TA505's Box of Chocolate - On Hidden Gems packed with the TA505 Packer

By Deutsche Telekom AG

Published: 2020-03-26 · Archived: 2026-04-02 12:42:19 UTC

In my very first two blogs I gave you an overview of Emotet - probably the biggest threat actor for now when talking about malware. I explained details of its modular structure and which tricks Emotet uses to stay undetected. And of course, I talked about the consequences for defenders. Want more?

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

This time I would like to introduce another big threat actor to you: TA505. This is a globally spread malware, which acts mainly out of financial motivation. TA505 has been active since 2014, but we at Telekom Security have seen increased activity of this group, especially since the second half of 2019. I would like to show you which tools TA505 uses in contrast to Emotet to sneak into companies and organizations. So, here we go.

As of February 2020, they are mostly known for Big Game Hunting operations, in which they target large organizations with their ransomware attacks. This in turn ensures very high ransom payouts, easily in the range of six figure Euro amounts. For instance, TA505 targeted the University of Maastricht in December 2019 and demanded 30 bitcoins (BTC), roughly €220,000 at time of valuation, as ransom. Subsequently, the University of Maastricht took the decision to acquire a decryptor to get back their data.

Big Game Hunting operations can take from a couple of days up to one year. This includes the initial compromise of one or more endpoints in a network, the subsequent network exploration and lateral movement, the takeover of strategic points like domain controllers, and the final deployment of the ransomware to as many endpoints on the local network as possible.

As these operations comprise different stages, TA505 utilizes a wide range of hacking tools to accomplish their missions. Furthermore, they continuously change and update their toolset. For instance, they added the downloader Get2 and the Remote Access Trojan (RAT) SDBBot to their repertoire of malware in mid-2019. These frequent changes and updates are a major difference to the group behind Emotet (TA542 / MUMMY SPIDER), whose tools remain unchanged for long periods of time. I blogged on this group a couple of weeks ago. In this blog article, I will review hacking tools that TA505 is currently using.

TA505 Packer

Before we dive into TA505 current tool set, let us first have a look at how these tools are packed. As of time of writing, and at least since the second half of 2019, TA505 utilizes a custom packer to obfuscate its tools. While custom packers always mean more work, since they may require manual unpacking of the payload, they are a perfect way to track threat actors.

In addition to this custom packer, TA505 may pack their tools a second or even a third time with UPX. I observed that TA505 packed their Get2 downloader with one layer of UPX, a second layer of the TA505 packer, and a final third layer of UPX again (see Hashes in Appendix).

In a nutshell, the TA505 packer decrypts its payload using simple xor and rol/ror operations and its technical details are well covered by this blog article. There is no need to manually unpack TA505 binaries, since Tera0017 published a static unpacker. This unpacker is called TAFOF-Unpacker and it is available on github. As of time of writing, it works with the latest TA505 x86 binaries. Unfortunately, TAFOF-Unpacker does not work for x64 binaries yet. Thorsten Jenke and Daniel Plohmann provided the generic unpacker RoAMer, which is capable of unpacking the latest TA505 x64 binaries.

Let's look behind the packer

Now that we know how TA505 currently packs its tools and how to unpack them, let us have a look behind the curtains and see which tools TA505 is currently using. Throughout the last months, I obtained 121 samples that were packed by the TA505 packer. 46 samples are x86 binaries and 75 samples are x64 binaries. TAFOF-Unpacker unpacked all x86 binaries and RoAMer unpacked roughly 80% of all x64 binaries. In the following, I will review the tools that I found in the order of when they are typically utilized in a Big Game Hunting operation: from the initial malicious document to the final ransomware. Note that there are some outliers that I will address in this section as well as at the end of this article. A full listing of all samples and their classification can be found in the Appendix.

The Spam and The Maldocs

TA505 carries out high-volume spam campaigns to gain its initial foothold in an organization. As of February 2020, the spam emails come with an HTML redirector attachment, which points to a server with an office / a share-hoster themed domain name.

Figure 1TA505 HTML redirector faking Cloudflare DDoS protection.

This server typically serves Microsoft Excel documents. These documents include a malicious VBA Macro and try to lure the victim to activate Macros.

Figure 2Recent TA505 Excel document convincing the victim to activate Macros.

If the targeted user enables Macros then the embedded VBA Macro loads either a x86 or x64 embedded payload. As of February 2020, this is typically the Get2 downloader.

