TLP:WHITE

DEVELOPMENT OF THE ACTIVITY OF THE TA505 CYBERCRIMINAL GROUP

20/08/2020

TLP:WHITE

Table of contents

1 TA505 from 2014 to 2017

It would seem that the TA505 intrusion set goes back to at least 2014 but was only mentioned publicly for the first time on Twitter in 2017. Until 2017, its activity seems to have been confined to the distribution of trojans and ransomwares [1].

1.1 Malware distributed

1.1.1 Banking trojans

In terms of final payload, TA505 has always widely used banking trojans that are not specific to it, such as Dridex and Trickbot:

Dridex

TA505 is supposed to have distributed the **Dridex** malware [2] as of July 2014, i.e. one month after its creation (June 2014) [1]. Its use of specific ID botnets[1] within the Dridex network of botnets, controlled by the Evil Corp cybercriminal group, would suggest that TA505 was a Dridex affiliate from 2014 to 2017. ID botnets used by TA505 between 2014 and 2015 would have been botnet IDs 125, 220 and 223. The 220 botnet is thought to have contained 9650 bots in April 2015 [3], and mainly targeted banks [4], particularly in France. In 2016, TA505 is thought to have mainly concentrated on the use of Locky ransomware, to the detriment of Dridex malware, then resumed propagation of Dridex in 2017 through 7200 and 7500 ID botnets. TA505 finally stopped using Dridex in 2018 [5].

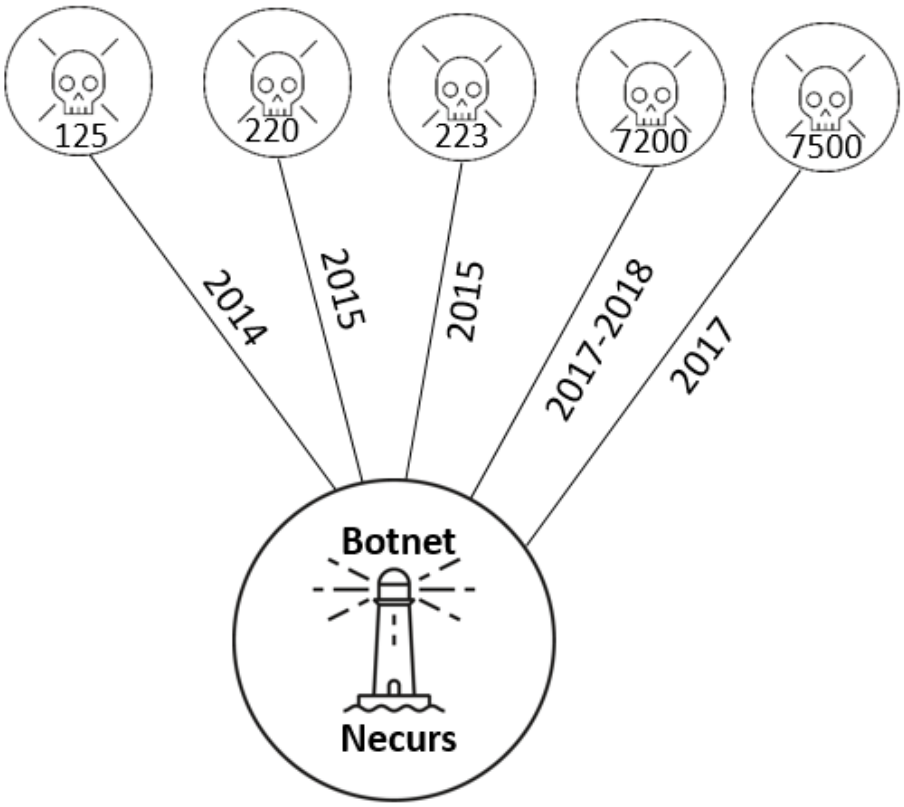

Fig. 1.1: Dridex Botnet IDs corresponding to TA505

[1]The number attributed to the version of **Dridex** associated with a subset of bots it handles. These ID botnets are used to differentiate the activity of each of its affiliates and associate different ID botnets with the same operator.

TrickBot

TA505 is also thought to have been an affiliate of TrickBot[2], known under the pseudonym of *mac1* [5]. The use of **TrickBot** by TA505 only lasted a few months in 2017. For example, a campaign dating back to June 2017 targeted France and the United Kingdom [5].

1.1.2 Ransomware

2016 saw the appearance of **Locky** ransomware. Frequently used, it has targeted many victims. Like **Dridex**, **Locky** works on the principle of affiliates [1].

According to Proofpoint, affiliate number 3 of **Locky** and the affiliate of ID botnet **Dridex** 220, TA505, have points in common, such as similar lures on their phishing emails and very strong similarities regarding Javascript, VBScript codes and Microsoft Word macros used [7]. There is also an absence of **Dridex** 220 campaigns concomitant with the emergence of Locky [8]. Proofpoint [7] also pinpoints links between **Locky** and the affiliate of **Dridex** ID botnet 7200, TA505 at this time, comparing **Dridex** 2017 campaigns with **Locky** past campaigns [1]. TA505 is therefore presumed to be affiliate number 3 (”Affid=3”) of this ransomware.

Although the main ransomware used by the group remains **Locky**, TA505 is thought to occasionally use other ransomwares (**Bart**[3], **Jaff**[4], **Scarab** [5], **Philadelphia**[6], **GlobeImposter**[7] and **GandCrab**[8]).

Locky stopped operating in 2017.

1.2 Distribution and compromise methods

TA505 seems to have distributed its malware only through phishing email campaigns. This intrusion set was characterised by its massive use of Necurs botnet (see appendix in chapter 5) for the distribution of emails [9].

Comment: open source reports associate all ransomwares distributed by the Necurs botnet to TA505. However, some of these ransomwares were used over the same periods. It seems unlikely that TA505 operated as many encryption codes at the same time. It is more likely that Necurs had several clients simultaneously.

This intrusion set relies exclusively over that period on social engineering to run its payload contained in malicious attachments linked to emails sent [9]. These attachments could be zip or 7zip archives containing VBS script or Javascript to be run by their victims, HTML pages containing malicious Javascript, or Offices documents bugged with malicious macros.

