Eager Beaver: A Short Overview of the Restless Threat Actor TA505

telekom.com/en/blog/group/article/eager-beaver-a-short-overview-of-the-restless-threat-actor-ta505-609546

TA505 is a very active – almost tireless - threat actor that prepares one campaign after another from Monday to Friday. They target organizations across industries / government in many countries around the world including Canada, Germany, South Korea, the UK, and the USA. A severe threat to a great number of organizations: on one side, they conduct Big Game Hunting operations, that is encrypting large parts of a corporate network to extort high ransom payouts. On the other side, they likely work on initial access development and hand over network access to associated threat actors.

Restless? TA505 prepares one campaign after another from Monday to Friday.

In my previous blog posts, I wrote about their tools and about their recent activity phase that started in June 2020. In this blog post, I will summarize what I know about TA505 as of September 2020, leaving the past aside. I will answer questions that we are frequently asked by customers and by the cyber security community in general. Finally, I will give recommendations to proactively fight them and share two generic ways to detect TA505 intrusions in your network.

Our Incident Response Service at Deutsche Telekom Security GmbH can quickly investigate and remediate ongoing TA505 intrusions. Please contact security-info@t-systems.com for more information.

What is TA505?

TA505 is a very active threat actor whose history reaches back at least until 2014. It is believed that this threat actor resides in Eastern Europe (likely Russian-speaking country). It is natural that the objectives of threat actors change over time. In this blog post, I will give an overview of its recent history starting in late Summer 2019, leaving the past aside.

TA505's activity pattern follows a classic workweek from Monday until Friday. Like a clockwork, they prepare one daily campaign after another, hardly leaving one or two day gaps. They are one of the busiest but also loudest – due to their high spam volume - cybercrime gangs as of 2020. They primarily target enterprises across all industries. But there are also reported cases of victims in Government agencies.

As of September 2020, I believe they primary engage in two different activities. First, TA505 likely works on initial access development for other threat actors. The current consensus among analysts is that they gain access to corporate networks, conduct the initial reconnaissance of these networks, likely including a first estimation of the target value. Afterwards, they sell the access to these networks on the underground. Finally, they hand over the network access to a second threat actor, which continues to operate in these networks. Second, TA505 likely engages in Big Game Hunting operations: they exfiltrate corporate secrets, deploy the CL0P ransomware, demand ransom, and threaten to publish said corporate secrets, if the ransom is not paid. Even though it is likely that TA505 only works in access development, there are several indications that TA505 (or a subset of it) runs the CL0P ransomware operations, e.g. they share the same custom packer.

Why are they so dangerous?

TA505 seems to work on initial access development. They hand over the access to the networks that they compromise to further threat actors. Therefore, you never know who is really compromising a network. Little is publicly known about TA505's clients. We should keep in mind that many organizations are rather tight-lipped about intrusions and we must expect that there are more than the publicly documented threat actors that follow an initial TA505 intrusion.

Two intrusion sets have been repeatedly and publicly linked to TA505 over the last months. First, the threat actor operating the CL0P ransomware. This threat actor engages in Big Game Hunting operations. On the one side, they encrypt large parts of a corporate network in order to extort ransom. On the other side, they exfiltrate corporate secrets. Subsequently, they threaten victims to publish these secrets to their leak portal, which they run on the darknet.

CL0P^-LEAKS website announcing the publication of files and customer data of several victims.

Second, another threat actor that is said to cooperate with TA505 is Lazarus / APT38. This nation-state backed threat actor conducts espionage as well as bank robbing.

While I tend to believe that CL0P is run by TA505 or a subgroup of it, there are opposing voices suggesting the CL0P gang is just another customer of them. As of September 2020, there are further hypotheses of possible clients like Silence that are still to be corroborated.

Furthermore, TA505 is dangerous because their spamming volume is high. On heavy campaign days, one organization alone may receive up to several thousand spam mails. While I do not have any global numbers, informal exchanges with other analysts seem to confirm this. Given this sheer number of spam emails, it is likely that one employee downloads the malicious document and executes the macro. And this is all this threat actor needs: just one infection to get a foothold in an organization. Above all, this brings medium-sized enterprises into the focus that normally would not be in the focus of such targeted cybercrime: throw enough mud at the wall, some of it will stick.

How does TA505 operate?

