is used to deploy other payloads.

During more recent campaigns (in May 2019), Group-IB observed the use of the fileless loader Ivoke as a primary loader, rather than the Truebot one [1].

Moreover, Silence sometimes uses a proxy utility program, Silence.ProxyBot (Turncard) or Silence.ProxyBot.net (Fourthstreet), which forms a proxy between the compromised systems and the C2 server, so as to reach the local components of the compromised networks that cannot be accessed remotely.

[5] CHM files are compiled HTML files. When a Windows user opens a CHM file, Windows runs Microsoft's HTML Help program to display the compiled HTML file. By tampering with the legitimate help file to include malicious content activated when the documentation is displayed (such as when launching a PowerShell command), a threat actor can compromise an IS.
[6] Vulnerability in Office, discovered in March 2017, enabling malicious instructions to be concealed in a document saved in .RTF format.
[7] Vulnerability enabling code to be run remotely, existing in the Microsoft Office software when this fails to properly handle objects in memory, discovered in November 2017.
[8] File used to point to a file that can be run under Windows.

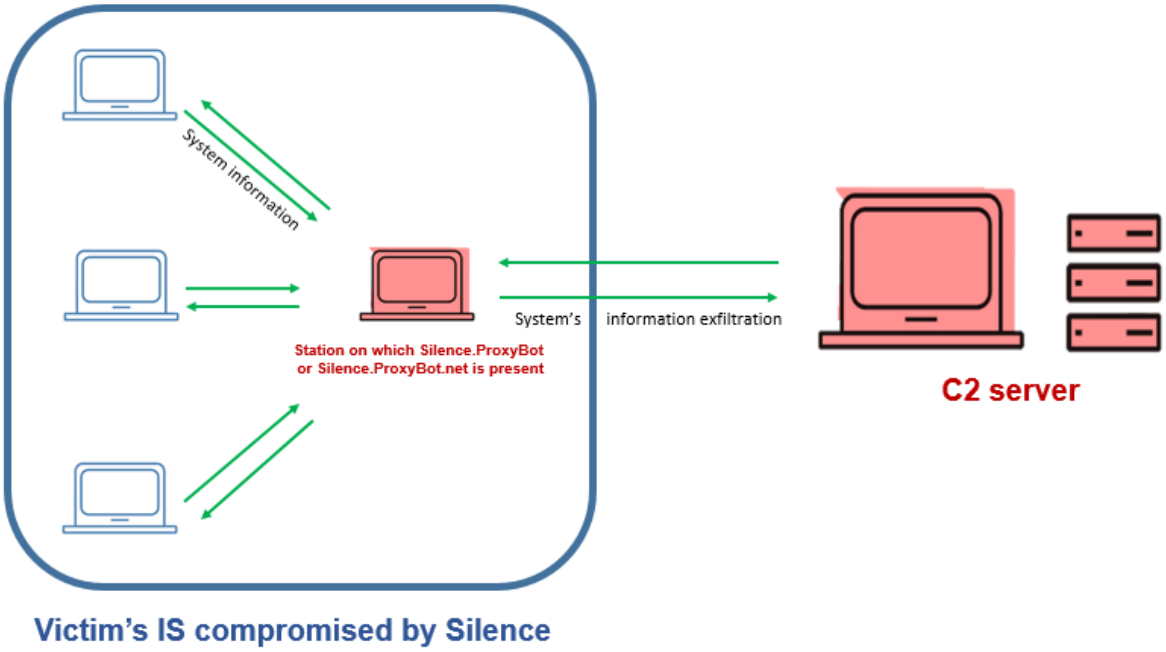


Fig. 2.1 : System information exfiltration via a proxy utility program

Silence retrieves information, exfiltrates data or downloads files within the IS by using at least three possible malicious codes:

- Slowroll (Silence.Mainmodule): this backdoor communicates directly with the C2 server or via a proxy server;
- EmpireDNSAgent (EDA): this tool, based on Empire and on dnscat2te, is a backdoor, distributed by Slowroll, and communicating with the C2 server by DNS tunnel;
- Cardcam[9]: this utility program makes screenshots and video recordings of the compromised system to give the threat actors an insight into how the victim's system works and enable them to identify the software the system uses.