Although TA505 does not seem to have used software vunerability to compromise its targets, it is interesting to observe that it has kept up to speed with the latest social engineering techniques. It therefore distributed bugged Office documents via the DDE mechanism less than a month after the potential abuse of this feature became common knowledge [10].

[2] **Trickbot**, which appeared in October 2016, and a derivative of **Dyre**, possibly operated by members of the Business Club until November 2015. Reminder: the Business Club was responsible for JabberZeuS and GameOverZeuS(GoZ) malware. When the GoZ botnet was dismantled, the Business Club is thought to have divided its activites between Dridex and Dyre malware. **Trickbot** could be operated by former members of the Business Club, or by a *copycat* having acquired the source code of **Dyre** [6].
[3] ransomware which was very limited during 2016.
[4] ransomware active from May to June 2017.
[5] Variant of the first open-source **Hidden Tear** ransomware (published in 2015), used for the first time by TA505 in June 2017.
[6] *Ransomware-as-a-Service* available for 400 dollars on the Dark Web.
[7] ransomware used from July to December 2017. 24 campaigns distributing **GlobeImposter** were found by Proofpoint in December 2017 [9, 5]
[8] *Ransomware-as-a-Service* used from January to March 2018 [5]

2 Development of TA505 since 2018

The year 2018 was a turning point in the attack methods of the intrusion set. TA505 gradually reduced its distribution of malicious banking codes and ransomwares to move into the distribution of backdoors.

However, this intrusion set does not seem to be content with running a payload on its victim's computer. When it deems it useful, TA505 tries to compromise the entirety of the information system (IS) it penetrated.

It also seems, in some cases, to resell accesses to the backdoors it has installed, which makes it difficult to distinguish between specific TA505 activities and those of potential clients.

The chain of attack described in this chapter corresponds to the activities that ANSSI believes are linked to the intrusion set.

2.1 Infection vector

The only infection vector currently known to be used by the TA505 intrusion set is phishing emails including a malicious attachment or link. Until 2018, the intrusion set relied practically exclusively on the Necurs botnet to distribute its payloads. However, following the unavailability of the botnet in January and February 2018, TA505 seems to have less often used its services [9].

This last point however is uncertain as there is little information on the alternative email distribution methods of the intrusion set. Given that TA505 has often deployed an email credentials theft implant among its victims [11][12], it is possible that it accumulates email addresses to distribute its new phishing campaigns.

It has also been mentioned that some of its phishing emails had been distributed via machines infected by the **Amadey** [11] malware. Given that TA505 also uses **Amadey** malware as indicated in section 2.3.1, it may have created its own Amadey botnet to distribute its malicious emails, or may use the services of an existing Amadey botnet.

This operating mode also usurps the recipient addresses of its emails, which makes it difficult to analyse its email distribution infrastructure [13].

2.2 Social engineering

The intrusion set continues to rely on social engineering to run its malicious payloads on the machines of its email recipients, using several formats for attachments to work around its targets' security systems: .url [14], .iqy [9], SettingContent-ms [15], MS publisher files [16], .wiz and .pub [17], .iso [18]. The aim of these documents was often to run *msiexec*[9] commands via macros on the victim's machine to upload and run a malware.

However, in the second half of 2019 and first half of 2020, TA505 seems to have modified and stabilised its social engineering scheme. It now sends an HTML page as an attachment containing malicious Javascript code. This code redirects the victim towards an URL of a legitimate but compromised website.

This same URL corresponds to an HTML page containing a minimal Javascript code redirecting the victim towards a page hosted by a machine controlled by the intrusion set. This page mimicks that of a legitimate file-sharing site adapted to the target such as Onedrive, Dropbox [19] or Naver[10] (during one of its campaigns in South Korea) [20]. The victim is then encouraged to download, open and enable VBA macros of an Office document, usually Excel, containing a malicious payload .

[9] Tool used to interact in command line with the installation, updating and de-installation engine of software specific to Microsoft operating systems

[10] Korean internet portal service.