TA505 runs campaigns on almost all weekdays. They move very fast and setup the campaign infrastructure just a couple of hours before the daily campaign starts. These campaigns may target one or several specific countries (e.g. German-speaking countries). In this case, they restrict access to their command and control servers by the geographical position of the infected client (geofencing). But sometimes they target a broader set of countries in one campaign. A campaign does normally not last longer than one afternoon. I get the feeling that the campaigns are timed to start after lunch time, when many employees tend to check their emails again. Furthermore, most campaign domains and artefacts like malware are created or generated just in time for one campaign. This all ensures a tactical advantage of this threat actor and it is a reason why, for instance, commercial feeds may lag behind.

TA505 utilizes spam as initial attack vector. Targets receive an email with subjects that are money-themed (e.g. “billing”, “payroll”, “sales forecast”) or human-resources-related (e.g. “sick note”). The emails often carry a link that redirects via a compromised blog website to a sharehoster-themed domain (e.g. onedrives-live[.]com). Sometimes they attach an HTML file to the email instead of the redirection link. The HTML files mimic known services (e.g. Cloudflare, Mozilla, …) and also redirect via a compromised blog website to a sharehoster-themed domain.

Example HTML file mimicking a known service to distribute malicious documents.

At this sharehoster-themed domain, TA505 serves the target a Microsoft Office Excel Worksheet that contains a macro. Since TA505 does not utilize any zero day attacks, they rely on the user to enable the macro in order to continue the infection process. They lure the

user into enabling the macro by telling them, for instance, that the document is protected and requires macro execution in order to be fully rendered.

If the user enables macro execution then the macro drops and executes TA505's downloader Get2. This simple downloader exfiltrates information about the local machine to its command and control server such as computer name, user name, and the list of running processes. Based on this information as well as its geographic location, the command and control server decides whether or not the third stage payload should be served to the target.

The Get2 command and control server distributes the third stage of the attack: TA505's RAT (Remote Administration Tool) SDBBot. They use this RAT to conduct an initial reconnaissance of the target system. First, SDBBot automatically sends information to its command and control server including the computer name, Windows domain name, the Windows version, and whether the target system utilizes a proxy to connect to the Internet. Promising targets are then checked by manual operators, likely for a first estimation of the target value. SDBBot offers many commands to manipulate the file system, download and execute payloads, enabling of RDP, and so on.

In addition to their RAT SDBBot, Get2 frequently downloads PuTTY SFTP client. Since months I observe the same and by now outdated version 0.73, which is vulnerable to a man-in-the-middle-attack (CVE-2020-14002). It is likely that TA505 operators exfiltrate documents from the target system with the help of PuTTY SFTP client and not SDBBot. One reason could be that this exfiltration process is more comfortable with PuTTY SFTP client than with SDBBot.

The current understanding of TA505 is that they also work on initial access development. Hence, after the initial reconnaissance, they hand over the network access to another threat actor. Therefore, the modus operandi from this point in time may differ from intrusion to intrusion.

It is important to understand what is static and what is dynamic during a campaign. Note that a campaign lasts just one day. There are typically four important domains during each campaign. First, a sharehoster-themed domain that they utilize to serve malicious documents. Second, a domain for the Get2 command and control server. Third, two domains for the SDBBot command and control server. The first two domains change between each (daily) campaign. The latter two SDBBot domains typically change every seven to ten days. Furthermore, there are dozens of domains of compromised Wordpress websites that they utilize for traffic redirection.

Most other artefacts change from campaign to campaign. Some may even change during one campaign. The theme of the spam mail and its subject line may change a couple of times during one campaign. The malicious documents that the sharehoster-themed server serves change their hash value as well as their file name periodically. I observed changes every couple of seconds. Even though the maldocs and the spam mails may change during

one day, they still follow a certain pattern. For instance, the file name of the maldocs is just incremented during a campaign: Angebot_09082020_XXX.xls, where XXX stands for a three-digit integer that is incremented continuously. The payloads Get2 and SDBBot are repacked for each campaign. However, TA505 tends to serve the same PuTTY SFTP client since months.

Is there innovation?

While the TTPs of their current intrusion set are stable since late Summer 2019, they experiment with new techniques every now and then. They rely mostly on the same modus operandi but they adapt slowly and steadily. Their experimentation likely shows them the way to go.