## 2.3 Attack execution

### 2.3.1 Access to the ATM management software

CEN/XFS is a standard with which most ATM manufacturers (Diebold, Wincor, NCR) comply. Owing to their variable interpretation of the standard, it has become common to use the XFS manager. This is middleware which provides customer-server architecture for the Windows program managing ATMs. It therefore represents the interface between the program and the ATM.

[9] Identified by Kaspersky in November 2017, it is named Cardcam by FireEye.

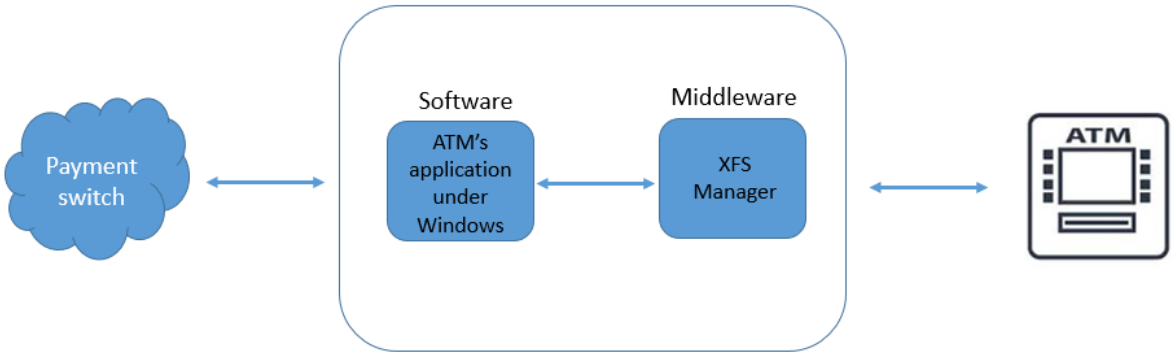


Fig. 2.2 : Interactions with the ATM

*Comment: any program developed in compliance with the XFS standard could assume control of an ATM, because this standard harmonises the operation of programs with any ATM. Any program, whether legitimate or malicious, that has been developed with the logic of this standard in mind, is capable of controlling low-level objects at an ATM. [4].*

Truebot distributes Atmosphere.Dropper in the victim's IS. Atmosphere.Dropper detects the ATM management program and its process, the function of which is to transfer commands to ATMs. For example, for Wincor-Nixdorf ATMs, this process is called fwmain32.exe.

Once the process has been detected, Atmosphere.Dropper or Atmosphere.Injector (which is distributed by Atmosphere.Dropper), injects the Atmosphere *dynamic link library* (DLL)[10] into it. This enables the threat actor to activate the payload Atmosphere.

