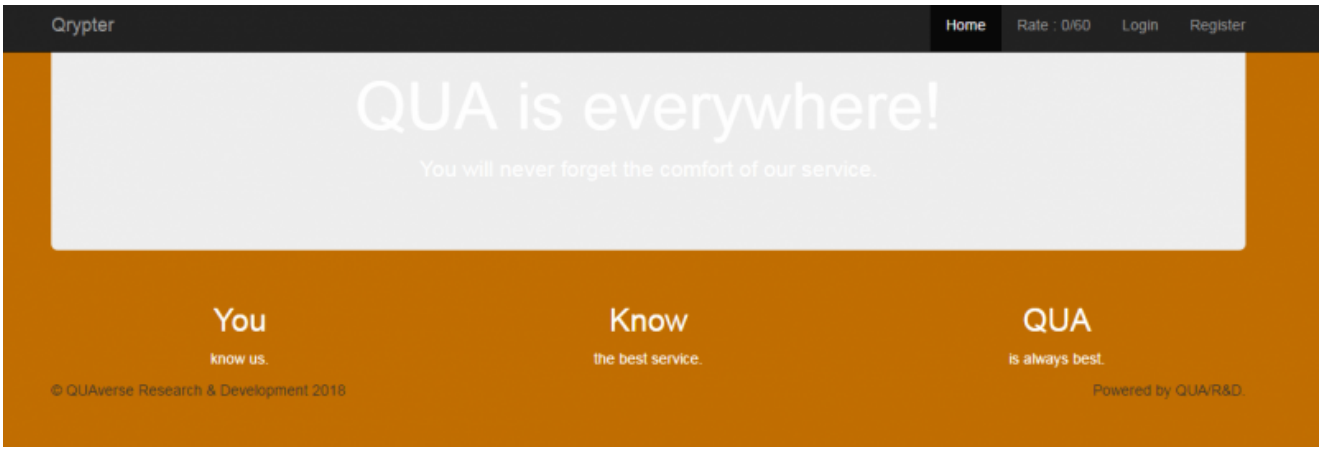
BITTER: a targeted attack against Pakistan

forcepoint.com/blog/security-labs/bitter-targeted-attack-against-pakistan

October 21, 2016

Introduction

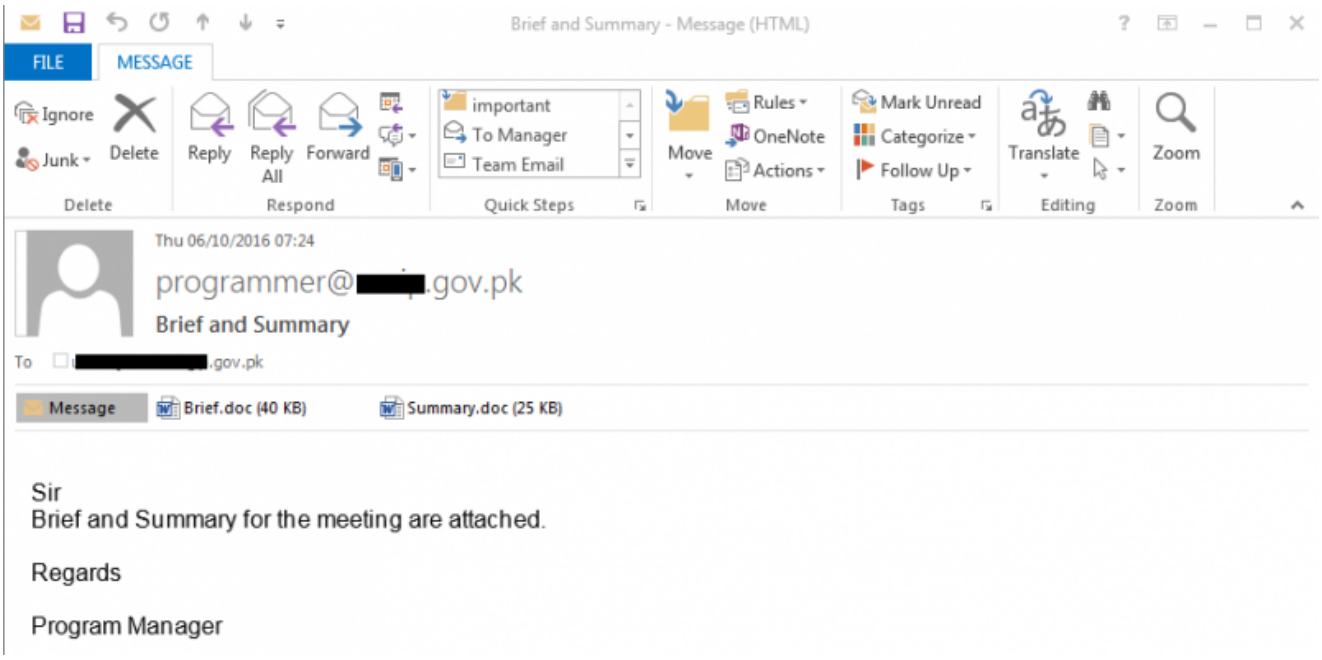
Forcepoint Security Labs™ recently encountered a strain of attacks that appear to target Pakistani nationals. We named the attack "BITTER" based on the network communication header used by the latest variant of remote access tool (RAT) used:



Our investigation indicates that the campaign has existed since at least November 2013 but has remained active until today. This post intends to share the results of our research.

Infection Vector

Spear-phishing emails are used to target prospective BITTER victims. The campaign predominantly used the older, relatively popular Microsoft Office exploit, CVE-2012-0158, in order to download and execute a RAT binary from a website. Below is an example of a spear-phishing email they used earlier this month. The recipient is an individual from a government branch in Pakistan, while the sender purports to be coming from another government branch of Pakistan:



Other attachment filenames they used that also contained the CVE-2012-0158 exploit are as follows:

Requirement List.doc

Cyber Espionage Prevention.doc

New email guidelines.doc

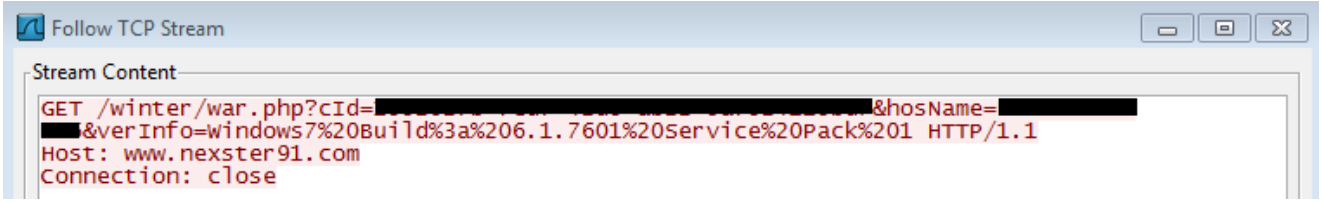
Gazala-ke-haseen-nagme.doc

Rules.xls

In one instance, they used a RAR SFX dropper that drops both their RAT and a picture of a Pakistani woman as a decoy. A quick Google image search on the dropped picture indicates that the picture was grabbed from Pakistani dating sites.

RAT Component

BITTER used RATs that are compiled using Microsoft Visual C++ 8.0. They use a few iterations of their RAT with the main difference being the RAT's command and control (C2) communication method. Earlier variants communicated to its C2 via an unencrypted HTTP POST. Below is an example of an older variant's phone home request:

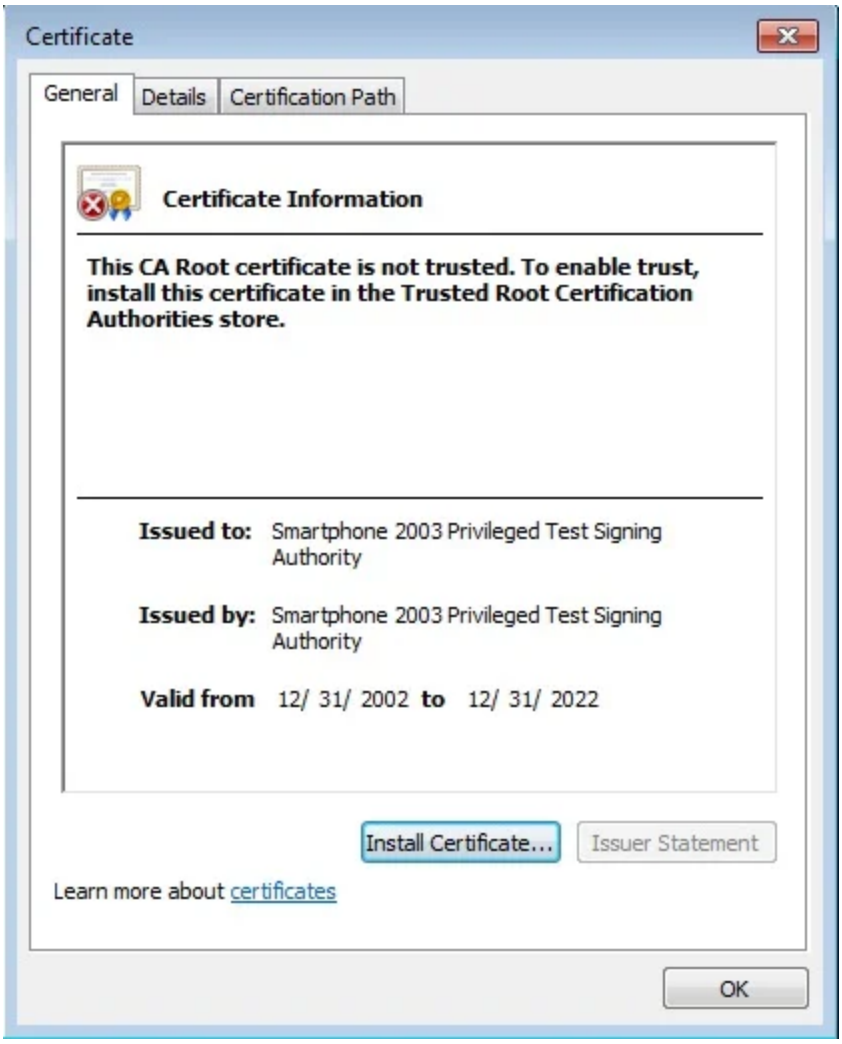


Newer ones, on the other hand, use encrypted TCP connection such as the one shown in the introduction above. Both older and newer variants are used simultaneously today in the campaign.

The RAT version (SHA1 *d7a770233848f42c5e1d5f4b88472f7cb12d5f3d*) that they used in their latest campaign is capable of executing the following backdoor capabilities, essentially allowing the attackers to gain full remote control over a victim's PC:

- Get system information - computer name, current user name, and operating system
- Enumerate logical drives
- Enumerate and log files and their corresponding timestamps
- Open a remote command shell
- List processes with active UDP connections
- Manipulate running processes
- Manipulate files
- Download a file

In addition, the vast majority of their RAT binaries contained the following digital signature with a non-trusted CA Root certificate:



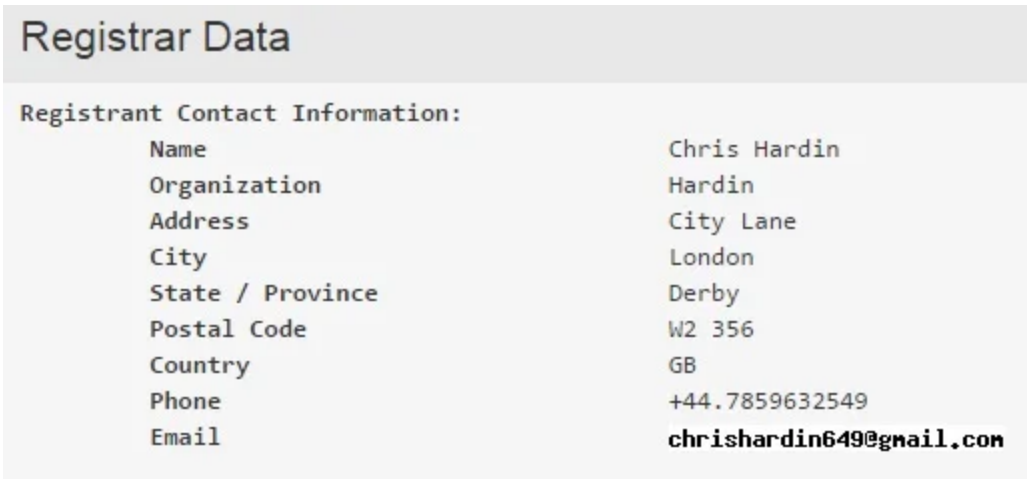
The following table shows the timeline of appearance of BITTER RATs, based on their compilation timestamps, along with their embedded PDB paths:

RAT SHA1	Compilation Timestamp	PDB Path
42cdfe465ed996c546c215a8e994a82fea7dc24c	19/11/2013 05:24	C:\Users\ANONYMOUS\Documents\Visual Studio 2008\Projects\Down Free\DownWin32\Release\DownWin32.pdb
3ab4ce4b3a44c96d6c454efcece774b33335dda2	10/09/2014 09:06	C:\Users\Bit\Desktop\uploader- Catroot 09-09-14 - Edit me\Final Uploader for ibmsoft-16-07-2014 - Copy - Copy\Uploader\fupldr_wapp\Release\svcf.pdb
1990fa48702c52688ce6da05b714a1b3e634db76	02/12/2014 05:38	F:\Fileuploader\Final\New Upl v2 -18-11-2014\fupldr_wapp\Release\svcf.pdb
93e98e9c4cf7964ea4e7a559cdd2720afb26f7f7	30/07/2015 05:03	C:\Users\ARAGON\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
c3a39dc22991fcf2455b8b6b479eda3009d6d0fd	13/08/2015 11:41	c:\Users\ARAGON\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
37e59c1b32684cedb341584387ab75990749bde7	16/10/2015 06:31	E:\RATFUD\dllhost\Release\dllhost.pdb
52485ae219d64daad6380abdc5f48678d2fbdb54	24/10/2015 04:57	C:\Users\ARAGON\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
137a7dc1c33dc04e4f00714c074f35c520f7bb97	03/12/2015 12:13	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
e57c88b302d39f4b1da33c6b781557fed5b8cece	19/12/2015 08:53	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
0172526faf5d0c72122febd2fb96e2a01ef0eff8	20/01/2016 05:23	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\DownWin32\Release\DownWin32.pdb
e7e0ba30878de73597a51637ff52e20dc94ae671d	07/03/2016 07:49	C:\Users\pc5\Documents\Visual Studio 2008\Projects\WMIS\Release\WMIS.pdb
fa8c800224786bab5a436b46acd2c223edda230e	11/03/2016 06:15	C:\Users\INFINITE\Documents\Visual Studio 2008\Projects\NewDown\Release\NewDown.pdb
c75b46b50b78e25e09485556acd2e9862dce3890	02/05/2016 17:54	C:\iexpo\Release\iexpo.pdb
72fa5250069639b6ac4f3477b85f59a24c603723	04/05/2016 04:09	c:\Users\Dexter\Documents\Visual Studio 2008\Projects\1\Release\1_3.pdb
f898794563fa2ae31218e0bb8670e08b246979c9	23/06/2016 05:42	None
2b873878b4cfbe0aeab32aff8890b2e6ceed1804	28/06/2016 09:13	C:\iexpo\Release\iexpo.pdb
d7a7702338848f42c5e1d5f4b88472f7cb12d5f3d	12/07/2016 06:27	D:\MyWork\VisualSudio\mwow\Debug\mwow.pdb
ddf5bb366c810e4d524833dcd219599380c86e7a	22/07/2016 08:56	None
23b28275887c7757fa1d024df3bd7484753bba37	02/09/2016 10:38	C:\poke\Release\poke.pdb
6caae6853d88fc35cc150e1793fef5420ff311c6	02/09/2016 10:38	C:\poke\Release\poke.pdb
1a2ec73fa90d800056516a8bdb0cc4da76f82ade	05/09/2016 07:14	C:\medal\Release\medal.pdb
ff73d3c649703f11d095bb92c956fe52c1bf5589	06/09/2016 05:48	C:\Users\ULTRON\Documents\Visual Studio 2008\Projects\Down02Sept\Release\Down02Sept.pdb

It is important to note that some of these RATs are distributed at a later time than their compilation date.