For instance, at the beginning of September 2020, TA505 modified their malicious documents in order to evade detection. Their documents still rely on human interaction; the user must enable macros. But these documents used to have two PE files embedded (Get2 x86 and x64 version), which should ring a bell in many heuristics. Then, at the beginning of September 2020, they embedded these two files as two separate ZIP archives with obvious filenames like str_join1.dll that the aforementioned macro unpacks and executes. Since mid-September there are no obvious signs of PE files or zipped PE files in the malicious documents.

Furthermore, TA505 continues to update their tools on which they rely for more than a year by now. While SDBBot's version was 2.0 in September 2019, it is version 3.11b as of September 2020. For instance, they continue to add new features like certificate pinning. This feature was added in version 3.9 in June 2020.

At this point in time, the (public) analysis and detection of their tools as well as infrastructure continues. I expect TA505 to continue their experiments and to consequently innovate while maintaining the high velocity of their campaigns, which is the key to their success. I would say that we are not yet ready to see a complete retooling within the next couple of months.

What can your organization do about them?

There are several proactive and reactive steps that you can take to prevent significant damage to your organization.

First, you have to keep the gateway closed and your best defense here are security-aware employees. Explain the typical attack chains via email that other threat actors like the Emotet gang also follow. Especially, explain the problem with macros in documents coming from an external source. If possible then disable macros globally in your organization. Unfortunately, there are groups of employees that have to deal with many documents from external sources every day.

Second, block SDBBot domains at your perimeter network. As simple as it sounds, this ensures that there will not be any manual reconnaissance and further downloads of payloads (e.g. CobaltStrike). This should prevent a full compromise of your network, though you will have infected machines that require a cleanup.

Third, act quickly on detected TA505 intrusions since it may be a matter of hours or days until a full compromise of your infrastructure. Keep in mind that TA505 likely acts as a door opener and that you may have further threat actors in your network. Each of them may have further backdoors installed (e.g. CobaltStrike, TinyMet, etc.) that require a special treatment.

How can you detect an TA505 intrusion in your organization?

There are two ways to generically detect a possible TA505 intrusion. Generic detection means that it does not matter from which campaign the intrusion originated. The first way is host-based and you have to check it on your network clients. The second way is network-based and you can check it at your SIEM / in your proxy logs.

First, you can check the presence of PuTTY SFTP client in version 0.73. TA505 distributes this version in close to all daily campaigns. Get2 drops PuTTY SFTP client in the %APPDATA% directory. Hence, a recursive search on a supposedly infected network client for the MD5 hash bc59fa5dbb11f5d286fc41e8f25c6cc0 could reveal a possible TA505 intrusion. While this does not replace a full forensic investigation, it can help you to quickly narrow down on clients where a possible TA505 intrusion may have started, if you get a match.

Second, SDBBot conducts a check of its geographic position on each start. It utilizes a third-party service for it: IP Geolocation API. It sends a HTTP GET request to the URL http://ip-api.com/json using the hard-coded user agent “Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36”. If you detect such requests by a local network client, for instance, at your proxy, then this might be a good sign of a live SDBBot infection. Consequently, you should start a forensic investigation on this client.

Hard-coded user agent string that SDBBot utilizes when contacting IP Geolocation API.

Appendix: IoCs

Ioc	Description
98d01979e1020baa9a8e6af2c14da0da	maldoc (embedded PE files, visible)

077f697d9c6eb89baf98ecdd479e9c02	maldoc (embedded PE files in ZIP archives, visible)
bb0ae6a1edcdfe74efe5bf275deaf943	maldoc (invisible PE files)
2a343a9c588ab2478d64457873b12d54	test maldoc (without macro)
ac43b411b9bd455a8cde89face9ea9b9	Get2 x86
9cab3a1e56303949b7b54897d84c77fe	Get2 x64
b27b040dec41bb9cb1df456a7949ee5b	SDBBot x86 installer (version 3.11b)
7732577a4db34389a7cc93b08bdba714	SDBBot x86 installer (version 3.11b)
bc59fa5dbb11f5d286fc41e8f25c6cc0	PuTTY SFTP client (version 0.73)
news-37876-mshome[.]com	SDBBot domain (since 2020-09-11)
news-389767-mshome[.]com	SDBBot domain (since 2020-09-11)