Surtr: Malware Family Targeting the Tibetan Community

August 2, 2013

Tagged: Malware, targeted threats, Tibet

Categories: Reports and Briefings, Research News

by Katie Kleemola and Seth Hardy

Background

As part of our ongoing study into targeted attacks on human rights groups and civil society organizations, the Citizen Lab analyzed a malicious email sent to Tibetan organizations in June 2013. The email in question purported to be from a prominent member of the Tibetan community and repurposed content from a community mailing list. Attached to the email were what appeared to be three Microsoft Word documents (.doc), but which were trojaned with a malware family we call "Surtr".[1] All three attachments drop the exact same malware. We have seen the Surtr malware family used in attacks on Tibetan groups dating back to November 2012.

Delivery Mechanism

While the malicious attachments appear to be DOC files due to their file extension, they are actually RTFs crafted to exploit a vulnerability in Microsoft Word: CVE-2012-0158.

This particular vulnerability was first exploited in early April 2012 and a patch was released by Microsoft on April 10, 2012. Currently, the sample is detected as malicious by 34 percent of antivirus (AV) engines on VirusTotal (VT).

The malicious attachment is created using a shared template that we have seen used against multiple Tibetan groups. This template was created in March 2013 and, instead of specifically using the vulnerable ActiveX controls described in the vulnerability description, it utilizes the Chartspace Office Web Component. This component either suffers from the same vulnerability or uses one of the named ActiveX controls resulting in the attacker being able to execute malicious code.

Figure 1: Hexdump of the malicious attachment

```
00002e70  7b 5c 6f 62 6a 65 63 74  5c 6f 62 6a 6f 63 78 5c  |{\object\objocx\|
00002e80  66 31 33 5c 6f 62 6a 73  65 74 73 69 7a 65 5c 6f  |f13\objsetsize\o|
00002e90  62 6a 77 31 39 38 31 5c  6f 62 6a 68 31 33 32 30  |bjw1981\objh1320|
00002ea0  7b 5c 2a 5c 6f 62 6a 63  6c 61 73 73 20 4f 57 43  |{\*\objclass OWC|
00002eb0  31 30 2e 43 68 61 72 74  53 70 61 63 65 2e 31 30  |10.ChartSpace.10|
00002ec0  7d 7b 5c 2a 5c 6f 6c 65  63 6c 73 69 64 20 5c 27  |}{\*\oleclsid \'|
00002ed0  37 62 30 30 30 32 45 35  35 36 2d 30 30 30 30 2d  |7b0002E556-0000-|
00002ee0  30 30 30 30 2d 43 30 30  30 2d 30 30 30 30 30 30  |0000-C000-000000|
00002ef0  30 30 30 30 34 36 5c 27  37 64 7d 7b 5c 2a 5c 6f  |000046\'7d}{\*\o|
00002f00  62 6a 64 61 74 61 20 30  31 30 35 30 30 30 30 30  |bjdata 010500000|
00002f10  32 30 30 30 30 30 30 31  38 30 30 30 30 30 30 34  |2000000180000004|
00002f20  64 37 33 37 38 36 64 36  63 33 32 32 65 35 33 34  |d73786d6c322e534|
00002f30  31 35 38 35 38 34 64 34  63 35 32 36 35 36 31 36  |158584d4c5265616|
00002f40  34 36 35 37 32 32 65 33  35 32 65 33 30 30 30 30  |465722e352e30000|
00002f50  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
```

Although CVE-2012-0158 was first published and used in the wild in April 2012, samples using this template were only initially detected by three AV engines (on VT). Therefore, while a third of AV engines had a detection signature for CVE-2012-0158 as late as April 2013, it was possible to design a document using a year old vulnerability that was recognized as malicious by very few AV products. This number has since risen and it is currently being detected by 34 percent of the AV products listed on VT.

This vulnerability highlights the need to keep both operating systems and applications up to date as well as to exercise vigilance concerning links and email attachments.

Malicious attachments with this template all use a similar dropper which originally drops the payload to the temporary file directory.

Payload

Surtr creates either a new explorer or iexplore process and injects itself into this new process using CreateRemoteThread function.