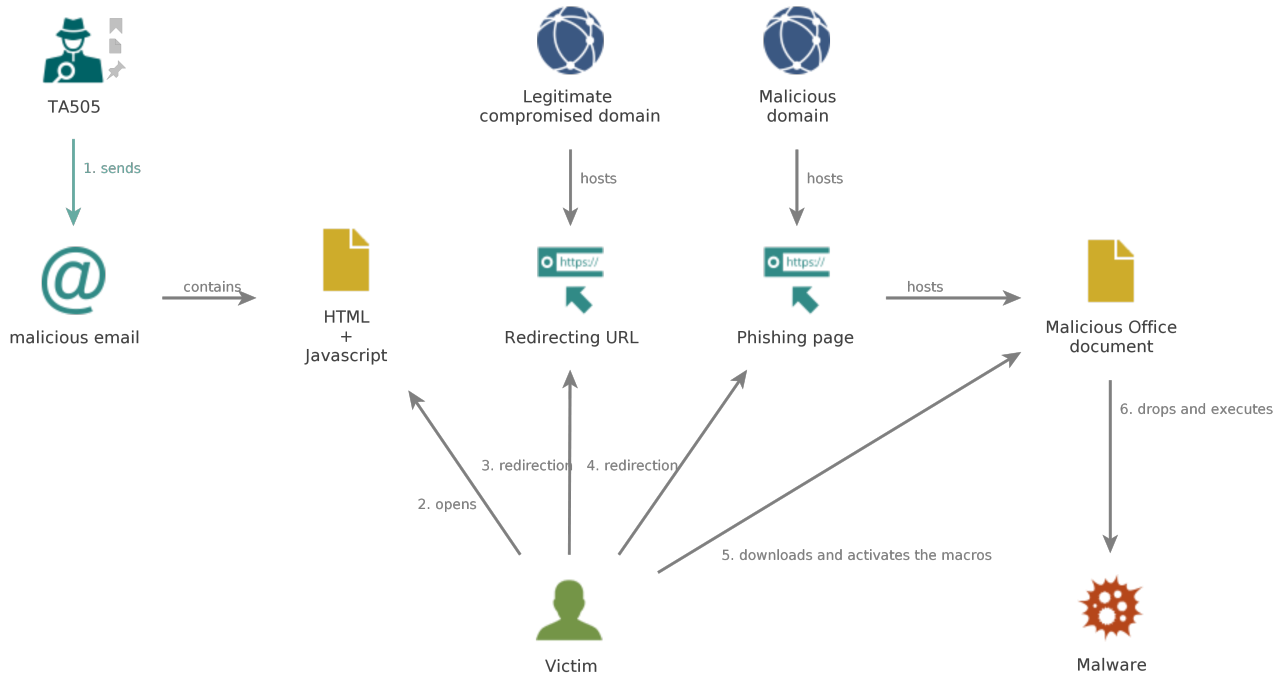

Fig. 2.1: Initial TA505 compromise method

The intrusion set gradually increases the complexity of its social engineering method. In October 2019, it is thought to have directly sent links towards phishing pages in its malicious emails. It then used URL shorteners to mask these malicious links.

In late February 2020, it abandoned the URL shortener strategy and started to use HTML attachments with Javascript with redirection from a compromised site, which made it even more difficult to detect its emails. Furthermore, some of its redirection pages integrate a link towards iplogger.org, a service allowing the intrusion set to inspect IP addresses visiting these pages[21].

Finally, it has already been observed that the phishing pages of the intrusion set distributed empty Office documents when a person other than the victim visited them. This behaviour can be explained by the fact that the intrusion set filters the IP addresses to which it chooses to distribute its malicious documents or only distributes them within limited time slots.

2.3 Initial compromise

TA505 has a varied attack arsenal to be deployed among its victims having run its malicious attachments. It consists of codes available both publicly and commercially on the black market or which seem to be exclusive to it. It therefore has malware development capabilites or financial resources to obtain them. The intrusion set deploys its arsenal in several stages and has different codes for each of them.

2.3.1 Stage 1 codes

The TA505 intrusion set seems to have tested several stage 1 codes[11]. It briefly used the following codes:

[11] a stage 1 code is defined here as an implant with limited features aimed at deploying a more sophisticated code and possibly rapidly performing reconnaissance of the infected system to help the intrusion set determine if the victim and their IS are of interest.

- **Quant Loader** is a simple, low-cost downloader available on the black market. The intrusion set used it from January to April 2018 [9].
- **Marap** is a downloader that seems specific to the intrusion set. Athough it has a modular structure and a known reconnaissance module, few attacks using this code have been documented and the intrusion set does not seem to have used it since August 2018 [22].
- **Amadey** is a downloader available on the black market. This code is thought to have been used from April to June 2019 by the intrusion set [23].
- **Andromut**, also known as **Gelup**, is a downloader that seems specific to the intrusion set. This code differs from the previous ones by setting up anti-analysis mechanisms. However, no occurrence of this code seems to have been detected apart from in summer 2019 [24].

The TA505 intrusion set therefore does not seem to hesitate to discard some of its malwares in order to test others. Despite that, a trend does emerge: it seems to more regularly use the stage 1 malware **Get2**, whose backdoor component is also called **Friendspeak** [13]. Since the first publication of this malware in September 2019 [19], the intrusion set regularly uses it.

Get2 performs a basic reconnaissance of the machine it infects by sending to its C2 server information such as the name of the infected machine, the name of the user, the version of the Windows operating system and list of active processes on the machine. In return, if the machine is deemed to be of interest, it receives the URL to which it can upload the next stage malware.

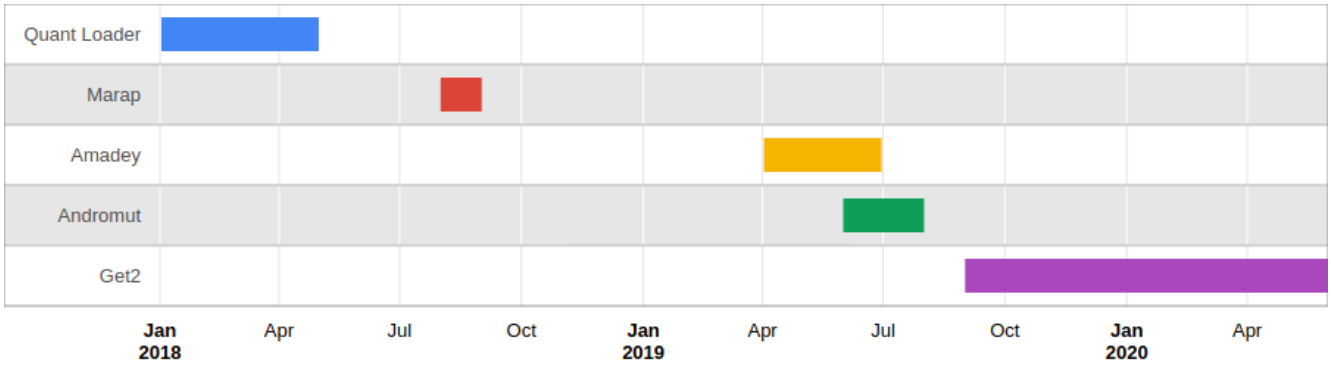

Fig. 2.2: Timeline of the stage 1 codes used by TA505

2.3.2 Second-level codes

Once its stage 1 code has been deployed, the intrusion set can deploy several malwares.

- The **FlawedAmmyy** malware exists since 2016 and is built from the source code of the publicly disclosed legitimate remote-administration tool Ammyy Admin. Although it has RAT[12] features, **FlawedAmmyy** has also been used by the intrusion set as a stage 1 code. The intrusion set is thought to have used it between March 2018 and September 2019 [18]. **FlawedAmmyy** seems to be exclusively used by TA505 since 2018. However, this backdoor is thought to have been used before this time period, when TA505 did not use this type of code yet. It is therefore not entirely confirmed that **FlawedAmmyy** is exclusive to TA505.
- The **tRat** malware was used by TA505 in October 2018 [16]. Little information is available about this door. Modules need to be downloaded for the backdoor to acquire features, yet none of its modules have been documented.
- Remote Manipulator System, also called RMS or RmanSyS, is a legitimate tool developed by the Russian company TEKTONIT, used for malicious purposes. This tool is available free of charge for non-commercial purposes and corrupted versions are also available on the black market. TA505 is thought to have started to deploy this tool from November 2018, and until June 2019 [25].