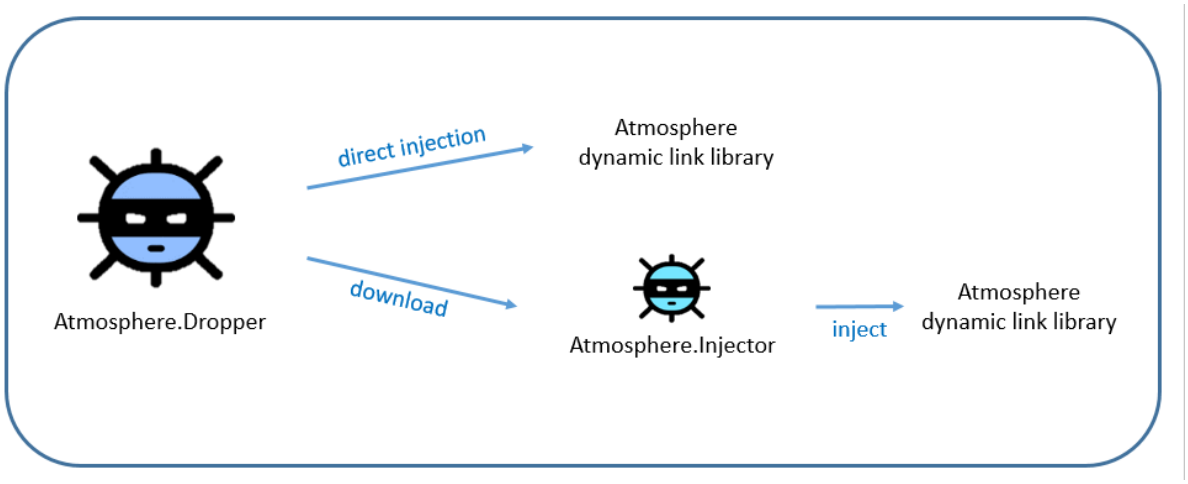


Fig. 2.3 : Injection of the malicious DLL into the legitimate process for controlling ATMs

Once activated, the threat actors can use it to:

- run a command to retrieve information about the content of the ATM cassettes;
- remotely control cash withdrawals by sending a command to the ATM;
- or physically control the ATM by entering a specific combination on the ATM keypad.

[10] A DLL is a software library that contains code and data whose functionality is loaded in a memory by a program as necessary at run time.

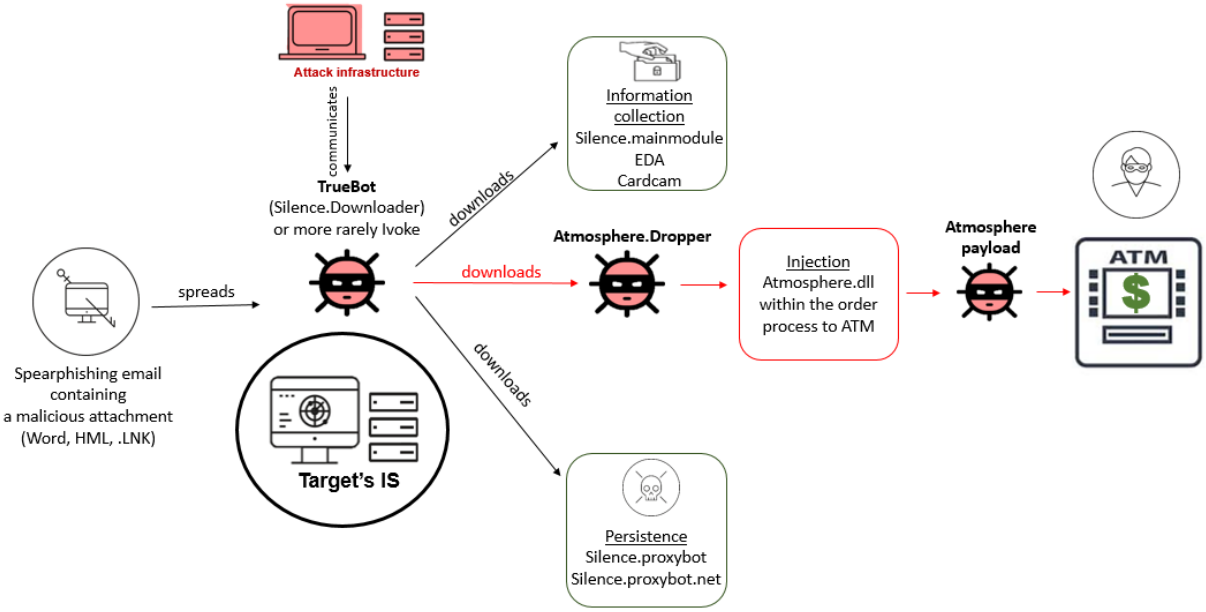


Fig. 2.4 : Silence's TTPs, resulting in fraudulent withdrawals at ATMs

*Comment: This technique for detecting ATM command processes and injecting a malicious DLL does not seem to have been invented by Silence, judging by open-source evidence dating from 2009 [5]. What's more, this technique is not the only one that can compromise an ATM. The hacker group Lazarus, for example, allegedly uses a malicious code intercepting their mules' fraudulent withdrawal requests in order to authorise the withdrawal without the knowledge of the bank's legitimate program.*