It also creates the following folders:

%ALL USERS%/Application Data/Microsoft/Windows/123
%ALL USERS%/Application Data/Microsoft/Windows/Burn
%ALL USERS%/Application Data/Microsoft/Windows/LiveUpdata_Mem

It creates multiple copies of the payload including in both the Burn and LiveUpdata_Mem folders. The copy in the Burn folder is called [VICTIM COMPUTER NAME].dll and there are three copies in the LiveUpdata_Mem folder whose names consist of 6 random alphanumeric characters which are then appended with .dll, _Fra.dll and _One.dll. These copies will differ from the original payload dropped in the %TEMP% folder by filling the resource section with varying amounts of 00 bytes. This also results in the malware having a much larger file size (30-50mb) possibly in an attempt to evade antivirus heuristics.

Surtr connects to a command and control server (C2) and downloads a stage two component to %ALL USERS%/Application Data/Microsoft/Windows/Burn/_[VICTIM COMPUTER NAME].log. This particular sample connects to internet.3-a.net on port 9696.

In May 2012, internet.3-a.net resolved to the same IP (184.82.123.143) as android.uyghur.dnsd.me, which is a C2 used in Android malware attacks that targeted the Tibetan community as previously documented by the Citizen Lab.

The stage two component that was downloaded in this particular case has an internal name of x86_GmRemote.dll, however we have seen an alternate stage two used with the name Remote.dll as well. Our analysis in this post focuses on the GmRemote variation as it has been seen in multiple attacks.

Surtr's capabilities include listing of file directories and contents on the victim computer and any USB drives connected to a victim machine, viewing web cache, executing remote commands and logging keystrokes.

In order to store temporary information, Surtr creates the following folders:

%ALL USERS%/Application Data/Microsoft/Windows/MpCache
%ALL USERS%/Application Data/Microsoft/Windows/nView_DiskLoydb

%ALL USERS%/Application Data/Microsoft/Windows/nView_KeyLoydb
%ALL USERS%/Application Data/Microsoft/Windows/nView_skins
%ALL USERS%/Application Data/Microsoft/Windows/UsbLoydb
For example, in nView_DiskLoydb, a file called FileList.db that contains file and directory listings will be placed and nView_KeyLoydb will contain text files with keylogger output. The keylogger output is disguised by adding a constant to the ordinal value of the character.

This data can then be sent to the C2. It is compressed using zlib DEFLATE so the network traffic is not human readable without decompression.

It can also download additional malware onto the victim computer, which can provide attackers with further abilities like accessing the victim computer's webcam or microphone. In particular, we have seen Surtr used in conjunction with the Gh0st RAT derived LURK0 malware.

For persistency, Surtr adds a key to the registry to ensure it runs when the infected computer is restarted. It also stores its C2 information and a campaign code in the registry.

Depending on the configuration, Surtr will either create multiple registry keys in Software\Microsoft\Windows Media in HKU (hkey users) with text data or a single key called XC consisting of binary data. These are usually xor encrypted with a key of 0×1.

Figure 2: Encrypted data in XC key

```
00000000  03 00 00 00 00 00 00 00  68 6f 75 64 73 6f 64 75  |........houdsodu|
00000010  2f 32 2c 60 2f 6f 64 75  00 00 00 00 00 00 00 00  |/2,`/odu........|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000080  00 00 00 00 00 00 00 00  68 6f 75 64 73 6f 64 75  |........houdsodu|
00000090  2f 32 2c 60 2f 6f 64 75  00 00 00 00 00 00 00 00  |/2,`/odu........|
000000a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000100  00 00 00 00 00 00 00 00  68 6f 75 64 73 6f 64 75  |........houdsodu|
00000110  2f 32 2c 60 2f 6f 64 75  00 00 00 00 00 00 00 00  |/2,`/odu........|
00000120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000180  00 00 00 00 00 00 00 00  e1 24 00 00 e1 24 00 00  |.........$...$..|
00000190  e1 24 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |.$..............|
000001a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000370  00 00 00 00 00 00 00 00  56 46 31 37 33 35 00 00  |........VF1735..|
00000380  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
000003a0  a1 0e 00 00 00 00 00 00  2d 05 00 00 45 4e 42 2d  |........-...ENB-|
000003b0  51 45 47 2d 00 00 00 00  00 00 00 00 00 00 00 00  |QEG-............|
000003c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000420
```