[12] *Remote Administration Tool*

- The **ServHelper** backdoor comes in two [17] versions: one version acts as a stage 1 code, the other has RAT features. The intrusion set is supposed to have used this backdoor over a period covering at least from November 2018 to August 2019 [18]. **ServHelper** does not seem specific to the intrusion set: several IT security researchers have observed attacks in which it was involved but also using methods and tools that are different from those of TA505 [5][18][26].
- **FlawedGrace**, also known as **Gracewire**, is a backdoor with standard RAT features. It was mentioned for being used for the first time by TA505 in December 2018 [17] and is thought to be still used by it in 2020 [27]. Like **FlawedAmmyy**, TA505 seems for the time being to be the only one to use this backdoor. However its existence prior to 2018 makes it uncertain whether it was used by TA505 exclusively.
- The **FlowerPippi** backdoor was detected once in June 2019 [11]. This malware has basic RAT features and it is also designed to be used as a stage 1 code by offering initial recognition of the infected system.
- **SDBbot** is a malware that seems to be specific to the intrusion set. Its first use was probably September 2019 [20] and the intrusion set has constantly used it since.

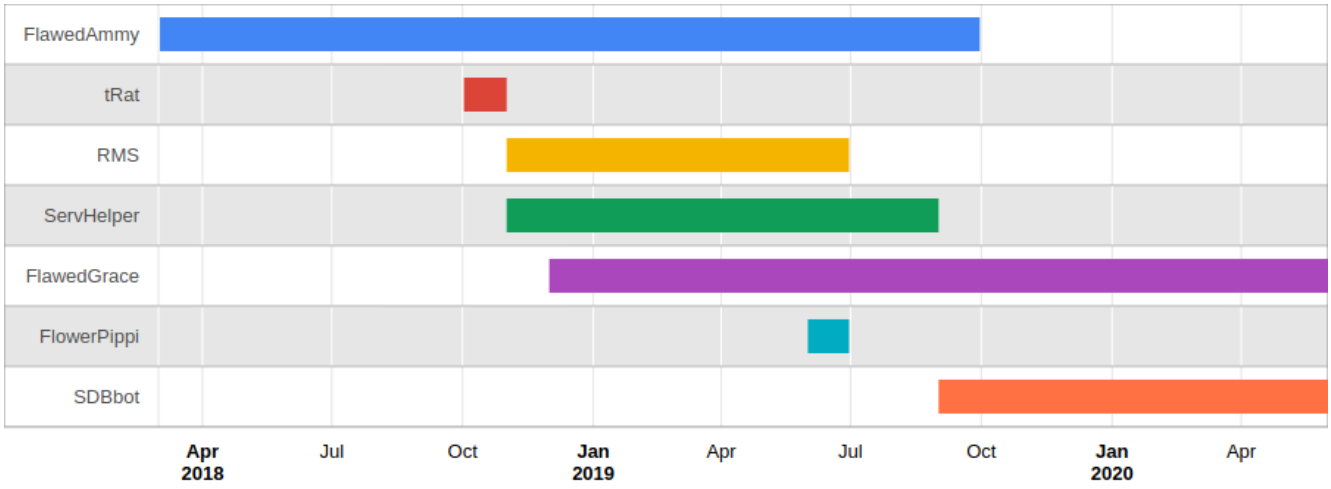

Fig. 2.3: Timeline of the stage 2 codes used by TA505

2.4 Compromising of the information system

Once its malwares are installed, the intrusion set can try to lateralise itself within a compromised network. Its goal is to become the domain administrator. To achieve this, it uses several methods.

2.4.1 Exploration of the IS

The intrusion set scans the network to collect more information on the IS and discover vulnerable services [28]. One of the tools used by TA505 is the PowerSploit suite, a set of PowerShell scripts available in open-source and used to test the security of an IT network. The intrusion set particularly focuses on the *Active Directory* of the IS and has already deployed in the past another penetration test tool, PingCastle, to test configuration weaknesses affecting that service.

Although crucial to take over the network, the intrusion set does not necessarily seem to perform these operations first. In several cases observed, the intrusion set firstly tends to try to compromise several other machines before scanning the IS and the *Active Directory*.

The intrusion set seems to continue its network mapping work after having compromised the credentials of a domain administrator. It has already been observed that TA505 used a query software of *Active Directory* called AdFind on a domain controller to fully map an IS of which it had become the domain administrator.

2.4.2 Increasing privileges

The method preferred by TA505 to increase its privileges and lateralise throughout a network seems to be the collection of credentials on compromised machines. The Mimikatz collection tool, available free of charge in open-source, is regularly used by the intrusion set and other tools of this type may also have been used. Unconfirmed hypotheses have also been made on the use of MS17-010 vulnerability [13] by the intrusion set [28].

2.4.3 Lateralisation

To facilitate its lateralisation operations and increase its robustness within a compromised network, the intrusion set has very frequently used Cobalt Strike, a penetration testing framework, and the TinyMet tool[14]. However, TA505 also often uses native Window tools such as WMIC and RDP to run its malware on new machines by using stolen credentials.

2.5 Actions on objective

2.5.1 IS encryption

The main goal of the intrusion set is to deploy ransomware. The use of ransomware by this intrusion set goes back to at least 2016 with its use of the **Locky** malware.

Major developments since 2018 can be explained by the fact that TA505 now seeks to use ransomware to compromise entities liable to pay a high ransom (*big game hunting*) and to encrypt all the machines of the compromised IS.