The Downloader: Get2

Get2 is a very simple downloader. It has only two objectives. First, it calls home to its Command and Control (C2) server and exfiltrates information regarding the victim’s system. This information includes the username, the device name, the Windows version, and the list of running processes. Based on this information, the C2 server decided to serve another payload to Get2. Second, Get2 executes the payload provided by its C2 server. As of February 2020, this is typically the RAT SDBBot.

Another Downloader: Amadey

Even though Get2 seems to be current downloader, I found one Amadey dropper sample packed with the TA505 packer. Amadey is a very simplistic downloader that is sold for $600 in the Russian cybercrime underground. There is only one Amadey sample in the corpus that I analyzed. There could be many possible reason for this, which I will address at the end of this article.

The RAT: SDBBot

Since September 2019, I have observed SDBBot to be a consistent third stage payload, which Get2 downloads. SDBBot is a Remote Administration Tool (RAT) that a human operator utilizes to prepare lateral movement.

Its capabilities include, amongst other, execution of further payloads, video recording, enabling of RDP, as well as listing, writing, and deleting of files / directories. A good write-up about SDBBot's capabilities can be found here. SDBBot is very prevalent in my data set. A huge share of the x64 samples was SDBBot, however, there were no x86 samples of SDBBot. This is in line with the market share of 64 bit Windows. Another explication could be that x86 SDBBots are packed differently and therefore the data set does not comprise any of them.

Another RAT: FlawedGrace

FlawedGrace is another RAT that was first observed in 2017. It seems to be exclusively utilized by TA505 at this point in time. In my data set there were only two FlawedGrace samples and dozens of SDBBot samples, which may indicate that FlawedGrace was mostly replaced by SDBBot.

Yet Another RAT: Silence

Silence is a RAT that is (exclusively) developed and operated by the Silence Group, a presumably Russian cybercrime gang. They carry out attacks against financial organizations. Group-IB pointed out a connection to TA505, stating that the downloader of TA505's RAT FlawedAmmyy and the downloader of Silence are similar. Finding Silence packed with the TA505 packer suggests a possible on-going collaboration of these two gangs, although possibly a minor one due to the low sample count of two.

The Information Stealer: Azorult

Azorult is a classic information stealer that steals saved passwords, credit card information, and cookies from browsers, as well as credentials from a wide range of software such as Filezilla, Microsoft Outlook, and Thunderbird. Potential use cases of TA505 could be utilizing stolen credentials for lateral movement, feeding stolen mail account credentials back to the spamming stage, or selling them to the highest bidder. Researchers at Blueliv also observed other information stealer like Predator The Thief in the context of TA505.

The Post-Exploitation Tool: TinyMet

TinyMet is a very small (around 4KB) stager for Metasploit's Meterpreter. Its main objective is to establish a communication channel between the attacker and victim and to execute a file-less payload on the victim's machine.TA505 utilizes TinyMet during the post-exploitation phase in order to deploy their ransomware Clop.

The utilization of public Offensive Security Tools (OSTs) by threat actors involved in Big Game Hunting operations is a common trend. It is logical since these OSTs provide capabilities that threat actors do not have to build on their own. In addition, many of them are freely available, either as open source software or as cracked versions (e.g. Cobalt Strike).

The Preparation Tool: DeactivateDefender

TA505 proceeds the last stage of rolling out their ransomware by deactivating security tools. The objective is preventing any behavioral analysis from stopping their ransomware and the ongoing encryption process. The tool DeactivateDefender achieves this by changing Windows Defender related registry keys. In my sample set, I only found several samples that deactivate Windows Defender, though there seem to be variants, which target other security tools like Malwarebytes.

The Ransomware: Clop

TA505 finishes its Big Game Hunting operations with their ransomware Clop. At this stage the threat actor must be pretty confident that their operation will succeed: strategic points of the target network have been taken over and antivirus software has been disabled. As a consequence, Clop encrypts many, if not all, endpoints of the target network within minutes. From a technical point of view, Clop emerged as a variant of another ransomware called CryptoMix but by now it seems to be developed separately.

Conclusion

In this blog article, I have had a look at a partial set of TA505 tools that are currently in use. Note that this is only a snapshot of their toolset. A couple of weeks ago, Blueliv mentioned additional tools like the RAT ServHelper and a modified TeamViewer client. In general, TA505 continuously replaces parts of their toolset. They have abandoned many tools and they certainly will abandon at some point the tools I observed. One of TA505 tactics seems to continuously change their tools to evade detection and to make tracking more difficult.

Having reviewed the tools that are behind the TA505 packer, there are many questions that one now could pose regarding TA505 and this packer: is TA505 one group or several groups? Or is it a group of subgroups that share one packer? Or do they share their packer with affiliated groups like Silence? Or is the TA505 packer not exclusive to TA505 and it just another packer sold in the cybercrime underground? I believe that this packer is exclusive to what is publicly tracked as TA505 since the majority of samples are in line with what is publicly tracked as TA505. Only few samples seem to be outliers. For instance, the Amadey downloader sample, which could have been an experiment or a service to a client / affiliated group. Otherwise I would have expected to see more samples of this early stage tool like in the case of the Get2 downloader. And in the case of the Silence RAT, there seems to be at least some form of cooperation between TA505 and Silence Group. Even though these outliers exist, the vast majority of samples falls into the Big Game Hunting category.

Another question regarding TA505 that may come to one’s mind is whether there is another branch of TA505 that carries out more targeted attacks (e.g. as reported by BlueLiv and by FireEye) or it is the same group that carries out these attacks. At least the ServHelper RAT that is mentioned in the BlueLiv report (see Appendix) seems not to

be packed with the TA505 packer, which is another modus operandi. In fact, FireEye started to track this subset of what is publicly tracked as TA505 as another group.

Appendix

Hashes of representative samples

d84bf8370e8f75de9cc8de410d4c4fd0256ab31542c63b797684e3eb8df185d0	Maldoc with UPX-packed Get2
017c8e29cda1b77fdaef28b22ab0200385ff1b7b452e6252131bae86c0ef0cf6	Get2
0617ddb1b7e7ab86159bc7be01c86c50a9d7a57db0914486c496e277c10b19ae	Amadey
e49953079c9f18adc26bfdd01d17add9b50f145936457ce01abc1489b143a25b	SDBBot
43723e8cea065bbbd4339ed83cb2edb4c1f4d686301a8a26d2c0d02672c07ed4	FlawedGrace
4b0eafcb1ec03ff3faccd2c0f465f5ac5824145d00e08035f57067a40cd179d2	Silence
e4eb1a831a8cc7402c8e0a898effd3fb966a9ee1a22bce9ddc3e44e574fe8c5e	Azorult
74c5ae5e64d0a850eb0ebe3cbca4c6b92918a8365f2f78306643be9cffc32def	TinyMet
6d13ddebdb7c57d61afecf6450b6d5667367d2ca8a263c6977af83eb143190d1	DeactivateDefender
6d8d5aac7ffda33caa1addcdc0d4e801de40cb437cf45cface5350710cde2a74	Clop
d83063586bbdd28a3936fc508e69c0d880673fb985429ede6d0369c91250cbc2	ServHelper RAT referenced by BlueLiv

Hashes (x86)

017c8e29cda1b77fdaef28b22ab0200385ff1b7b452e6252131bae86c0ef0cf6	Get2
04e97922edd766b69fecf42370b52f81fe9efd7927e16eb8374042f565430365	Clop
0617ddb1b7e7ab86159bc7be01c86c50a9d7a57db0914486c496e277c10b19ae	Amadey
0ba5294285461185a370af117d551080b678b399271143e9ede8a86aa74f4b9a	Get2
0bd7ec24742b5b87136e47396c0462865c92d29dc86e64468f4cefe7d6d7d863	TinyMet
13831c641d1c0df39505b45fb71edc6cfb7bd6990415cf69d675d14f75df0f93	Clop
155463dc90693d42ef1ab1910e4fdaad7216555bcaefaf60d1e6582468775dc3	DeactivateDefender
238d40bbc430c6098a8ad4682ac3722e36b1d2e91fc9030124e5152b6b186e94	TinyMet
25bfe1bd30bbe5100498ed74eb413168a3740cb03a6cca489a88324f20b71c0f	Get2
28534d617055925d0bd3f8fb6ec8f0f66731744cac5997ffa18ecd8e9986a2ff	TinyMet
318f86f9af6dca3431fb88d56171a637fbc49d87e222488692a19f59f5f56ae9	TinyMet
3b5f2d1f3e9400ce830945a6a2e3ca5dc6ce1263eaed79ca1a66f40eed676b96	Get2
41ed4f18b095f8a28dcb2f1a046fdd60de60321847eea7fa7b792b94017437a0	Get2
43061ac4c490c98f7b225c6143c048a7c4b0c9cb1607bf17ad3d7e5f867aae5b	Clop
43723e8cea065bbbd4339ed83cb2edb4c1f4d686301a8a26d2c0d02672c07ed4	FlawedGrace