Figure 3: Decrypted data (note: e0 25 is 0x25e0 which is 9696 in hex)

```
00000000  02 01 01 01 01 01 01 01  69 6e 74 65 72 6e 65 74  |........internet|
00000010  2e 33 2d 61 2e 6e 65 74  01 01 01 01 01 01 01 01  |.3-a.net........|
00000020  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
*
00000080  01 01 01 01 01 01 01 01  69 6e 74 65 72 6e 65 74  |........internet|
00000090  2e 33 2d 61 2e 6e 65 74  01 01 01 01 01 01 01 01  |.3-a.net........|
000000a0  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
*
00000100  01 01 01 01 01 01 01 01  69 6e 74 65 72 6e 65 74  |........internet|
00000110  2e 33 2d 61 2e 6e 65 74  01 01 01 01 01 01 01 01  |.3-a.net........|
00000120  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
*
00000180  01 01 01 01 01 01 01 01  e0 25 01 01 e0 25 01 01  |.........%...%..|
00000190  e0 25 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |.%..............|
000001a0  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
*
00000370  01 01 01 01 01 01 01 01  57 47 30 36 32 34 01 01  |........WG0624..|
00000380  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
*
000003a0  a0 0f 01 01 01 01 01 01  2c 04 01 01 44 4f 43 2c  |........,...DOC,|
000003b0  50 44 46 2c 01 01 01 01  01 01 01 01 01 01 01 01  |PDF,............|
000003c0  01 01 01 01 01 01 01 01  01 01 01 01 01 01 01 01  |................|
*
00000420
```

Other Samples & Variations

We have seen a large number of similar samples sent to Tibetan groups that use the same stage two (GmRemote) and communicate with the following C2s: dtl.dnsd.me, dtl.eatuo.com, dtl6.mooo.com and tbwm.wlyf.org. These C2s were also used in previous attacks documented in an earlier Citizen Lab post on LURK0 malware targeting the Tibetan community.

One particular sample (md5: ad9e5f79585eb62bc40b737e98bfd62e) which connects to C2 domain dtl6.mooo.com (which resolved to the same IP as the other dtl domains mentioned above) on port 6178 was seen to download LURK0 malware after the initial Surtr infection. This LURK0 sample had the campaign code ZQ6 that connects to C2 domain tbwm.wlyf.org on port 3103. This domain also resolved to the same IP as the dtl domains.

We have also found reports of other Surtr stage 2 (GmRemote) samples that have campaign codes which suggest they may be targeted at commercial and government targets.

The first sample was found via ThreatExpert. It uses campaign code kmlg-0308, and connects to a C2 at flyoutside.com. This domain and eight others are registered to toucan6712@163.com:

flyoutside.com	67.198.227.162
52showfly.com	112.121.169.189
mydreamfly.com	112.121.186.60
dreaminshy.com	119.42.147.101
52flyfeel.com	119.42.147.101
eyesfeel.com	180.178.63.10 (now registered to lili@nuo.cn)
outsidefly.com	74.55.57.85
showflyfeel.com	199.119.101.40
51aspirin.com	not resolving

Searching for more samples in Virus Total Intelligence (VTI) using domains and other identifying features reveals four related files:

7fbdd7cb8b46291e944fcecd5f97d135 – connects to C2 domain www.flyoutside.com, campaign code kmlg-0409tb

58ff38412ebbedb611a3afe4b3dbd8b0 – connects to C2 IP 112.121.182.149 (similar to above), campaign code lly-0311

81bc8974967e1c911b107a9a91e3178b – connects to C2 domain www.paulfrank166.2waky.com (192.198.85.102), campaign code 0201-2116

44758b9a7a6cafd1b8d1bd4c773a2577 – connects to C2 domain www.flyoutside.com (same as the first sample found on ThreatExpert), campaign code lg-0109

Most of these samples have campaign codes that suggest commercial targets. However, we do not have information about where these samples were submitted from, so the target sector and victims cannot be confirmed.