### 2.3.2 Accessing the card processing system

In order to make fraudulent withdrawals from ATMs, it would seem that Silence sometimes attempts to access the *card processing* system within the IS of the target bank in a bid to remove the withdrawal and overdraft limits of pre-activated payment cards, and then sends mules to withdraw the cash.

*Comment: Once threat actors have access to the card processing system, the money can be withdrawn from the ATM of any bank in any country. However, when these actors directly compromise the ATM management program, mules must travel to the target bank's actual location to be able to withdraw the money. This is what happened during Silence's attack against the Bangladeshi bank DBBL in May 2019 [6].*

For the purposes of accessing the card processing system, Silence is believed to compromise the account with the privileges of an employee at the target bank, by retrieving their password through the tool Farse. This tool is a modified version of Mimikatz (whose source code is available on Github).

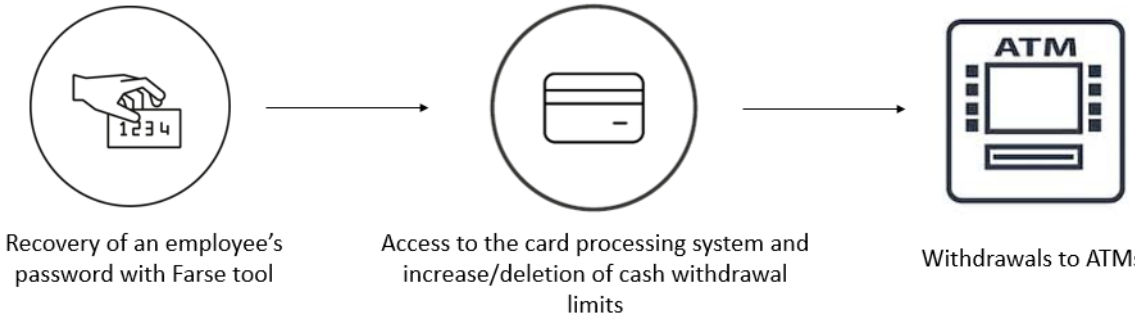


Fig. 2.5 : Compromising the card processing system

*Comment: Exfiltrations of customer data from payment/withdrawal system companies the likes of Mastercard or Visa can lead to this data being sold on the Dark Web, and used by cybercriminals to clone payment cards. Mules can then use these cards to make fraudulent cash withdrawals from ATMs. For example, the data exfiltration that MasterCard suffered in August 2019 could have been used for such purposes.*

# 3 Links between Silence and TA505

According to Group-IB, Truebot and FlawedAmmyy.Downloader[11] were likely developed by the same Russian-speaking individual. That said, FlawedAmmyy.Downloader has purportedly been in use since 2016 as part of sweeping and targeted phishing campaigns, most of which are attributed to TA505 [7, 8, 9]. .

*Comment: FlawedAmmyy and Truebot are also thought to have been developed in 2016, the year the group Silence emerged, while TA505 had already been operating since 2014.*

Finally, both TA505 and Silence sometimes use .LNK files as a malicious attachment within their phishing emails, to deliver FlawedAmmyy.downloader and Truebot respectively. And yet this file format is seldom used.

As mentioned by Group-IB [10], it is quite possible that the links between TA505 and Silence are down to the fact that Silence buys access to banks' ISs, particularly from TA505. Such access purchasing would tally with the fall in phishing emails that Silence is sending out.

On that note, at the end of 2019 TA505 looks to have granted Silence access to the IS of at least one bank in Europe [11].

