TA505: A Brief History Of Their Time

blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time/

November 16, 2020

Threat Intel Analyst: ***Antonis Terefos (@Tera0017)***
Data Scientist: ***Anne Postma (@A_Postma)***

1. Introduction

TA505 is a sophisticated and innovative threat actor, with plenty of cybercrime experience, that engages in targeted attacks across multiple sectors and geographies for financial gain. Over time, TA505 evolved from a lesser partner to a mature, self-subsisting and versatile crime operation with a broad spectrum of targets. Throughout the years the group heavily relied on third party services and tooling to support its fraudulent activities, however, the group now mostly operates independently from initial infection until monetization.

Throughout 2019, TA505 changed tactics and adopted a proven simple, although effective, attack strategy: encrypt a corporate network with ransomware, more specifically the *Clop* ransomware strain, and demand a ransom in Bitcoin to obtain the decryption key. Targets are selected in an opportunistic fashion and TA505 currently operates a broad attack arsenal of both in-house developed and publicly available tooling to exploit its victims. In the Netherlands, TA505 is notorious for their involvement on the Maastricht University incident in December 2019.

To obtain a foothold within targeted networks, TA505 heavily relies on two pieces of malware: *Get2/GetandGo* and *SDBbot*. Get2/GetandGo functions as a simple loader responsible for gathering system information, C&C beaconing and command execution. SDBbot is the main remote access tool, written in C++ and downloaded by Get2/GetandGo, composed of three components: an installer, a loader and the RAT.

During the period *March* to *June 2020*, Fox-IT didn't spot as many campaigns in which TA505 distributed their proven first stage malware. In early *June 2020* however, TA505 continued to push their flavored GetandGo-SDBbot campaigns thereby slightly adjusting their chain of infection, now leveraging *HTML* redirects. In the meantime – and in line with other targeted ransomware gangs – TA505 started to operate a data leak platform dubbed *"CL0P^_- LEAKS"* on which stolen corporate data of non-paying victims is publicly disclosed.

The research outlined in this blog is focused around obtained Get2/GetandGo and SDBbot samples. We unpacked the captured samples and organized them within their related campaign. This resulted in providing us an accurate view on the working schedule of the TA505 group during the past year.

2. Infection Chain and Tooling

As mentioned above, the Threat Actor uses private as well as public tooling to get access, infect the network and drop Clop ransomware.

2.1. Email – XLS – GetandGo

Figure 1. Initial Infection

1. The victim receives an HTML attachment. This file contains a link to a malicious website. Once the file is opened in a browser, it redirects to this compromised URL.

2. This compromised URL redirects again to the XLS file download page, which is operated by the actor.

3. From this URL the victim downloads the XLS file, frequently the language of the website can indicate the country targeted.