During TA505-related attacks, **Clop** ransomware, also called **Ciop**, was deployed. This malware was observed for the first time in February 2019 [20]. It has no automatic propagation functions. Consequently, the intrusion set uses some specific tools to deploy it within a whole IT system. Using a script, it deploys a malware, poorly documented in open-source but until now systematically called « `sage.exe` » by the intrusion set, on several machines [28]. These machines then connect to all the machines of the victim IS to successively run two payloads on each of them with a domain administrator account:

- a malware called **DeactivateDefender** whose aim is precisely to disable Windows Defender [20][28];
- the ransomware itself.

It is probable that TA505 relies on the network mappings performed during the gradual compromission of the IS to choose the machines on which to run « `sage.exe` » and maximise the impact of its ransomware.

An occurrence of use of the **Rapid** ransomware by TA505 was also observed by the South Korean Financial Security Institute (FSI) [20] in December 2019.

2.5.2 Blackmail

A website was created in March 2020 to publish exfiltrated data of **Clop** ransomware victims not having paid their ransom, probably to increase pressure on future victims. A release was published by the attackers stating that should a hospital be accidentally victim of their ransomware, the data decrypter would be immediately provided. If, as sugested in section 2.5.3, **Clop** is specific to TA505, this illustrates the capability of this intrusion set to follow a trend initiated by other ransomware operators [29].

This trend is also interesting as it indicates that the intrusion set is required to exfiltrate data of its victim's IS. If such data were to exceed a certain volume, it is then probable that TA505 needs to deploy specific tools and infrastructure for this task. Such things have not yet been observed for this intrusion set.

[13] Critical vulnerability in the SMB service(*Server Message Block*) of Windows-run machines. This vulnerability was used during the WannaCry international campaign in 2017.

[14] This tool, freely available in open-source, is a particularly small loading code used to download and run the Meterpreter penetration testing tool.

2.5.3 Spécificity of Clop for TA505

ANSSI had mentioned a technical link between **Clop** ransomware and TA505. Indeed, **Clop** and **FlawedAmmyy** had been signed by the same valid but malicious security certificate [30].

To this, it is possible to add that these two malwares were compiled in similar environments and modified at the same time to change the letter « `l` » into « `i` » uppercase [20] in their chains. Furthermore, they have the same characteristic name « `swaqp.exe` » in separate attacks.

It therefore seems probable that one single intrusion set handles both codes. Given that TA505 is the only one to have been seen to use them since 2018, it seems that both codes are specific to it.

2.6 Evasion methods

The intrusion set multiplies strategies to minimise the detection of its malware. Besides the use of attached document with unusual formats mentioned in section 2.2, TA505 has also used Excel 4.0 type macros. These very old macros were not often detected by security solutions during their adoption by the intrusion set. Likewise, TA505 relies heavily on native Windows tools, which require closer supervision of the IS to detect their malicious use.

2.6.1 Use of compression codes

TA505 uses a compression code[15] to make it more difficult to analyse its malware. This code, called **Minedoor** [13], was used to compress both early stage malwares such as **FlawedGrace**, and final codes deployed by TA505 such as **Clop** or **DeactivateDefender** [31].

Although this compression code is a valuable way to monitor TA505's arsenal, caution is required. Attacks using codes protected by **Minedoor** with very different kill chains from that of TA505 have already been observed [13]. It therefore seems that this code is not specific to TA505.

2.6.2 Use of siged binaries

The intrusion set signs its malware by using legitimate but malicious security certificates. They often take over names of existing businesses. TA505's codes are therefore more difficult to detect [20].

Like the **Minedoor** malware, it is not certain that all the malware signed by the certificates used by TA505 are linked to this intrusion set. Indeed it may be that TA505 used a third party to sign its codes and that this same third party may reuse those certificates to sign the malware of other intrusion sets.

2.7 Attack infrastructure

As mentioned in section 2.1, the infrastructure used by the intrusion set to distribute its emails is not widely documented.

TA505 particularly seems to rent its infrastructure to conduct its operations, in particular to host its malicious Office documents and for its **Get2** C2 servers[16]. The life cycle of this infrastructure is usually less than a month and the intrusion set permanently generates new domain names. These domain names often consist of several words separated by « - » and usually try to typosquat[17] file-sharing services such as Onedrive ou Onehub for example.

TA505 is thought to use a different strategy for the C2 servers of its penetration tools such as TinyMet or Cobalt Strike. It directly uses IP adresses as C2 servers and not domain names but still relies on a rented infrastucture.

[15] Called *packer*.
[16] Command and control servers: these machines are used to send instructions to malware and receive results.
[17] Show strong similarities with another domain name for misleading purposes.

Little information is available about the infrastructure compromised by TA505. Web servers compromised by the intrusion set were analysed in February 2019 [20], indicating that several copies of the malicious web console **Filesman** had been found as well as a non-documented Linux backdoor.

2.8 Targeting

Although they only represent a fraction of the intrusion set's real activity, the table below presents a set of campaigns conducted by TA505, documented in open-source since 2018.

Period	Targeted geographical area	Targeted sector	Source
January 2018	N/A	Automotive industry	[14]
August 2018	N/A	Financial	[22]
September-October 2018	N/A	Financial	[32]
November 2018	N/A	Financial Retail	[17]
December 2018	N/A	Financial Retail	[17]
November-December 2018	United States	Food industry Distribution Retail Catering	[33] [34]
December 2018 – March 2019	Chile, India, Italia, Malawi, Pakistan, South Africa, South Korea, China, United Kingdom, France, United States	Financial Hospitality	[25]
February 2019	South Korea	N/A	[20]
April 2019	N/A	Financial	[35]
April 2019	Chile, Mexico, Italia, China, South Korea, Taiwan	N/A	[23]
June 2019	United Arab Emirates, South Korea, Singapore, United States, Saudi Arabia, Morocco	N/A	[11]
June-July 2019	United States, Bulgaria, Turkey, Serbia, India, Philippines, Indonesia	Banks	[19] [18] [11]
June 2019	Japan, Philippines, Argentina	N/A	[11]
July-August 2019	Saudi Arabia, Oman	Government agency	[18]
July-August 2019	Turkey	Government agency Education	[18]
September 2019	Canada, United States	N/A	[19]
September 2019	Greece, Singapore, United Arab Emirates, Georgia, Sweden, Lithuania	Financial	[19] [18] [36] [11]
October 2019	United Kingdom, France, United States	Financial, Healthcare, Retail, Education Research	[19]
December 2019	South Korea	N/A	[20]
December 2019	Germany, Netherlands	Education	[37]
January-March 2020	United States	Pharmaceutical Healthcare Retail	[27] [19]

The financial sector used to be the exclusive target of the intrusion set before 2018 and has remained a regular target since.