Command and Control

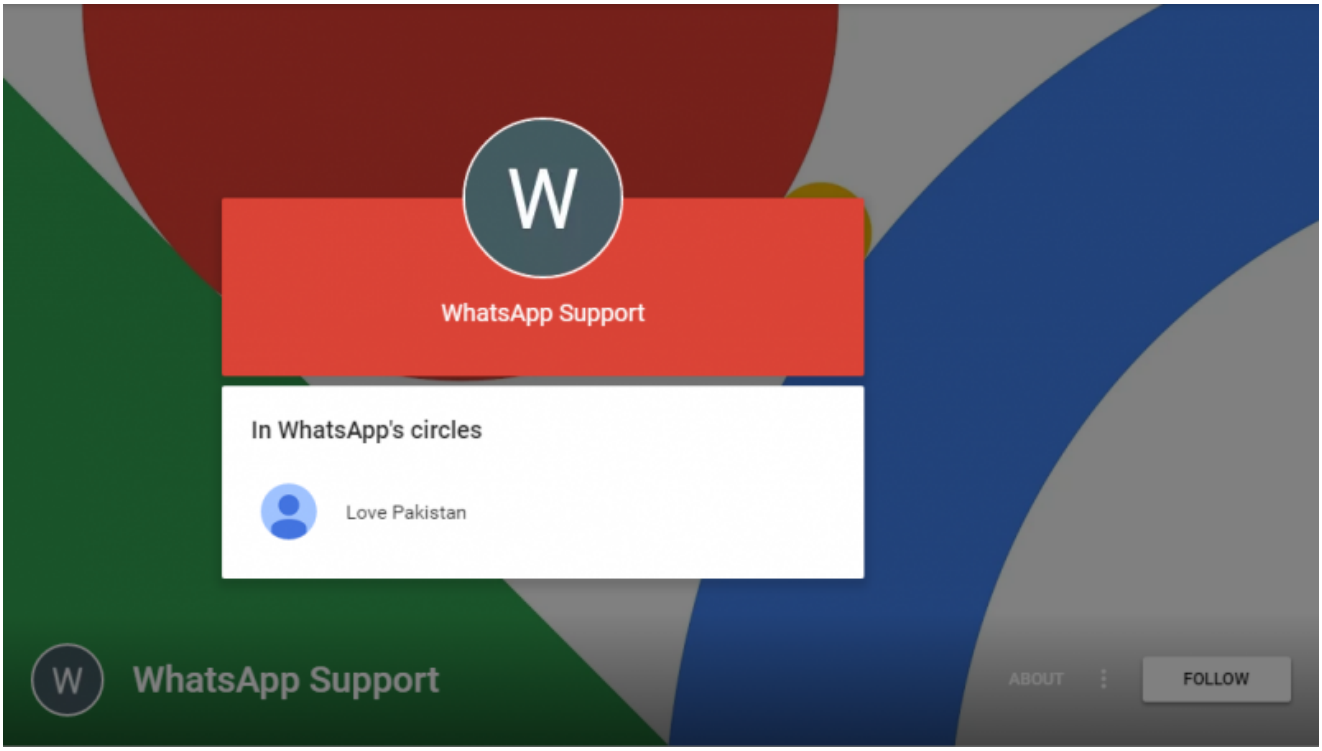
BITTER used free dynamic DNS (DDNS) and dedicated server hosting services in order to set up their C2s. The download site where the exploit documents download the RAT binaries are, in most cases, different from the actual RAT C2. However, both of them are typically registered using a Gmail email address and a spoofed identity purporting to be either from United Kingdom or Great Britain. Below is an example of a spoofed registrant information for the C2, **spiralbook71[.]com**:



A list of all related malicious domains we managed to collect are as follows:

Domain	Registrant Email	Type
ranadey.net78.net	Unknown	C2
info2t.com	Unknown	C2
range7.com	Unknown	C2 / Download Site
www.queryz4u.com	damek-martin17@post.cz	C2
www.sportszone71.com	benpaul1967@gmail.com	C2
micronet.no-ip.co.uk	Unknown	C2
www.inspire71.com	neiljohn212@gmail.com	C2
spiralbook71.com	chrishardin649@gmail.com	C2
govsite.ddns.net	Unknown	C2
randomvalue90.com	jesshardin467@gmail.com	C2
marvel89.com	fring1879@gmail.com	C2
cloudupdates.servehttp.com	Unknown	C2
pickup.ddns.net	Unknown	C2
marvel89.com	fring1879@gmail.com	C2
updateservice.redirectme.net	Unknown	C2
pickup.ddns.net	Unknown	C2
destiny91.com	andrewadams1799@gmail.com	C2
medzone71.com	roblee1546@gmail.com	C2
www.nexster91.com	witribehelp@gmail.com	C2
kart90.website	trentjohn1986@gmail.com	Download Site
scholars90.website	Unknown	Download Site
frontier89.website	Unknown	Download Site
reloadguide71.com	thomasbaker1342@gmail.com	Download Site
creed90.com	chrishardin649@gmail.com	Download Site
wester.website	Unknown	Download Site
chinatel90.com	chinglei580@gmail.com	Download Site
wester.website	Unknown	Download Site