4. Once the XLS is downloaded and triggered, GetandGo is executed, communicates with the C&C and downloads SDBbot.

2.2. SDBbot Infection Process

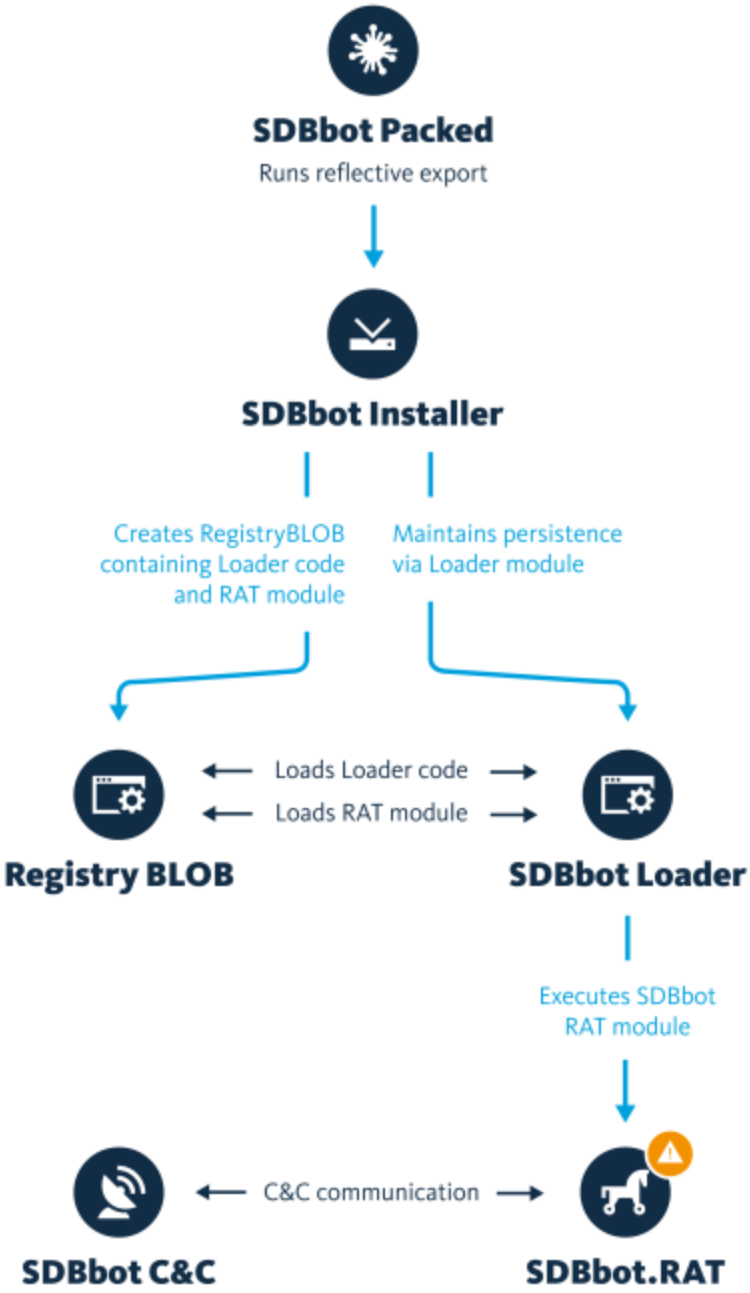


Figure 2. SDBbot infection

process

1. GetandGo executes the *"ReflectiveLoader"* export of SDBbot.

2. SDBbot contains of three modules. The Installer, Loader, RAT module.

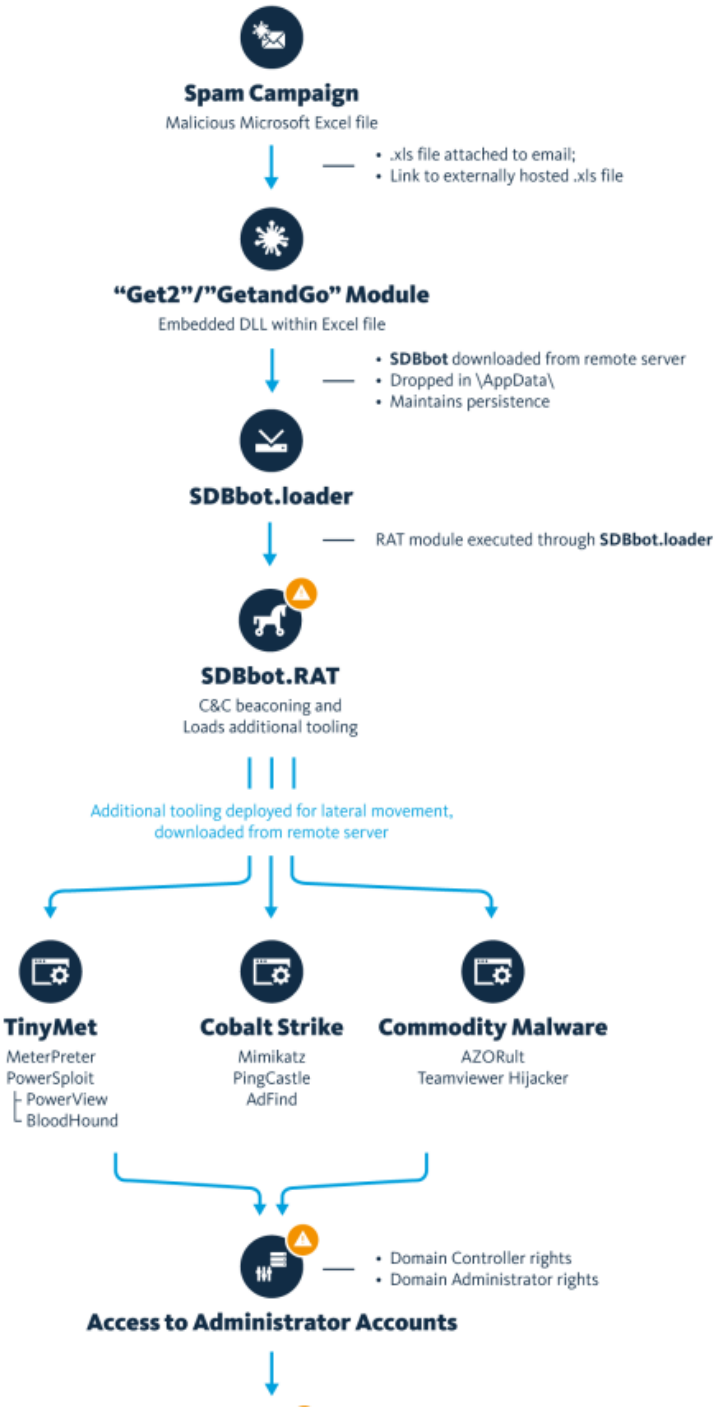
3.Initially the Installer module is executed, creates a Registry BLOB containing the Loader code and the RAT module.

4. The Loader module is dropped into disk and persistence is maintained via this module.

5. The Loader module, reads the Registry Blob and loads the Loader code. This loader code is executed and Loads the RAT module which is again executed in memory.

6. The RAT module communicates with the C&C and awaits commands from the administrator.

2.3. TA505 Infection Chain



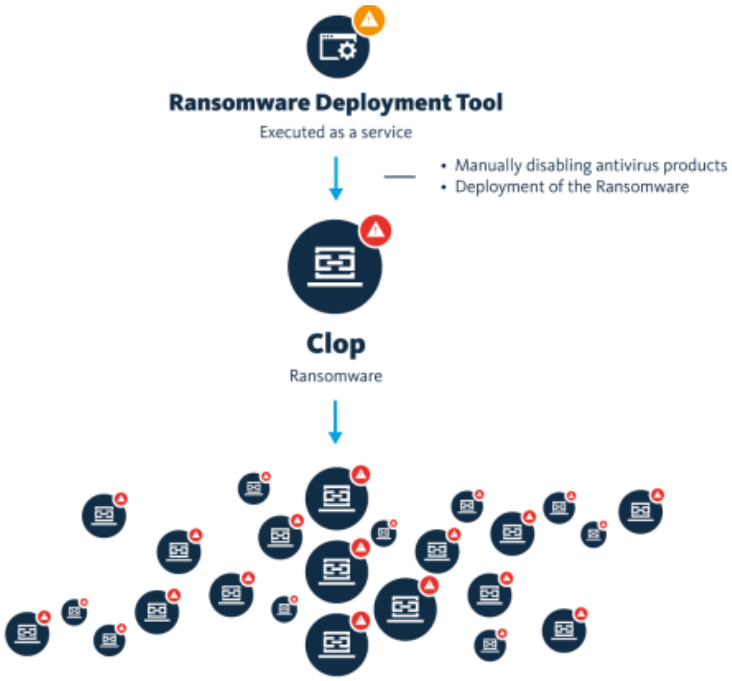


Figure 3. TA505 Infection Chain

Once SDBbot has obtained persistence, the actor uses this RAT in order to grab information from the machine, prepare the environment and download the next payloads. At this stage, also the operator might kill the bot if it is determined that the victim is not interesting to them.

For further infection of victims and access of administrator accounts, FOX-IT has also observed *Tinymet* and *Cobalt Strike* frequently being used.

3. TA505 Packer

To evade antivirus security products and frustrate malware reverse engineering, malware operators leverage encryption and compression via executable packing to protect their malicious code. Malware packers are essentially software programs that either encrypt or compress the original malware binary, thus making it unreadable until it's placed in memory.

In general, malware packers consist of two components:
• A packed buffer, the actual malicious code
• An "unpacking stub" responsible for unpacking and executing the packed buffer

TA505 also works with a custom packer, however their packer contains two buffers. The initial stub decrypts the first buffer which acts as another unpacking stub. The second unpacking stub subsequently unpacks the second buffer that contains the malicious executable. In addition to their custom packer, TA505 often packs their malware with a second or even a third layer of *UPX* (a publicly available open-source executable packer).

Below we represent an overview of the TA505 packing routines seen by Fox-IT. In total we can differentiate four different packing routines based on the packing layers and the number of observed samples.

		X64	X86
1	UPX(TA505 Custom Packer(UPX(Malicious Binary)))	0%	0.5%
2	UPX(TA505 Custom Packer(Malicious Binary))	13.7%	0%
3	TA505 Custom Packer(UPX(Malicious Binary))	0%	98.64%
4	TA505 Custom Packer(Malicious Binary)	86.3%	0.86%

TA505 Packing Routines
To aid our research, a Fox-IT analyst wrote a program dubbed *"TAFOF Unpacker"* to statically unpack samples packed with the custom TA505 packer.

We observed that the TA505 packed samples had a different *Compilation Timestamp* than the unpacked samples, and they were correlating correctly with the *Campaign Timestamp*. Furthermore, samples belonging to the same campaign used the same XOR-Key to unpack the actual malware.

4. Data Research

Over the course of approximately a year, Fox-IT was able to collect TA505 initial XLS samples. Each XLS file contained two embedded DLLs: a x64 and a x86 version of the Get2/GetandGo loader.