46cab94e42a739b6ff68c310e17189ae685116b89b54c1893aa858e434e6996a	Get2
4b0eafcb1ec03ff3faccd2c0f465f5ac5824145d00e08035f57067a40cd179d2	Silence
4d8c313d585ab2912037d8e07ce4dfc1fe7870dba1a8d75964128ce4d5a3168d	Silence
5bf2ec8edf8e6c69a0f3b8cc84ce22b06c96d7cd9bd388ea3b7a99e990b253ce	FlawedGrace
6d115ae4c32d01a073185df95d3441d51065340ead1eada0efda6975214d1920	Clop
6d13ddebdb7c57d61afecf6450b6d5667367d2ca8a263c6977af83eb143190d1	DeactivateDefender
6d8d5aac7ffda33caa1addcdc0d4e801de40cb437cf45cface5350710cde2a74	Clop
74c5ae5e64d0a850eb0ebe3cbca4c6b92918a8365f2f78306643be9cffc32def	TinyMet
7e43a3a9b4ed3820c91d74c6b128c00d0f0ba267f97c101fdc89fc66816258f1	Get2
7f122f4c8dd6adbb8e71e65ac5ed99e981ead827186518be88ae6f6a569d554f	DeactivateDefender
850adf1b855e043ec92b271d921502994bf8f39da090748fcc5fd40749ed0d0c	Clop
861284acf359d91bdcc68ea791bd807a569b4c289450b1eaf8fcbc7ca43be7ff	Get2
8a14d70433b5ec004e5295e1e8aef3ad406b80fa22eeeb8283edac706f1724d1	Get2
9065b394d99a5812a3d56b51992f9d4592c9c8d1cc96ee565299e0f6f5400329	Clop
93d60464aa6f4c46cfe71763e6b591d0444121d7e38e11b5122471715ff7b436	TinyMet

967a66466eec2345aabd6999507340ce9bc94b1f0ce8a99cb279620379ab59a6	Clop
9bcdf30646e15a28d3d4f00e5dc804bac1336a51a6f9f87098b8bf746bea0e96	Clop
9efaa4eaad1da49e4893f80295c473faefadd00370e13fa07e83aade88b5f390	Get2
a407101bb3f2cf7f34ee5b0025fa80d7c488dd7aa789522333461fa5d73b69e7	Get2
ae22f4d687957c368b55c3ee5c493c7e72f63dc6c8530f2c2caf1b29fd280349	Clop
bd5c800fa6b0f67cd7343158efca2ff95735cb7a82c62e0ce84442344e0b2f55	Get2
bd9c2c9a08d890c36ff8d83f2fe8adfa965faaeded961406722a87e53852c95e	Get2
c33899af88bd583bcf779d4516bd554c0b0bfb7277dab87a124852c81360c795	DeactivateDefender
c5aef005b14b035bc74142fea8de5ee40f9ea5644ad0fe0a71bd59167d14e1fa	Get2
c942c117e04a6173f1ee6da437a4e42544a92e4052fa72ea52dbc1e17ee138a7	DeactivateDefender
d2a09be9dfe59b5a24675a412117b3b0df23667fb8f7b2b6b06520519f0e15d1	DeactivateDefender
d3604c779b7decc195cee43251289568a957c0712c520868ddd0f3d0e0ca596f	TinyMet
d3b2385aee12637d932654552200dd63b5b34ab81b850f4f901a029f7e22d66e	Get2
e4eb1a831a8cc7402c8e0a898effd3fb966a9ee1a22bce9ddc3e44e574fe8c5e	Azorult
e8fa1317e21034a4279d49364182560783ff4ad903078c18edc6bd97d75d86e6	DeactivateDefender

ecc871318a482b1db40233db2ca9525c0131bd011db5de80191d9b5953b7976d	FlawedGrace
ef571b7ff5db8ea20ee42474c626cff52b83963fcd39bc5238cb84d070887882	Clop

Hashes (x64)