# 4 Conclusion

Back when it was just starting out, Silence made mistakes during its attacks and mimicked the techniques of other groups. For example, the idea of taking screenshots of the infected workstations of employees at the target bank seems to have come from Carbanak[12]. But fast-forward to today, and Silence is one of the most active and sophisticated cybercriminals to currently be targeting the banking sector.

Silence's attacks might be facilitated by the target banks' lack of PCI DSS[13] compliance. For example, a recent cash-out attack by Silence on the Dutch Bangladesh Bank Limited (DBBL), which resulted in withdrawals totalling USD 3m, was facilitated by the fact that the DBBL had not applied the PCI DSS standard, in the same way as 95% of Bangladesh-based banks and a number of Asia-based banks. These banks are therefore more exposed to Silence-led attacks than European banks, even if, since the latter half of 2018, Silence has broadened its horizons to include Europe. This widening in Silence's attack perimeter comes hand-in-hand with its increasingly sophisticated TTPs.

[11] FlawedAmmyy is a remote access trojan based on the leaked source code of the legitimate software Ammyy Admin in 2016, and containing a *downloader* and payload.

[12] The source code of the Carbep backdoor, active since 2010, leaked in 2013. The malware families Anunak and Carbanak are believed to have derived from Carbep, both of which were deployed from 2013 to 2015 by the group commonly called Carbanak, as part of targeted attacks on banks and payment systems across some thirty countries. The booty comprised more than a billion dollars.

[13] Global certification ensuring the security of processed data (bank data and cards). It applies to the various stakeholders in the monetary chain, and gives rise to 300 security audits. PCI DSS compliance particularly means securely saving the data of customer cards, not least via encryption, continuous assessment and card data access security testing.

# 5 Bibliographie

[1] Group-IB. “SILENCE 2.0”. Août 2019. In : (août 2019).

[2] Group-IB. “Silence : Moving into the Darkside”. Sept. 2018. In : (sept. 2018).

[3] ReaQta. *Silence Group Targeting Russian Banks via Malicious CHM*. 24 jan. 2019. URL : https://reaqta.com/2019/01/silence-group-targeting-russian-banks/.

[4] Kaspersky. *Le Jackpot des distributeurs automatiques de billets : malwares et autres méthodes d'enrichissement*. 26 avr. 2016. URL : https://securelist.fr/malware-and-non-malware-ways-for-atm-jackpotting-extended-cut/64949/.

[5] Ne scrie caiafa verde. *Study on ATM Security : Code Injection on Wincor Nixdorf ATMs*. 3 juin 2009. URL : http://caiafaverde.blogspot.com/2009/06/study-on-atm-security-code-injection-on.html.

[6] Bleeping Computer. *Silence Group Likely Behind Recent $3M Bangladesh Bank Heist*. 3 juil. 2019. URL : https://www.bleepingcomputer.com/news/security/silence-group-likely-behind-recent-3m-bangladesh-bank-heist/.

[7] Trend Micro. *FlawedAmmyy Malware Information*. 31 juil. 2019. URL : https://success.trendmicro.com/solution/1123301-flawedammyy-malware-information.

[8] Proofpoint. *Leaked Ammyy Admin Source Code Turned into Malware*. 7 mar. 2018. URL : https://www.proofpoint.com/us/threat-insight/post/leaked-ammyy-admin-source-code-turned-malware.

[9] Trend Micro. *TA505 At It Again : Variety Is the Spice of ServHelper and FlawedAmmyy*. 27 août 2019. URL : https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/.

[10] Group-IB. *Group-IB Presents Its Annual Report on Global Threats to Stability in Cyberspace*. 29 nov. 2019. URL : https://www.group-ib.com/media/gib-2019-2020-report/.

[11] Group-IB. “New Financially Motivated Attacks in Western Europe Traced to Russian-Speaking Threat Actors”. 27 mar. 2020. In : (27 mar. 2020).

1.0 - 17/07/2020
Licence ouverte (Étalab - v2.0)

**AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN