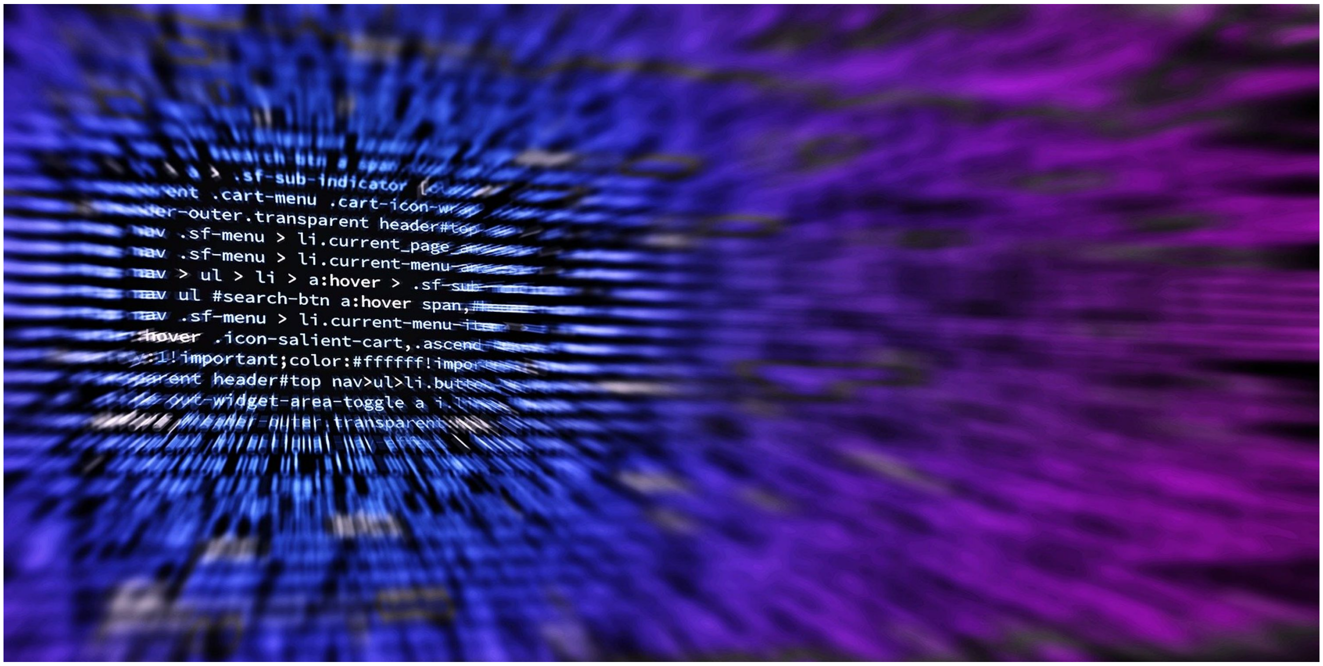
TA505 returns with a new bag of tricks

telekom.com/en/blog/group/article/cybersecurity-ta505-returns-with-a-new-bag-of-tricks-602104



Blog.Telekom

06-16-2020
Thomas Barabosch

7 Comments

- Share Share
  Two clicks for more data privacy: click here to activate the button and send your recommendation. Data will be transfered as soon as the activation occurs.

- Print
- Read out

In one of my last blog posts I already introduced TA505, an advanced threat actor, and their recent tool set to you. In this blog post I'll show you somenew techniques that they've recently adopted to increase their financial gain and to improve their operational security.

Cybersecurity: This TA505 threat acteur is active at least since 2014.Thomas Barabosch gives an overview of the hacking tools that TA505 currently uses.

TA505 is a cybercrime threat actor that conducts Big Game Hunting operations. In short, Big Game Hunting means selectively targeting organizations with ransomware in order to achieve huge ransom payouts. Today, organizations should treat ransomware events also as data breaches since ransomware actors steal data before encrypting it and leverage this data during the negotiation phase. If the victim organization does not pay the ransom, ransomware gangs publish the stolen data on their data leak websites. TA505 runs their own data leak website “CL0P^-LEAKS”. In addition to these Big Game Hunting operations, there is also a possible connection to another, more targeted activity cluster, which is closely related to TA505. Want to dive deeper here?

Since the beginning of June 2020, TA505 continues their operation with massive spam campaigns. Within a couple of days, they have run several campaigns: on 2020-06-02 and 2020-06-03, they started by targeting Germany, on 2020-06-04 and 2020-06-05, I observed them targeting Canada, and on 2020-06-08 as well as 2020-06-12, they ran a rather broad campaigns targeting many countries worldwide including Europe (Germany, Slovakia, UK) and America (USA). In this blog post, I review the recently observed activities and point out some interesting changes.

Same TTPs with some interesting changes

The TTPs that I have observed since the return of TA505 align mostly with the TTPs from earlier this year. To sum up, the initial attack vector is still spam. This spam carries a HTML file that redirects the victim via compromised websites to a XLS maldoc. The maldoc comprises macros and asks the victim to enable them. Once enabled, the XLS maldoc drops their downloader called Get2, which in turn downloads their Remote Administration Tool (RAT) SDBBot. From this point on, we must assume that a human operator explores the local network and as an ultimate goal may deploy the ransomware Clop. This is common in today’s human-operated ransomware attacks.

So far, so good. But there are some notable changes that I observed within the last months. Since the beginning of this year, their HTML redirectors that they attach to their spam mails mimic the DDoS protection service of Cloudflare in order to make the victim believe that they are redirected by a legitimate service.

DDoS protection service of Cloudflare.

Since this month, they added the Google service “reCAPTCHA” to these HTML redirectors. On one side, this increases credibility from the victim’s point of view. On the other side, this hinders automatic analysis of their infrastructure by sandbox systems and individual researchers.

Google service “reCAPTCHA”.

Another interesting change is that TA505 jumped on the data leak bandwagon. Today, ransomware actors steal data from victim networks before they actually conduct the ransomware attack. During the negotiation phase of the ransom, these actors utilize this stolen data in order to increase the pressure on the victim and threaten to publish the data if the victim does not pay. TA505 created their data leak website “CL0P^-LEAKS” for exactly this purpose. As a consequence, victims of these recent TA505 campaigns should not only treat this as a ransomware event but they should also prepare for a possible data breach.

Data leak website “CL0P^-LEAKS”.

SDBBot beefs up with Certificate Pinning

SDBBot is TA505’s currently preferred RAT, which they use during the human-operated phase of their ransomware attacks. During the spam campaigns that I observed in June 2020, they continued to distribute SDBBot to their victims.

SDBBot went through a number of iterations when looking at its version numbers. For instance, samples that TA505 distributed in November 2019 were tagged with version number 2.3. The samples that they distributed in June 2020 are tagged with version number 3.9.

One addition that stroke my eye was the addition of Transport Layer Security (TLS) to ensure communication security. TLS is definitely on the rise in malware. It is estimated that almost one quarter of malware utilizes TLS for its communication. SDBBot’s actual implementation is based on the open source TLS library “Mbed TLS”. While using TLS is not out of the ordinary for malware in 2020, SDBBot comes with certificate pinning, which is not very common for Windows-based cybercrime malware. In a nutshell, the malware comes with an embedded X509 certificate that is associated with its command and control (CC) server. When the malware connects to its CC server, it checks if the server’s X509 certificate matches its embedded certificate. If it does not match, then the malware refuses to talk to the CC server. The following screenshot shows the embedded X509 certificate observed in a SDBBot samples from 2020-06-08.

Embedded X509 certificate observed in a SDBBot samples from 2020-06-08.

The use of TLS and certificate pinning has three consequences. First, the communication between bot and CC server is cryptographically protected and eavesdropping is not possible without intrusive measures. Second, the certificate pinning ensures that bots cannot be taken over by claiming the CC server’s domain. Third, the reverse engineering of the malware’s communication protocol is more difficult since analysts have to patch the embedded certificate in order to make the malware talk to them.

Conclusion

TA505 is back and they probably will not go away soon. They continue with mostly the same TTPs that they utilized since at least Summer 2019. However, they naturally evolve and adjust their tactics to ensure constant success of their operations. On the one hand, they jumped on the data leak bandwagon with their website “CL0P^-LEAKS”. On the other hand, they continue to improve their tools like SDBBot, which gained new features like certificate pinning.

Appendix: List of IoCs

IoC	Description
e3f57d7d933d19d190ff27ec455875ac	SDBBot installer x86, version 3.9
a66e9afbba9b0f014d0774070b59c79e	SDBBot installer x64, version 3.9
s77657453-onedrive[.]com	SDBBot domain (2020-06-12)
s89065339-onedrive[.]com	SDBBot domain (2020-06-12)
s3-ap-southeast-1-amazonaws[.]com	SDBBot domain (2020-06-02)
s3-ap-southeast-2-amazonaws[.]com	SDBBot domain (2020-06-02)

On topicCybersecurity: TA505’s Box of Chocolate
Cybersecurity: Dissecting Emotet - part one
Cybersecurity: Dissecting Emotet - part two
Media information: Telekom presents current figures on cyber security
Media information: The Global Guardian never sleeps