Both DLLs are packed with the same packer. However, the XOR-key to decrypt the buffer is different. We have "named" the campaigns we identified based on the combination of those XOR-Keys*: x86-XOR-Key:x64-XOR-Key* (e.g. campaign 0X50F1:0X1218). All of the timestamps related to the captured samples were converted to UTC. For hashes that existed on VirusTotal we used those timestamps as first seen; for the remainder, the Fox-IT Malware Lab was used.

Find below an overview on the descriptive statistics of both datasets:

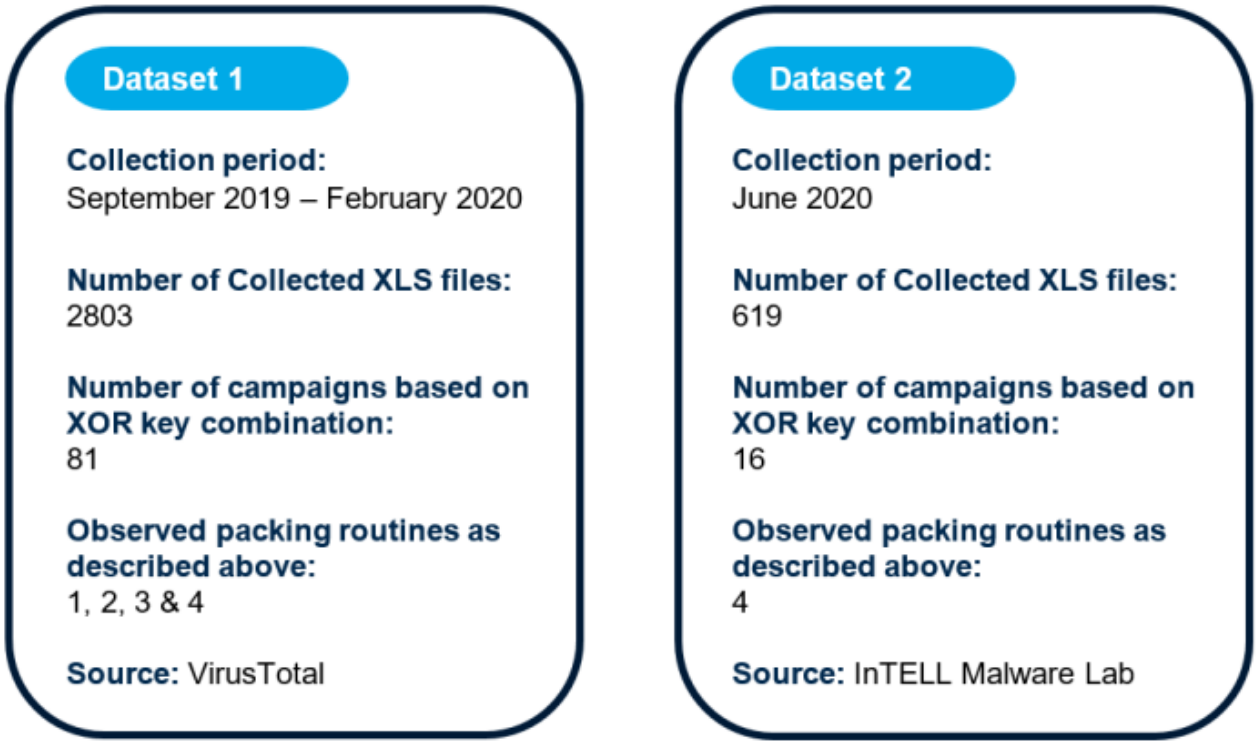


Figure 4. Datasets Statistics

4.1. Dataset 1, Working Hours and Workflow routine

During this period, we collected all the XLS files matching our TA505-GetandGo Yara rule and we unpacked them with TAFOF Unpacker. We observed that the compilation timestamps of the packed samples were different from the unpacked ones. Furthermore, the unpacked one was clearly indicating the malspam campaign date.

For the *Dataset 1*, we used the *VirusTotal* first seen timestamp as an estimation of when the campaign took place.

In the following graph we plotted all *81* campaigns (XOR-key combinations), and ordered them chronologically based on the C&C domain registration time.

What we noticed was, that we see relatively short orange/yellow/light green patches: meaning that the domain was registered shortly before they compiled the malware, and a few hours/days the first sample of this campaign was found on VirusTotal.

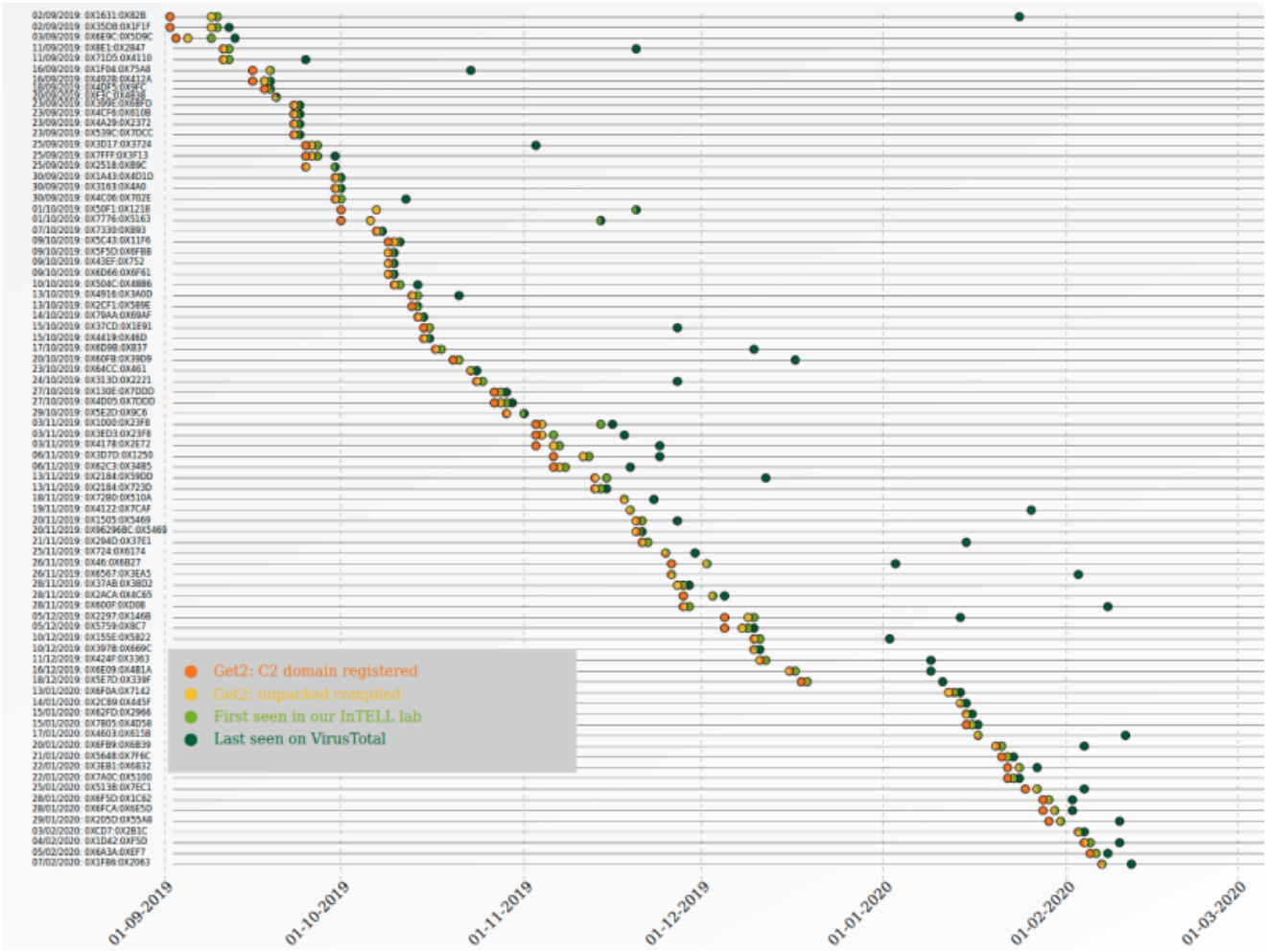


Figure 5. Dataset 1, Campaigns overview

As seen by the graph, it seems clear the workflow followed most of the times by the group: Registering the C&C, compiling the malware and shortly after, releasing the malspam campaign.

As seen on the *37%* of the campaigns, the first seen sample and compilation timestamp are observed within *12 hours*, while *79%* of the campaigns are discovered after *1 day* of the compilation timestamp and *91.3%* within *2 days*.

We can also observe the long vacations taken during the Christmas/New Year period (*20th December 2019* until *13th of January 2020*), another indication of Russian Cybercrime groups.

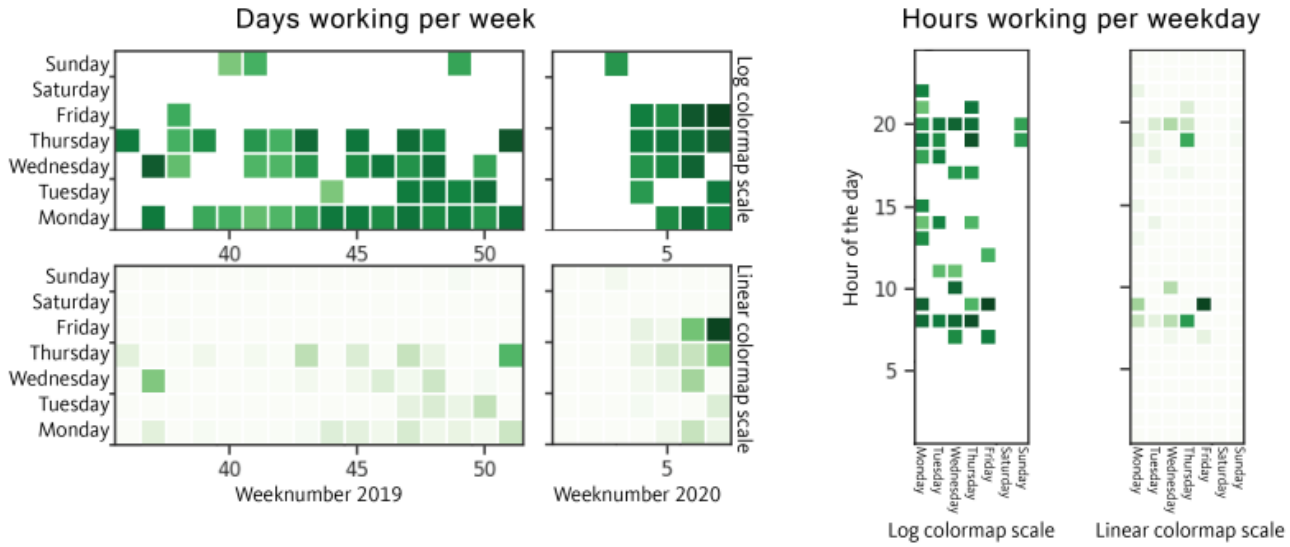


Figure 6. Dataset 1, Compilation Timestamps UTC

The group mostly works on Mondays, Wednesdays and Thursdays, less frequently Tuesdays, Fridays and Sundays (mostly preparing for Monday campaign). As for the time, earliest is usually 6 AM UTC and latest 10 PM UTC. Those time schedules give us once again a small indication about the time zone where the actor is operating from.

4.2. Dataset 2, Working Hours and Workflow routine

For the *Dataset 2*, we used as a source the first seen date of the *InTELL Malware Lab*. This dataset contains samples obtained after their time off. In this research we combined SDBbot data as well, which is the next stage payload of Get2. Furthermore, for this second dataset we managed to collect TA505 malspam emails from actual targets/victims indicating the country targeted from the email's language.