TA505 has however gradually expanded its victim profile to other new sectors.

From a geographical point of view, all the continents are targeted by this intrusion set. A point of interest is the special attention TA505 seems to pay to South Korea. This interest could be linked to the fact that the intrusion set could have been working in connection with the Lazarus intrusion set as mentioned in chapter 3.

3 Links with other attacking groups

3.1 Clients

Given its varied arsenal, the broadness of its targets, its sometimes massive, sometimes targeted campaigns, TA505 could well be a *hacker-for-hire* i.e. a provider of IS compromise and access qualification services. Its clients will provide it with a list of potential targets which TA505 will try to compromise, to then sell these compromised or qualified accesses to clients.

At least two potential clients have been identified by editors: the Lazarus intrusion set known to be tied to North Korean interests in open-sources and the Silence [38] group.

3.1.1 Lazarus

The simultaneous presence of Lazarus and TA505 has already been observed by different sources. In early January 2018, the Vietnamese CERT issued an alert relating to attacks targeting the financial sector, combining indicators of compromise attributed to intrusion sets linked to North Korean interests in open-sources to others attributed to TA505 [39]. According to Lexfo, IOCs found simultaneously on bank networks and Powershell scripts, attributed to TA505 and to Lazarus, seem similar [40].

*Comment: As **Dridex** was used by Lazarus during the Bangladesh Bank heist in 2016, it is legitimate to query the prior opening of access by a cybercriminal group before the intrusion by Lazarus. [41].*

In addition, the specific targeting of South Korea by TA505 could indicate an order from a final client such as an intrusion set known to be linked in open-sources to North Korean interests.

3.1.2 Silence

There are code and infrastructure links between **FlawedAmmyy** and **Truebot** (aka **Silence.Downloader**), a remote administration tool specific to Silence[18]. According to the Group-IB editor, **FlawedAmmyy.downloader** and **Truebot** were developed by the same individual [42]. Furthermore, Silence is thought to have attacked at least one bank in Europe via TA505 in order to compromise its IS [43].

Comment: If Silence does indeed call on TA505 for the initial compromise, it would be to change the TTPs, as Silence, from its beginning, in 2016, is autonomous in the sending of phishing emails and initial compromise.

3.2 FIN7

According to the Korean Financial Security Institute (FSI) [20], there are similarities between TA505 and the FIN7 cybercriminal group, the successor to Carbanak and now specialising in the theft of credit card information. The two groups are thought to:

- share the IPs of joint C2 servers ;
- use **FlawedAmmyy**, Cobalt Strike and TinyMet (BabyMetal for FIN7);
- use *batch script* for internal recognition purposes;
- be lateralised through the RDP protocol and PSExec;
- use Shim Database (SDB) in the same way. This particularity is also highlighted by Proofpoint [19].

Comment: FIN7 and TA505 could in fact be working together. It seems that the FSI observed that an infection chain in line with those of TA505 deployed malware targeting POS terminals (PoS systems), belonging to FIN7.

[18] Russian-speaking cybercriminal group specialising in compromising ATMs for fraudulent cash withdrawals [38].

4 Conclusion

Despite the scale of its activity as an affiliate of **Dridex** and **Locky**, TA505 was only identified as such in 2017, at the same time as its first uses of backdoors.

Often mistaken for the Evil Corp cybercriminal group (operating the Dridex botnet and BitPaymer ransomware), and sometimes considered to be the operator of the Necurs botnet, TA505 uses a scalable attack arsenal which it implements in varied and sometimes simultaneous campaigns, casting confusion over its motives. As such, the ties it has with Lazarus and Silence suggest that TA505 conducts parallel campaigns for its own behalf and campaigns for its clients.

The scale of its campaigns since 2019 and its targeting of several sectors in France, make this intrusion set a threat of special concern in 2020.

5 Appendix: the Necurs botnet

5.1 Return of the Necurs botnet

The Necurs botnet (alias CraP2P) first appeared in 2011 [44].

Two known botnet modules are:

- spam, used for example:
  - during *pump and dump* campaigns (especially relating to cryptoassets) as in March 2017;
  - in 2018, when Necurs acquired a new module *.NET spamming* [45]);
  - between 2016 and 2017, when Necurs propagated the **Kegotip** banking Trojan through **The Uprate loader** and **The Rockloader**[19], (Loader used to recover email addresses available in hard disks and to use them in future spam campaigns [47];
  - after the dismantling of the Kelihos botnet in 2017, when Necurs was thought to have retrieved some of its business, in particular consisting of *dating spam*.
- proxy/DDoS (addition of the DoS module in February 2017) [3].

The Necurs botnet communicates with its operators in different ways [48]:

- Its main communication network consists of a list of IP addresses and static hard-coded domains in the sampling of Necurs malware;
- If this method is not capable of obtaining an active C2, Necurs uses its domain generation algorithm (DGA): the main DGA produces 2048 C2 domains every 4 days. When Necurs operators record a DGA domain to inform bots of the existence of a new C2, the domain does not indicate the real IP address of the C2. This IP address is obfuscated with an encryption algorithm. All the domains are tried out until one of them matches and replies using the right protocol;
- If this method also fails, the C2 domain is recovered on the P2P network.

Furthermore, the C2 infrastructure is divided into three levels. The last is the *C2 backend*. In this way, an infected system communicates with at least two layers of the C2 proxy when it is trying to communicate with the *C2 backend*. The first C2 layer consists of cheap private virtual servers located in countries like Russia or the Ukraine whereas the second layer is usually hosted in Europe, sometimes Russia. There are thought to be 11 Necurs botnets, i.e. 11 *C2 backends*, tightly controlled by one single group [4]. Four of these botnets represent 95% of all infections [48, 49].