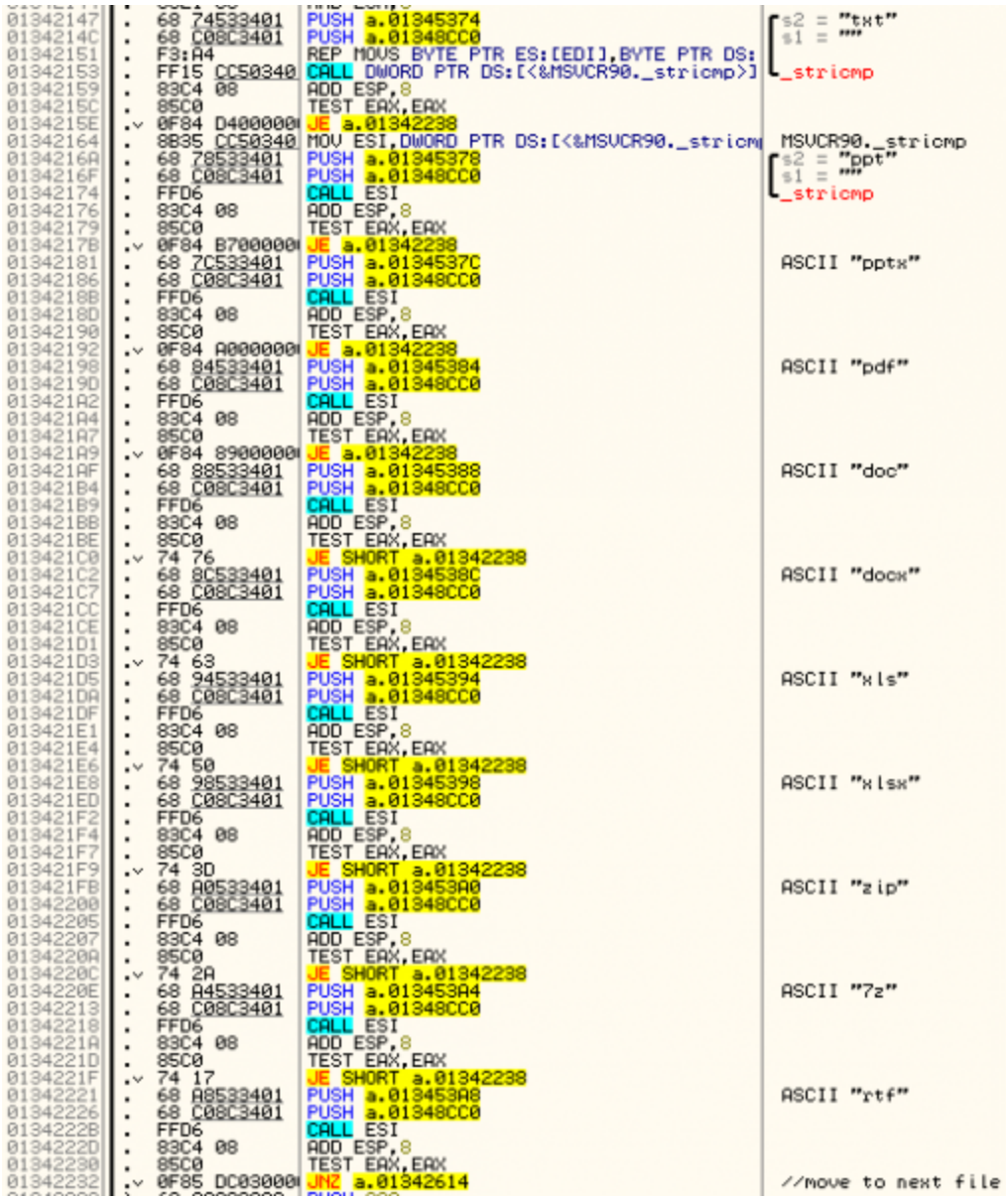
The email address **witribehelp@gmail.com** points to an empty Google Plus profile with the name "WhatsApp Support". Interestingly, however, the account is connected to another Google Plus account with the handle "Love Pakistan":



Intent

While cyber-espionage is a common motivation for targeted attacks, this is often hard to conclude unless a forensic investigation is conducted on the actual victims' machines. In some cases, specific capabilities in RATs provides us with clues on what the attackers' true intents are.

One of the backdoor capabilities mentioned above is the logging of files and files' time stamps from the victim's machine. Furthermore, an older variant of their RAT from 2014 that has the SHA1 *3ab4ce4b3a44c96d6c454efcece774b33335dda2* are found to look for more specific file types. After identifying the logical drives from a victim PC, this RAT variant proceeds to enumerate files and check if they match any of the hard coded document and archive file extensions below:

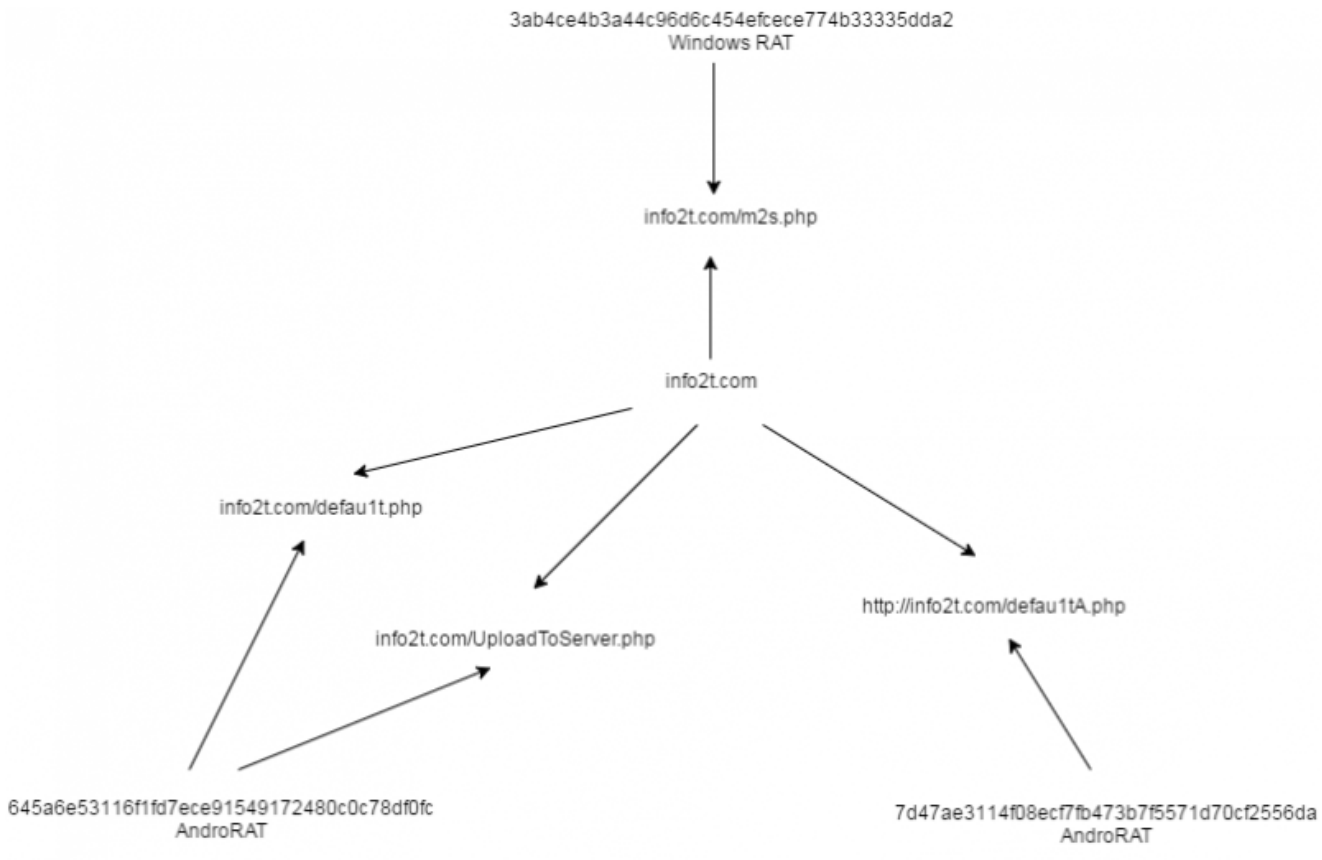


While it is hard to conclude based only on these artifacts, the nature of these targeted file types suggests that the attackers may be after sensitive documents.

Other Tools Used

In December 2015 one of the campaign's download sites hosted a binary at **scholars90[.]website/putty**. The downloaded file is a free SSH and Telnet client application called "PuTTY", which has been used in the past in other targeted attacks.

In addition, the same RAT variant previously mentioned (SHA1 *3ab4ce4b3a44c96d6c454efcece774b33335dda2*) connects to the C2 **info2t[.]com/m2s.php.** This has also served as a C2 for at least two **AndroRAT** variants in the past. The following diagram shows these relationships:



AndroRAT is an open source remote administration tool for Android. Its GitHub repository lists the following capabilities:

Get contacts (and all theirs informations)

Get call logs

Get all messages

Location by GPS/Network

Monitoring received messages in live

Monitoring phone state in live (call received, call sent, call missed..)

Take a picture from the camera

Stream sound from microphone (or other sources..)

Streaming video (for activity based client only)

Do a toast

Send a text message

Give call

Open an URL in the default browser

Do vibrate the phone

The AndroRAT variant with SHA1 *7d47ae3114f08ecf7fb473b7f5571d70cf2556da* disguises itself as the **Islam Adhan Alarm** - an Android app that alerts to prayer times of Islam, which is the state religion of Pakistan. The variant with SHA1 *645a6e53116f1fd7ece91549172480c0c78df0f*, on the other hand, disguises itself as **Kashmir News** app. Kashmir is the northernmost geographical region of South Asia and is a disputed territory between India and Pakistan.