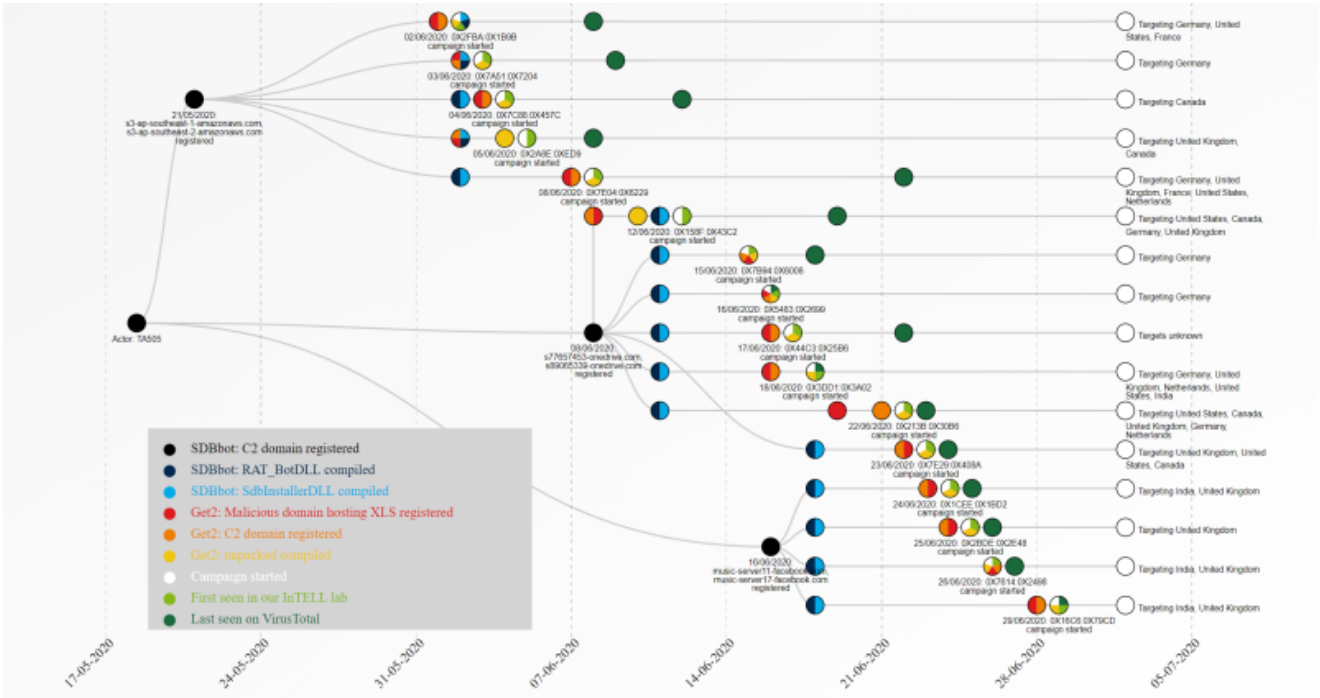


Figure 7. Dataset 2, Campaigns overview

From the above graph we can clearly behold, that multiple GetandGo campaigns were downloading the “same SDBbot” (same C&C). This information makes even more clear the actual use of the short lifespan of a GetandGo C&C, which is to miss the link with the SDBbot C&C (as happened for this research on the 24th of June). This allows the group for a longer lifespan of the SDBbot C&C, avoiding being easily detected.

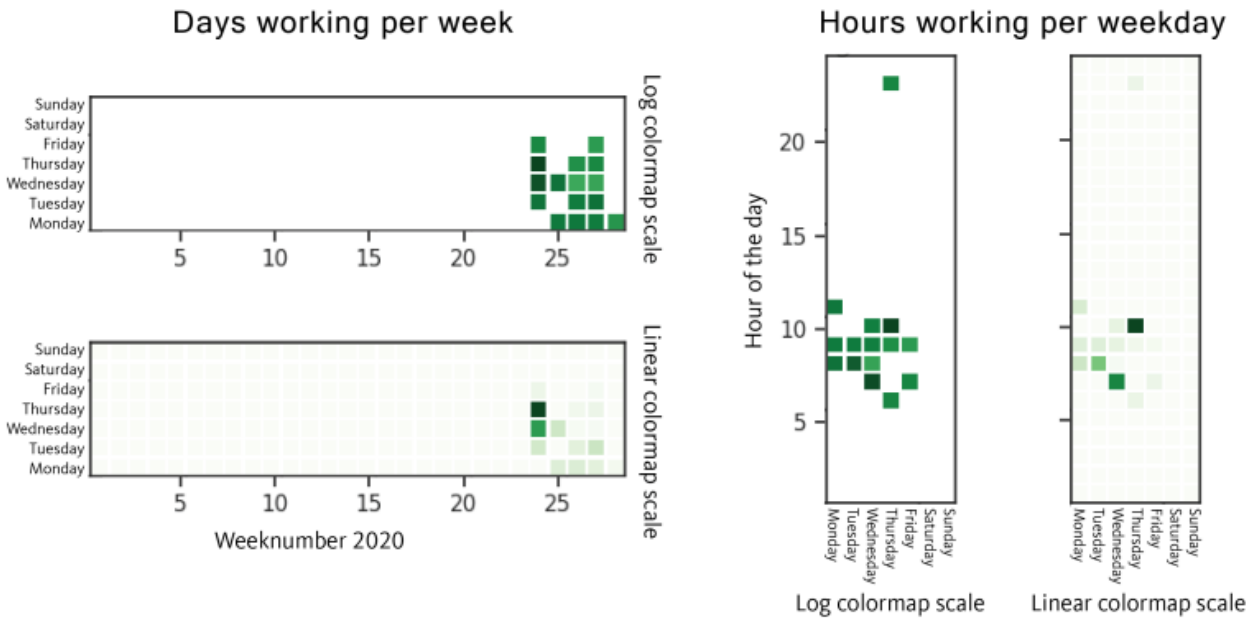


Figure 8. Dataset 2, GetandGo Compilation Timestamps UTC

The working days are the same since they restarted after their long time off, although now we see a small difference on the working hours, starting as early as 5 AM UTC until 11 PM UTC. This small 1 hour difference from the earliest working time might indicate that the group started “working from home” like the rest of the world during these pandemic times. However

as both periods are in respectively winter and summer time, it could also be related to daylight savings time. This combined with the prior knowledge that the group is communicating in Russian language this points specifically to Ukraine being the only majority Russian speaking country with DST, but this would be speculation by itself.

The time information does point however to a likely Eastern European presence of the group, and not all members have to be necessarily in one country.

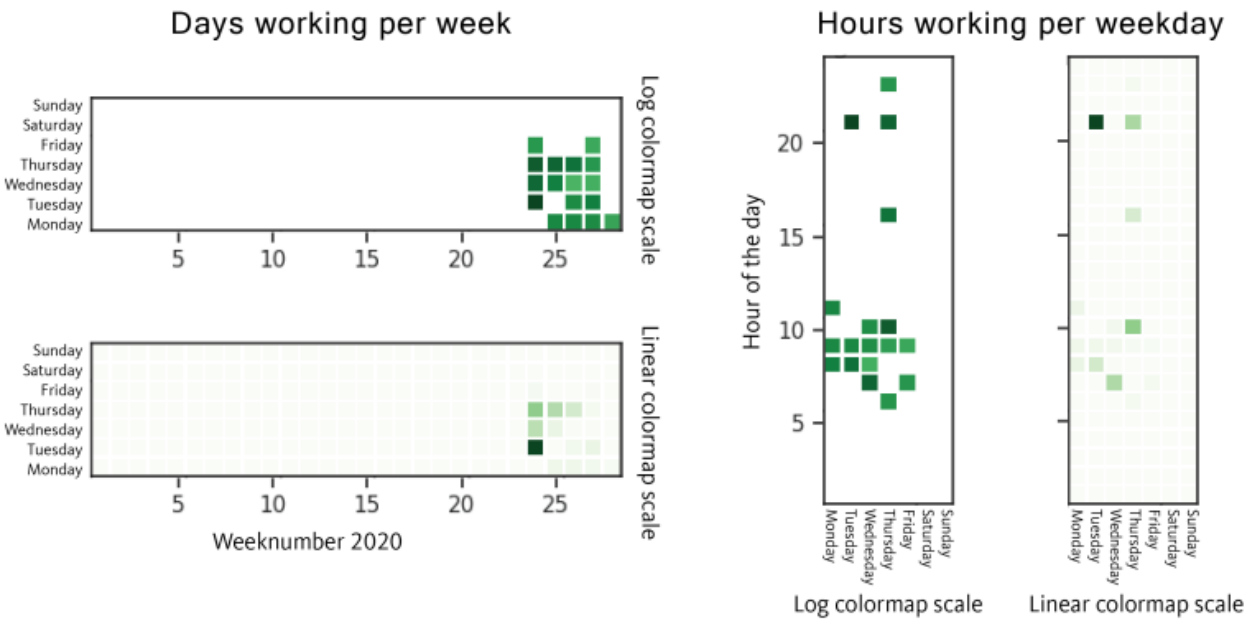


Figure 9. Dataset 2, GetandGo and SDBbot Compilation Timestamps UTC

When we plotted also the SDBbot compilation timestamps we observed that GetandGo is more of a morning/day work for the group as they need to target victims during their working schedule, but SDBbot is performed mostly during the evening, as they don't need to hurry as much in this case.

5. Dransom Time

"Dransom time, is the period from when a malicious attack enters the network until the ransomware is released."

Once the initial access is achieved, the group is getting its hands on SDBbot and starts moving laterally in order to obtain root/admin access to the victim company/organization. This process can vary from target to target as well as the duration from initial access (GetandGo) to ransomware (Clop).

Figure 10. Dransom Time 69 days

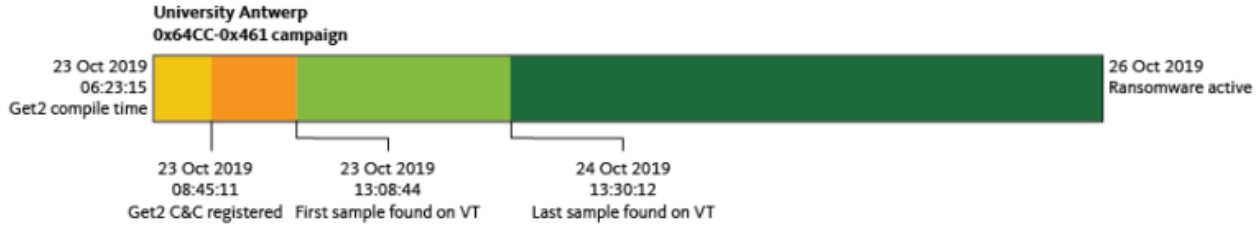


Figure 11. Dransom Time 3 days

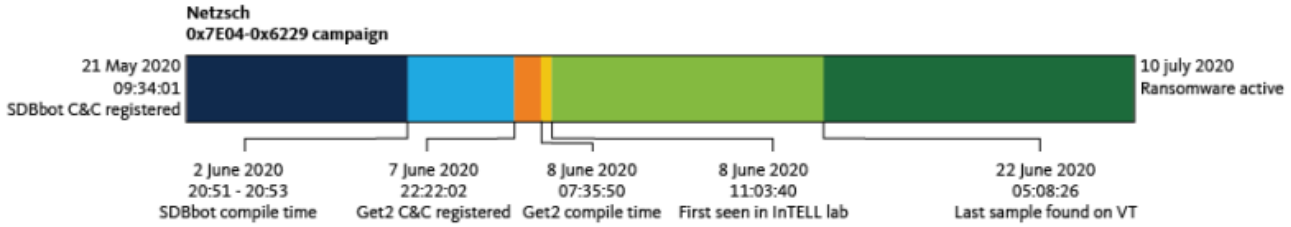


Figure 12. Dransom Time 32 days

The differences on the *Dransom time* manifests that the group is capable of staying undetected for long periods of time (more than 2 months), as well as getting root access as fast as their time allows (3 days).

* There are definitely more extreme *Dransom times* accomplished by this group, but the above are some of the ones we encountered and managed to obtain.

6. Working Schedule

With the above data at hand, we were able to accurately estimate the work focus of the group at specific days and times during the past year.

The below week dates are some examples of this data, plotted in a weekly schedule (time in UTC).

* Each color represents a different campaign.

6.1. Week 42, 14-20 of October 2019

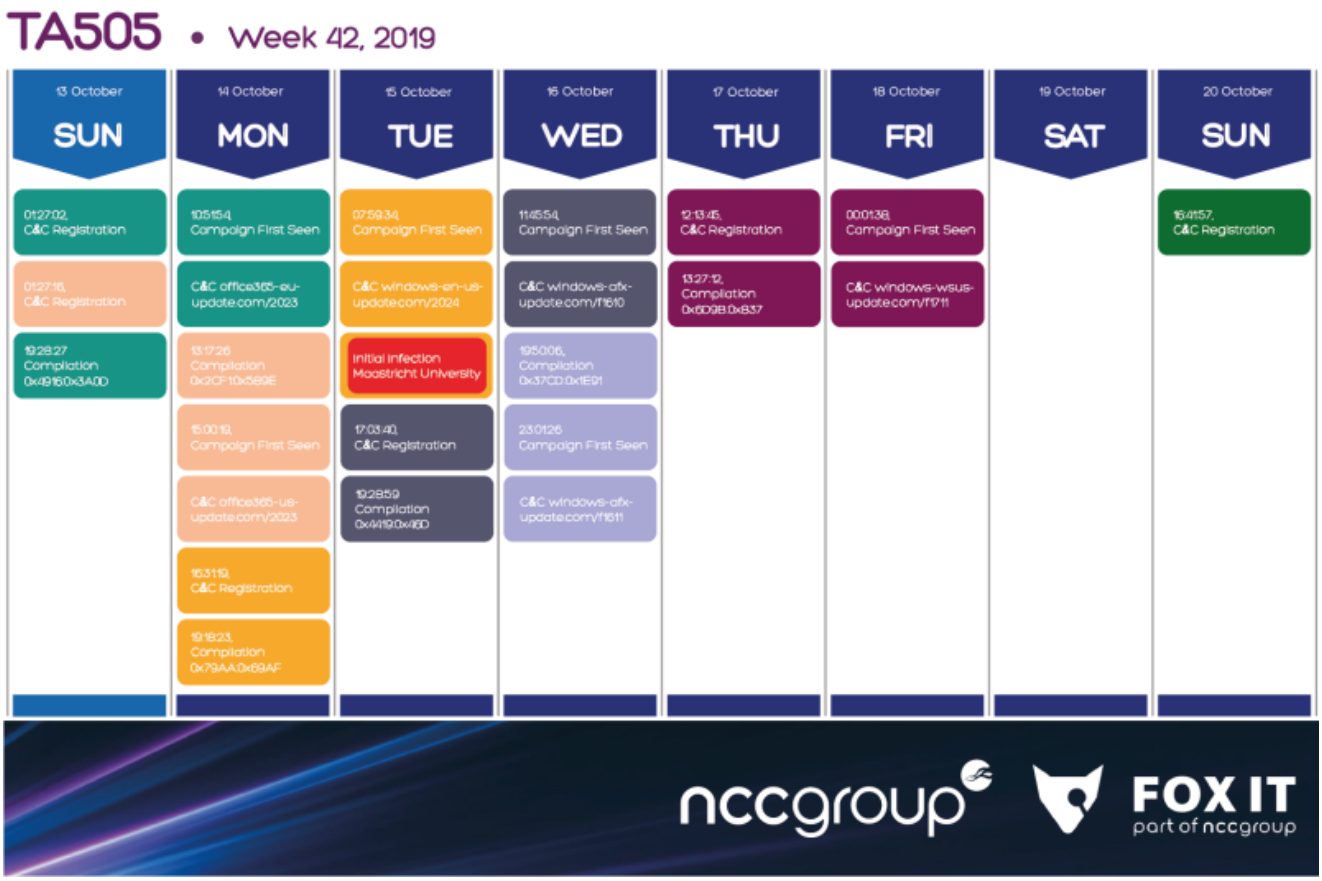


Figure 13. TA505 Weekly Schedule, week 42 2019

During this week, the group released six different campaigns targeting various geographical regions. We observe the group preparing two Monday campaigns on Sunday. And as for Tuesday, they managed to achieve the initial infection at Maastricht University.