5.2 Massive distribution by Necurs

From 2016 to 2019, Necurs was the most frequently used method to deliver spams and malware for cybercriminals, and responsible for 90% of malware distributed by email worldwide. 1 million systems were infected in 2016 rising to 9 million on 10 March 2020 [49].

Between 2016 and 2017, Necurs mainly distributed **Locky**, **Jaff** (copy cat of **Locky**, **GlobeImposter**, **Philadelphia**, **Lukitus** and **Ykcol** (variants of **Locky**) and **Scarab** ransomware, as well as **Dridex** and **TrickBot** banking Trojans.

As of August 2018, Necurs started to roll out phishing campaigns targeting financial institutions, while continuing its massive propagation of (**FlawedAmmyy**, **Quant Loader**, **AZOrult**, **ServHelper**) malware, a majority of which belongs to TA505's arsenal.

In 2020, Necurs lost clients to **Emotet**, which replaced it in the distribution of **Dridex** and **TrickBot** [50], and distributed massive *get-rich-quick* spam campaigns. Its daily infections are mainly located in India, Indonesia, Iran,

[19] Loader used during compromises to propagate **Locky**, **Dridex** 220, **Pony** and **Kegotip** ransomware [46].

Mexico, Turkey, Vietnam and Thailand. 4892 infections have been located in France. [48, 49].

TA505 is thought to have massively distributed malware via the Necurs botnet, to such an extent that it is possible that the group actually operates this botnet, or at least is very closely tied to its real operator.

Comment: although it is possible that TA505 and the operator of the Necurs botnet have been mistaken for each other, it appears that the open-source tends to attribute all campaigns propagated by Necurs to TA505 through to at least late 2017 (pump-and-dump spam campaigns and other frauds being excluded), whereas it is a gigantic botnet probably used by cybercriminal groups other than TA505. Indeed, users of remote-controlled botnets, are often capable of renting out access to segments of their botnet on the black market to send DDoS, span campaigns etc.

6 Bibliography

[1] Proofpoint. *Threat Actor Profile: TA505, From Dridex to GlobeImposter*. Sept. 27, 2017. URL: https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter (visited on 05/03/2019).

[2] CERT-FR, "Le Code Malveillant Dridex : Origines et Usages". In: (May 25, 2020).

[3] BITSIGHT, *Dridex: Chasing a Botnet from the Inside*. Jan. 1, 2015.

[4] Bit Sight. *Dridex Botnets*. Jan. 24, 2017. URL: https://www.bitsight.com/blog/dridex-botnets (visited on 04/09/2020).

[5] TWITTER, "@Kafeine". In: (Jan. 1, 2019).

[6] Secureworks. *Evolution of the GOLD EVERGREEN Threat Group*. May 15, 2017. URL: https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group (visited on 04/24/2020).

[7] PROOFPOINT, "High-Volume Dridex Banking Trojan Campaigns Return". In: (Apr. 4, 2017).

[8] Palo Alto. *Locky: New Ransomware Mimics Dridex-Style Distribution*. Feb. 16, 2016. URL: https://unit42.paloaltonetworks.com/locky-new-ransomware-mimics-dridex-style-distribution/ (visited on 04/24/2020).

[9] Proofpoint. *TA505 Shifts with the Times*. June 8, 2018. URL: https://www.proofpoint.com/us/threat-insight/post/ta505-shifts-times (visited on 11/20/2019).

[10] SENSEPOST, "Macro-Less Code Exec in MSWord". In: (Oct. 9, 2017).

[11] Trend Micro. *Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi - Trend-Labs Security Intelligence Blog*. July 4, 2019. URL: https://blog.trendmicro.com/trendlabs-security-intelligence/latest-spam-campaigns-from-ta505-now-using-new-malware-tools-gelup-and-flowerpippi/ (visited on 11/27/2019).

[12] KOREA INTERNET & SECURITY AGENCY, *KISA Cyber Security Issue Report : Q2 2019*. Aug. 13, 2019.

[13] FireEye. *STOMP 2 DIS: Brilliance in the (Visual) Basics*. Feb. 5, 2020. URL: https://www.fireeye.com/blog/threat-research/2020/01/stomp-2-dis-brilliance-in-the-visual-basics.html (visited on 04/09/2020).

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

[15] PROOFPOINT, "TA505 Abusing SettingContent-Ms within PDF Files to Distribute FlawedAmmyy RAT". In: (July 19, 2018).

[16] PROOFPOINT, "tRat: New Modular RAT Appears in Multiple Email Campaigns". In: (Nov. 15, 2018).

[17] PROOFPOINT, "ServHelper and FlawedGrace - New Malware Introduced by TA505". In: (Jan. 9, 2019).

[18] Trend Micro. *TA505 At It Again: Variety Is the Spice of ServHelper and FlawedAmmyy*. Aug. 27, 2019. URL: https://blog.trendmicro.com/trendlabs-security-intelligence/ta505-at-it-again-variety-is-the-spice-of-servhelper-and-flawedammyy/ (visited on 04/24/2020).

[19] Proofpoint. *TA505 Distributes New SDBbot Remote Access Trojan with Get2 Downloader*. Oct. 15, 2019. URL: https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader (visited on 11/19/2019).

[20] KOREAN FINANCIAL SECURITY INSTITUTE, "Profiling of TA505 Threat Group". In: (Feb. 28, 2020).

[21] MICROSOFT SECURITY INTELLIGENCE, "Mise à Jour Dudear". In: (Jan. 30, 2020).

[22] PROOFPOINT, "New Modular Downloaders Fingerprint Systems, Prepare for More - Part 1: Marap". In: (Oct. 16, 2018).

[23] Trend Micro. *Shifting Tactics: Breaking Down TA505 Group's Use of HTML, RATs and Other Techniques in Latest Campaigns*. June 12, 2019. URL: https://blog.trendmicro.com/trendlabs-security-intelligence/shifting-tactics-breaking-down-ta505-groups-use-of-html-rats-and-other-techniques-in-latest-campaigns/ (visited on 04/09/2020).