02e4e13a4471879c5b3943e1790af545099d8ac34a1e6bb50095dcb480f3376c	Get2
05eaf9287fbca272bdd08fd474983d898da496f48e023ca19ee26acab0102e72	SDBBot
078db073259af3d431e72d4f35befe3aef681fb140dd80d853ac5b29e064f596	Get2
07be5d876aa45fd4d6f68a7c3ffa9e0a67f4d3d5f557309e5621334ffea74b84	Get2
0dc28068279678cebc5a885cb56edab4fcf930d68a668f39a4e2de1e0d75a082	Get2
0e14d32b91cdd0e21c43c90924d93d5dd7f19596b2d771ae9ea4ab991c1d8a0a	Get2
0e2be7d0909f863d81986430084e4d64da6390c43c1846752c5dd8ac15e4aa99	SDBBot
0ec3608921fb357ad48365185edc71e8d40b2e8052ffcc48809e5a5a7f0cc1eb	Get2
121e581e1d1c553d3976a8b054fc42818025955093214a3233831db5a7905b08	Get2
141d71d86cd25b210b67fe8e49d2abf63324b7ce36736b95b51c9258c4b1ddbb	Get2
14341f74443e6d0dfde80fadb6dc48fa928e3ef31af2e05e357d5ed4d20f28d9	Get2
1597b0f644a89509472cae64a63c79aaf545c9712cde453849e79178a4be1519	Get2

1ac115a67bff6cd95a7150651807e8ffe5b67c3ada7897138ee2d01a4c7dd3b9	Get2
1d53b599a7059d476c1f4f7bd8b32979676f0d7c3953cac2cedf01ec25fb69cd	Get2
22aa6a954d6cc074e6ae159766c2e94d0b08b6cef6c635ea65c585bb4798b576	Get2
276ac3d7f9593b7f6bc1c282e27763581abf0571342ff446a9f81b9b58a41dcd	Get2
288756991e3cf5ee1296dd4b699b22140b8acc2d2460942e524175a9b0e30784	Get2
309c15c52e4d61e15901051428ea00e1b9c916ac6bc69449c03239e110864343	Get2
34b1f39453d2340cb78d2731ac4e5b85ec1dfa38fc60f49c40b66fcf8819e3d9	Get2
3b409268a8cfb58052e1e93ec38d94f260ea5bd64a1ebdcb7c69feba8fcc6995	Get2
4264e428e96376609462b8339b93c829b0b506784ab20c8561416aff2ca1f0c3	Get2
47fcafa29d3610f5ec276d7b6cdb3e4a7ae1f8a24762a56acc080be69a8667c1	Get2
4a3faf2bccb773086fb34e7c486ada09f0d2ec47e5a06c684130c153d4392ddd	Get2
4bda777159fcaf021cb5ac98dc6f427fc0dc4725abb6a3d6521d7a0f89897063	Get2
4c6a15b0efb1b3ac86869b7771cf57b75d4f6f6150c9e47655bcdf8ef387d18f	Get2
4e3afee4db687d1609541302b5b80d9c01cdc2b30f4f8d6481243b2b7217b97d	Get2
4fafcbd5009694e420fe85fa39c6c3f85fbb6c3ef871f6e9e1a232453742e475	Get2

511ecf63f0bce7287c1ed6c931a94761b9425f3def1aea3398cb1765cd472166	Get2
51730c6f705071b2ca031e2cd65a365dddcb07728f3e2c94715e8160ad37ab68	Get2
53a290caf81d44d56f57e7a9c7fefadca0a18fac73fdeba97c7dcf5989150702	Get2
5438272df636e70bf68dbaabc55a4f60452a0eb56c5e17e426c74ce179908211	Get2
5b07369ada0a27d3259fd9523752b0a64fd4ebf21453ed7a2c442e57e5806445	Get2
5ccfede2af0fd43d36d2d8f48787dc93d80dfb6e9655af367d406dc01994442e	Get2
5eeabd672965a671d7e75b40415a9c3502ba1987627122fdfe9f5064fc180ca6	Get2
5ff0b9b14305683b9d7a14e71390ce5c7a7b29a5da4410d3df3b35268e09d9be	Get2
64f9c5dfda76fa986efcc6bcc22d5d052a9ca06e165f7bcf5fac8dcc10339f49	Get2
66b35a54537946e23f17ef11ec217c88952f56849eb0ff535b324cd48ff109b5	Get2
679bdcf3c369a90e82cfa5f5467e42c5c288bcc5264a4400d455e4568bf1d525	Get2
6d5c207c998990f1e7c527971dfe0eb6d2b21fca136d616e6e211019d1c77698	Get2
7327b04cf529f21f8d12f353ca5135e5a81f862d6ab8056dfbcedfcf8caa3666	Get2
77329d82a96dfd81ec55c3e2ad8c4cef210d6d3dcdd7518f54aebe7f5606a6cd	Get2
7f4f69a2133ed3882bac7675c9aba77296bdeb3b4d624ca281de5032500b4f7f	SDBBot