On Wednesday, the group performed two campaigns targeting different regions, although this time they used the same C&C domain and the only difference was the URL path (*f1610/f1611*).

6.2. Week 43, 21-27 of October 2019

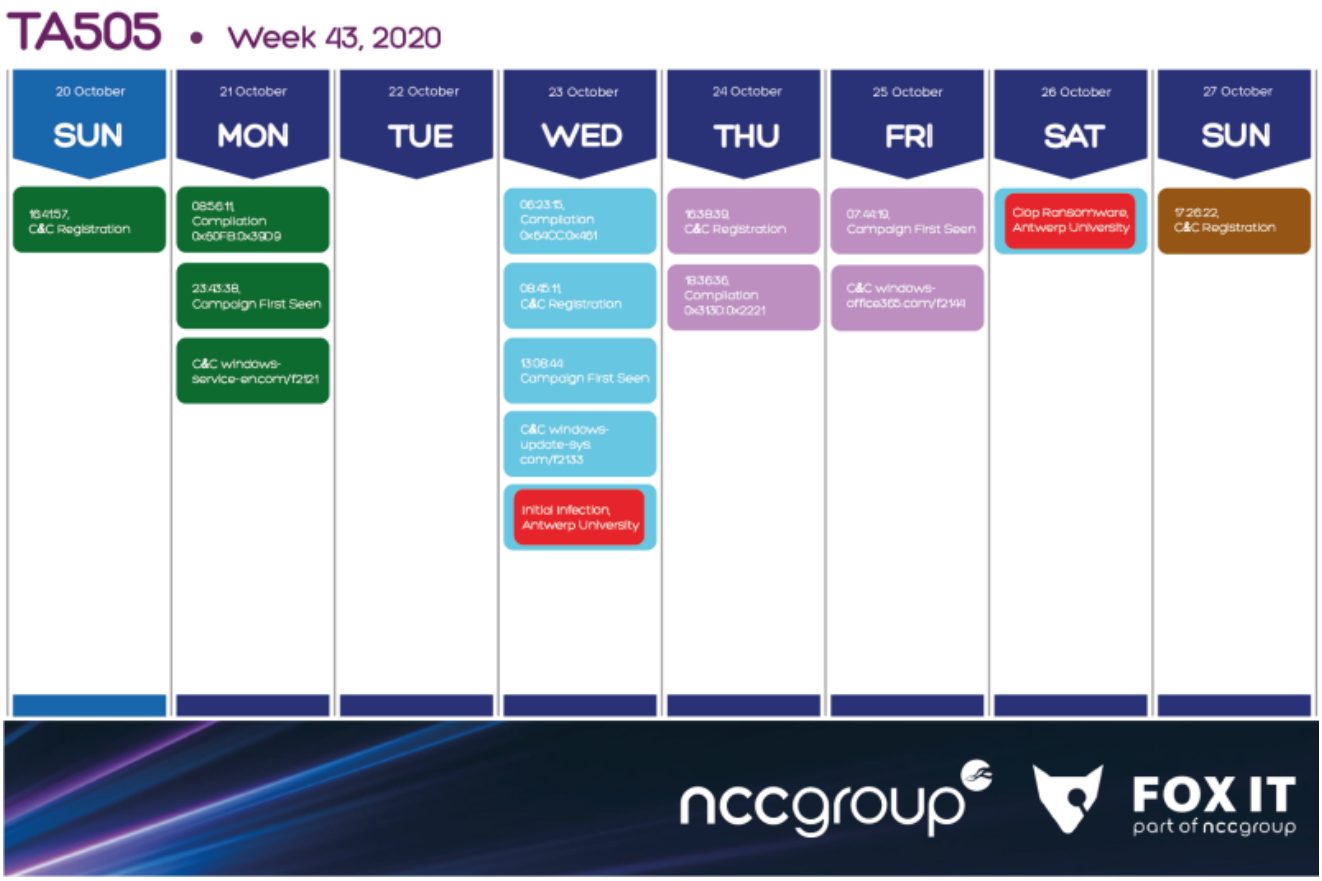


Figure 14. TA505 Weekly Schedule, week 43 2019

Throughout week 43, the group performed three campaigns. First campaign was released on Monday and was partially prepared on Sunday.

As for Wednesday, the group prepared and released a campaign on the same day, which resulted on the initial infection of Antwerp University. For the next three to four days, the group managed to get administrator access, and released Clop ransomware on Saturday of the same week.