Protection Statement

Stage 2 (Lure) - Spear-phishing e-mails associated with this attack are identified and blocked.

Stage 5 (Dropper File) - Related RATs are prevented from being downloaded.

Stage 6 (Call Home) - Communication between the RAT and command and control are blocked.

Conclusion

Many targeted attacks continue to be discovered today. It is interesting to see that while these attacks are not always sophisticated in nature, the same characteristic allows them to stay under the radar by blending in with common attacks in the wild. BITTER is able to achieve this by using available online services such as free DDNS, dedicated server hosting and Gmail to setup their C2s. Such setup is exhibited by today's common malware.

It is worth noting that in all the artifacts collected in this research, none of the English words that were used had spelling errors, suggesting that the actors behind BITTER are proficient in the English language. Furthermore, as discussed above, all the artifacts we have seen are consistent with Pakistan being the target of this group. There may be other targets that have not been discovered yet or BITTER may be a branch of a larger campaign with broader targets, but only time will tell whether any of these are correct.

Indicators of Compromise

RAT (SHA1)

```
42cdfe465ed996c546c215a8e994a82fea7dc24c
3ab4ce4b3a44c96d6c454efcece774b33335dda2
1990fa48702c52688ce6da05b714a1b3e634db76
93e98e9c4cf7964ea4e7a559cdd2720afb26f7f7
c3a39dc22991fcf2455b8b6b479eda3009d6d0fd
37e59c1b32684cedb341584387ab75990749bde7
52485ae219d64daad6380abdc5f48678d2fbdb54
137a7dc1c33dc04e4f00714c074f35c520f7bb97
e57c88b302d39f4b1da33c6b781557fed5b8cece
0172526faf5d0c72122febd2fb96e2a01ef0eff8
e7e0ba30878de73597a51637f52e20dc94ae671d
fa8c800224786bab5a436b46acd2c223edda230e
c75b46b50b78e25e09485556acd2e9862dce3890
72fa5250069639b6ac4f3477b85f59a24c603723
f898794563fa2ae31218e0bb8670e08b246979c9
2b873878b4cfbe0aeab32aff8890b2e6ceed1804
d7a770233848f42c5e1d5f4b88472f7cb12d5f3d
ddf5bb366c810e4d524833dcd219599380c86e7a
23b28275887c7757fa1d024df3bd7484753bba37
6caae6853d88fc35cc150e1793fef5420ff311c6
1a2ec73fa90d800056516a8bdb0cc4da76f82ade
ff73d3c649703f11d095bb92c956fe52c1bf5589
```

RAT Dropper (SHA1)

```
c0fcf4fcfd024467aed379b07166f2f7c86c3200
0116b053d8ed6d864f83351f306876c47ad1e227
4be6e7e7fb651c51181949cc1a2d20f61708371a
998d401edba7a9509546511981f8cd4bff5bc098
21ef1f7df01a568014a92c1f8b41c33d7b62cb40
c77b8de689caee312a29d30094be72b18eca778d
```

AndroRAT (SHA1)

```
7d47ae3114f08ecf7fb473b7f5571d70cf2556da
645a6e53116f1fd7ece91549172480c0c78df0f
```

RAT download sites

```
kart90.website/sysdll
range7.com/svcf.exe
scholars90.website/ifxc
scholars90.website/ifxc
scholars90.website/cnhost.exe
kart90.website/cnhost
frontier89.website/wmiserve
reloadguide71.com/winter/iofs
creed90.com/ismr
wester.website/uwe
chinatel90.com/min
wester.website/nqw
scholars90.website/splsrv
```

RAT C2s

```
ranadey.net78.net/Muzic/exist.php
info2t.com
range7.com/m2s_reply_u2.php
www.queryz4u.com
www.sportszone71.com/games/hill.php
micronet.no-ip.co.uk
www.inspire71.com/warzone/hill.php
spiralbook71.com/warzone/hill.php
govsite.ddns.net
randomvalue90.com/warzone/hill.php
marvel89.com/ahead.php
cloudupdates.servehttp.com
pickup.ddns.net
marvel89.com/msuds.php
updateservice.redirectme.net
pickup.ddns.net
destiny91.com/truen/adfsdsqw.php
medzone71.com/medal/adfsdsqw.php
nexster91.com/winter/war.php
```

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Our solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value.

Learn more about Forcepoint