[24] Proof Point. *TA505 Begins Summer Campaigns with a New Pet Malware Downloader, AndroMut, in the UAE, South Korea, Singapore, and the United States*. July 2, 2019. URL: https://www.proofpoint.com/us/threat-insight/post/ta505-begins-summer-campaigns-new-pet-malware-downloader-andromut-uae-south (visited on 04/09/2020).

[25] Cyberint. *Legit Remote Admin Tools Turn into Threat Actors' Tools*. Jan. 1, 2019. URL: https://e.cyberint.com/hubfs/Report%20Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%20Tools/CyberInt_Legit%20Remote%20Access%20Tools%20Turn%20Into%20Threat%20Actors%27%20Tools_Report.pdf (visited on 04/24/2020).

[26] Blueliv. *TA505 Evolves ServHelper, Uses Predator The Thief and Team Viewer Hijacking*. Dec. 17, 2019. URL: https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/research/servhelper-evolution-and-new-ta505-campaigns/ (visited on 04/09/2020).

[27] US-Cert. *COVID-19 Exploited by Malicious Cyber Actors*. Apr. 8, 2020. URL: https://www.us-cert.gov/ncas/alerts/aa20-099a (visited on 04/24/2020).

[28] Fox IT *Reactie Universiteit Maastricht Op Rapport FOX-IT*. Feb. 5, 2020.

[29] Bleeping Computer. *Three More Ransomware Families Create Sites to Leak Stolen Data*. Mar. 24, 2020. URL: https://www.bleepingcomputer.com/news/security/three-more-ransomware-families-create-sites-to-leak-stolen-data/ (visited on 04/09/2020).

[30] ANSSI, "Informations Concernant Le Rançongiciel Clop". In: (Nov. 22, 2019).

[31] Deutsch Telekom. *TA505's Box of Chocolate - On Hidden Gems Packed with the TA505 Packer*. Mar. 26, 2020. URL: https://www.telekom.com/en/blog/group/article/cybersecurity-ta505-s-box-of-chocolate-597672 (visited on 04/09/2020).

[32] Cyware. *The Many Faces and Activities of Ever-Evolving Necurs Botnet*. Dec. 29, 2019. URL: https://cyware.com/news/the-many-faces-and-activities-of-ever-evolving-necurs-botnet-1e8d2734 (visited on 04/16/2020).

[33] Morphisec, "Morphisec Uncovers Global "Pied Piper" Campaign". In: (Nov. 29, 2018).

[34] Proofpoint, "TA505 Targets the US Retail Industry with Personalized Attachments". In: (June 12, 2018).

[35] Cybereason. *Threat Actor TA505 Targets Financial Enterprises Using LOLBins and a New Backdoor Malware*. Apr. 25, 2019. URL: https://www.cybereason.com/blog/threat-actor-ta505-targets-financial-enterprises-using-lolbins-and-a-new-backdoor-malware (visited on 04/09/2020).

[36] Yoroi. *TA505 Is Expanding Its Operations*. May 29, 2019. URL: https://yoroi.company/research/ta505-is-expanding-its-operations/ (visited on 04/09/2020).

[37] Bleeping Computer, "Ransomware Hits Maastricht University, All Systems Taken Down". In: (Dec. 27, 2019).

[38] CERT-FR, "Le Groupe Cybercriminel Silence". In: (May 7, 2020).

[39] Norfolk Infosec. *OSINT Reporting Regarding DPRK and TA505 Overlap*. Apr. 10, 2019. URL: https://norfolkinfosec.com/osint-reporting-on-dprk-and-ta505-overlap/ (visited on 04/09/2020).

[40] Lexfo, *The Lazarus Constellation*. Feb. 19, 2020.

[41] Nice Ideas. *Deciphering the Bangladesh Bank Heist*. Jan. 27, 2020. URL: https://www.niceideas.ch/roller2/badtrash/entry/deciphering-the-bengladesh-bank-heist (visited on 01/27/2020).

[42] Group-IB, "SILENCE 2.0". In: (Aug. 1, 2019).

[43] Group-IB. *Group-IB: New Financially Motivated Attacks in Western Europe Traced to Russian-Speaking Threat Actors*. Mar. 27, 2020. URL: https://www.group-ib.com/media/silence_ta505_attacks_in_europe/ (visited on 04/24/2020).

[44] Twitter. *@Kafeine*. Apr. 24, 2020. URL: https://pbs.twimg.com/media/ERxmxQnWAAM8Fmj.jpg (visited on 04/24/2020).

[45] Threatpost. *Necurs Botnet Evolves to Hide in the Shadows, with New Payloads*. Jan. 27, 2020. URL: https://threatpost.com/necurs-botnet-hide-payloads/142334/ (visited on 01/27/2020).

[46] Proofpoint. *Locky Ransomware: Dridex Actors Get In The Game*. Apr. 6, 2016. URL: https://www.proofpoint.com/us/threat-insight/post/dridex-actors-get-in-ransomware-with-locky (visited on 04/24/2020).

[47] Security Intelligence. *The Necurs Botnet: A Pandora's Box of Malicious Spam*. Apr. 24, 2017. URL: https://securityintelligence.com/the-necurs-botnet-a-pandoras-box-of-malicious-spam/ (visited on 04/24/2020).

[48] BitSight. *Joint Effort with Microsoft to Disrupt Massive Criminal Botnet Necurs*. Mar. 10, 2020. URL: https://www.bitsight.com/blog/joint-effort-with-microsoft-to-takedown-massive-criminal-botnet-necurs (visited on 04/24/2020).

[49] The Shadowserver foundation. *Has The Sun Set On The Necurs Botnet?* Mar. 15, 2020. URL: https://www.shadowserver.org/news/has-the-sun-set-on-the-necurs-botnet/ (visited on 04/24/2020).

[50] Threatpost. *As Necurs Botnet Falls from Grace, Emotet Rises*. Jan. 29, 2020. URL: https://threatpost.com/as-necurs-botnet-falls-from-grace-emotet-rises/152236/ (visited on 01/29/2020).

- 20/08/2020

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