80d72b63347f9fa70ac03fafcc46247b400ef2cbbb258f1bb55aa4981faf03fd	Get2
80e806c1c9a5a96ae46ca01c9a5748ceb89bd9e51405e88c0d90e6bfad713440	Get2
81b6fe266fba724d6e37b751424d98111669971d8e8393bd5363c8b95d130dc6	Get2
89257472a6a65659a98245ea9ddbf01081a2e0ebc51d9c946d4c3d64d240f99c	Get2
8978e1825ddd5a175c27ea8e75f878dd68aa59c64fb393cce5bfd2692c3161ea	Get2
8e8a8d06f72f2a5ed79e478e644dea55062fc2b79535655089fd22c551922bb9	Get2
8f36df0c4f23d758cfa72aa706d28b7ce15513ba2c3354d7df0ee5335a5079c4	Get2
97528075acc198ebeecb18a66de53206808b5a9d791463af36b9b1c7a402bcb7	Get2
99eeb9b8ee908f6faf66982a5cef0098e261fcafdb558b56f6659f92510d4b4b	Get2
a04d0cb7362e3650239230b40fac1d2d42357cec1ded2e78456e49dd6713b470	Get2
a0c4d66ccb7d0a5aaa52a9d06f797bbb9be127d22f705a5c0472cac52f0f0ddd	Get2
a0e349afc168d890831e1353ce44abdd069b79d13f4170676ac2ffea3761bf01	Get2
a94a316ed134c43010709454d54f13327123f57a133d02351d2e19cf167b1e75	Get2
ac25d77a2091a5665d37b0a91be9b154ff61c16b35b5575c907ef4e6d8bbcc23	Get2
afd1c04e11ebfc8d3eed2e011c26be25d133c30de9bd80eaa2605573a0d49db3	Get2

b5c4b39ebf181b7bcb52176934fc46c608d0d4d1881d2fbe909d9d3889155930	Get2
b8b6a4ebe98146616012ffecee9651c51be7ce9fca10cda4b6bf17d66d71594d	Get2
bc62e6e52027724be2e3e78ab25c11dbcdd258f394014b6b1d637da6eee60217	SDBBot
bccf6ecd6987bac361df1eb0fb2e9324dcf41ed30a3b5c6a8ee075794a6a0713	Get2
c2a60385f73dcf2941ffd9fab11872f760cee6ef83b678696b16a179c079a870	Get2
c2f99a2bba225fe3ab49cb952e418b2ab29ba7f2e34db6cf9bc51b0349d0acd8	Get2
c530b2c85ba3b58e7174e754c73369a39e1e568f40d5cf777ea6f0f162bbe09a	Get2
cb855b21356e6562e5657bcf08a400b7eef69154f80e63616b1693a916902e94	SDBBot
d0a6f9cbd6b078ecb90b0dfba541dc52377e04cee4b7885ea12967c7a26547aa	Get2
d1e1b4d3a323692bd12e81e3d7581f6754c85e748a83bc1489f105a62f203687	Get2
d316684974989cdab30c4c4dd85d9f326ec5a57cff407a92bf202d3be5906e59	Get2
dbb8abdbb80f8e8eadd339fc4e4680a082ba988034abd5d72824600d0a4b002a	Get2
df9947332481ffbd90baf6939ae5bd5b62ff2305739ef91903803ae4d88d0f57	Get2
e49953079c9f18adc26bfdd01d17add9b50f145936457ce01abc1489b143a25b	SDBBot
e7bdf82ccbc1c0da78b5747e044e77c2610cc29bc251218810ba43593fd80cfe	Get2

e88e116e8ab8c20db727a548cea792c8db45393b4f77653feb8bc13b36f02bf2	Get2
fa6141e231b320d6ed94c1bdd2ab097474aea23eca7f511ebd895d80a2fc1eea	Get2
fc6f0f8a4ff16f1e3d04f4008a0cebef168517f1b80282422e2f537473d18f82	Get2
fe97f76dd2b0c461020968f84b4399cdebb3fc2e4934f0491377ccaee568d8c5	Get2