6.3. Week 51, 16-22 of December 2019

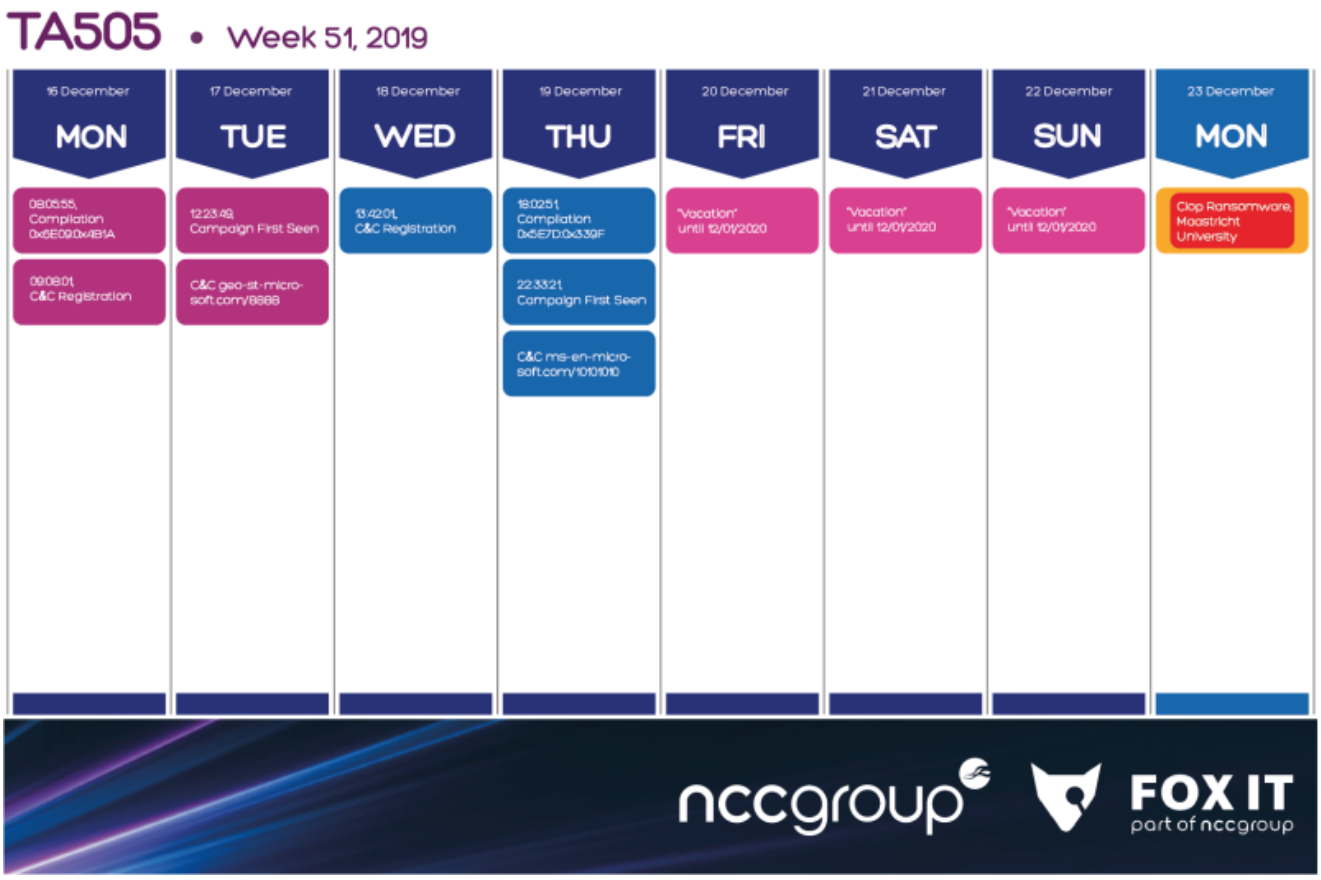


Figure 15. TA505 Weekly Schedule, week 51 2019

Week 51 was the last week before their ~20 days “vacation” period where Fox-IT didn’t observe any new campaigns. Last campaign of this week was observed on Thursday.

During those days of “vacations”, the group was mainly off, although they were spotted activating Clop ransomware at Maastricht University and encrypting their network after more than two months since the initial access (week 42).

6.4. Week 2, 6-12 of January 2020

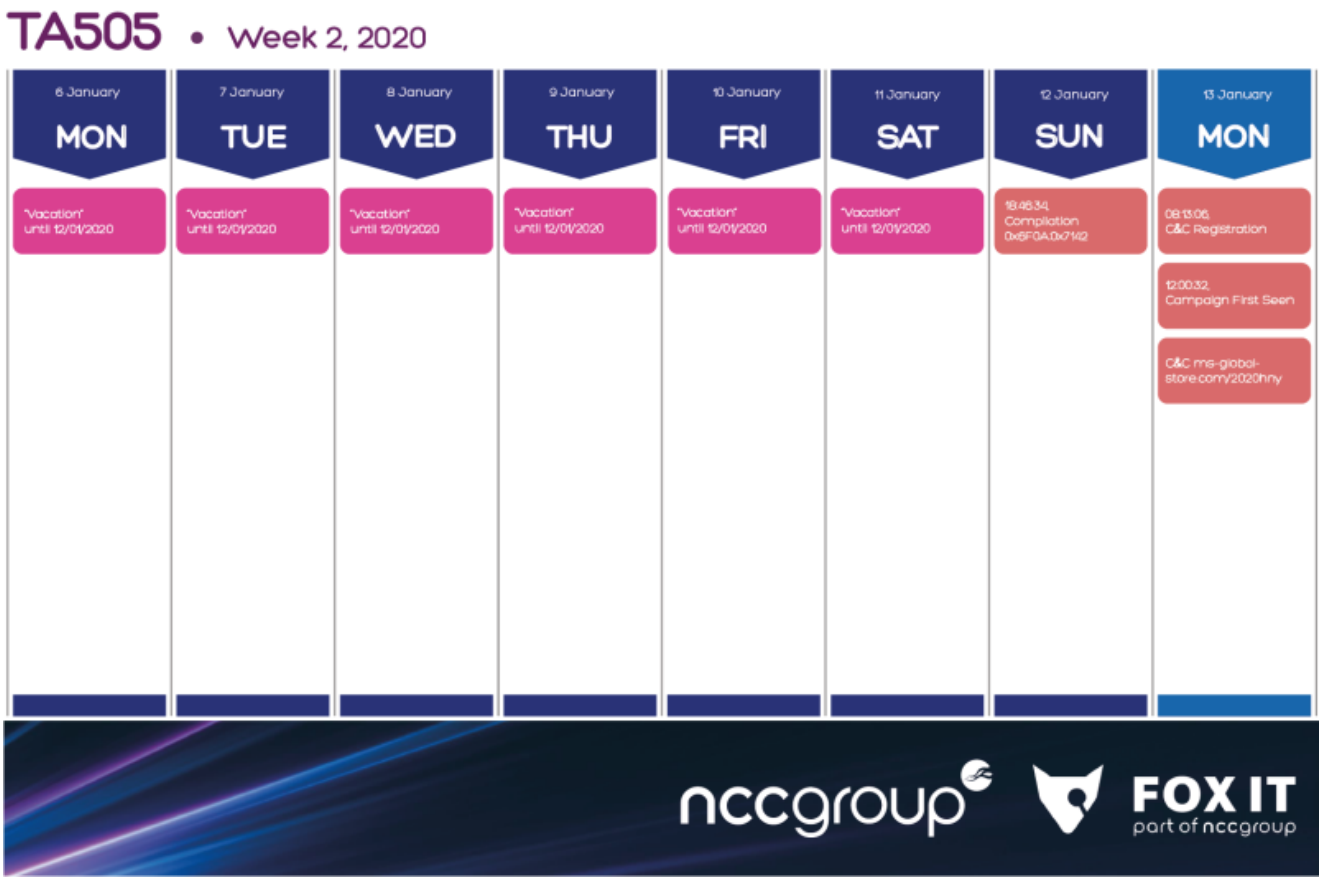


Figure 16. TA505 Weekly Schedule, week 2 2020

While on week 2 the group didn't release any campaigns, they were observed preparing the first campaign since their "vacations" on late Sunday, to be later released on Monday of the 3rd week.

7. Conclusion

The extreme *Dransom times* demonstrate a highly sophisticated and capable threat actor, able to stay under the radar for long periods of time, as well as quickly achieving administrator access when possible. Their working schedule manifests a well-organized and well-structured group with high motivation, working in a criminal enterprise full days starting early and finishing late at night when needed. The hourly timing information does suggest that the actors are in Eastern Europe and mostly working along a fairly set schedule, with a reasonable possibility that the group resides in Ukraine as the only majority Russian speaking country observing daylight savings time. Since their MO switched after the introduction of Clop ransomware in early 2019, TA505 has been an important threat to all kind of organizations in various sectors across the world.