A second GmRemote sample was found via the web, called Trojan/Subxe.89E1 by Anchiva. This sample connects to google.djkcc.com and uses campaign code in1102. Other subdomains under djkcc.com include:

airforce.djkcc.com
domain.djkcc.com
google.djkcc.com
indianembassy.djkcc.com
mailnic.djkcc.com (MailNIC is an Indian email site at the National Informatics Centre)
microsoft.djkcc.com
rediffmail.djkcc.com (Rediffmail is an Indian email site)

While we do not have information about what victims these samples target, the campaign code, C2 domain, and related subdomains give some possible indications.

One additional find via VTI is a GmRemote sample internally named: GmKeyBoradServer_DLL.dll (MD5 e7e1c69496ad7cf093945d3380a2c6f4).

It exports functions (GmFunctionType, GmInitPoint, GmMyInitPoint, GmRecvPoint, GmShutPoint, GmVerSion) that are referenced in other GmRemote samples, although none of them have any real content.

These additional samples suggest that Surtr is being used to target groups beyond the Tibetan community and is possibly being utilized by multiple threat actors.

Conclusions and Recommendations

The attacks we have observed that use the Surtr malware family are another example of the persistent targeted malware campaigns the Tibetan community faces. The specific attack reported in this post demonstrates that attackers are actively monitor mailing lists and discussion groups used by the Tibetan community and repurpose the content for use in targeted malware attacks.

For communities under persistent threat from targeted malware campaigns, user vigilance and education are essential for reducing risk.

- Users should carefully examine the sender's email address of emails and exercise caution in opening unexpected or unsolicited attachments or opening unverified links.
- See Citizen Lab's Recommendations for defending against targeted cyber threats for additional information, and Tibet Action Institute's Detach from Attachments and Think Before You Click campaigns.

The Citizen Lab is continuing to monitor targeted malware campaigns using Surtr and will post updates as they are available.

–

Appendix MD5's & Identifiers

Email Attachment Names & MD5s:

1) TCCC PRESIDENT & BOARD MEMBERS NOMINATION & ELECTION POLICY & PROCEDURE.doc –

8c06aec37c7e51f581aaa41f66d4ebad2) communication1.doc – 28444ee593653a4816deb186a6eddee83) communication2.doc – c269b3cf3d336a40c2fd7c2111b52982

Stage 1

Section: .text
MD5 hash: d4f9b3b573a8f1d70d58aa8daf9cb256
SHA-1 hash: a1d5128cd50959bc7008be1fdfe2cf6339ed7098
SHA-256 hash: aef9f55931d054dbf027639e30d0abf587696b13d8993aab6c22eb7d47f0de83

Section: .rdata
MD5 hash: e130ff2adbf4515b1af88b451396e1f6
SHA-1 hash: 248691810ae34407aa3486ef3faca6fe3286f630
SHA-256 hash: adae7b2306d7fc145ebd90fd1147bc352c56937d58e1996b89d5368cebdb438d

Section: .data
MD5 hash: c4fc864da3ee8462c5c25054f00e703f
SHA-1 hash: b28a02f68cbacdaa89cf274dc79b3c802a21599d
SHA-256 hash: 203ca80897fd63ca3fc55ec4be22cd302d5d81729ee8f347bd8f22c73ad1b61d

Section: .reloc
MD5 hash: bc2c349c1f4c338c6834a79c03c461fb
SHA-1 hash: c71504a96ea72656ef826677a53f9a5230fcb049
SHA-256 hash: 58c192f73afe761b42493a36ded1a5724f06e14f44304b946341eb46b3bdfa7d

The hashes of the resource section vary based on how much it is padded.

Notable Strings:

cScCssvdcfhgshtj
CrtRunTime.log
aCvVpR
_One.dll
_Fra.dll
asasdasrqwfsdvctyqwm
efskdfjaslkfjlaksd
dksfjasdklfjasd
casfjaklsdjfaskdlf
bakjfasdkljfkldfjaslkd
adskjfksldjfklsad
soul
LiveUpdata_Mem\
Burn\

Stage 2 (downloaded component)

MD5: 21aa9dd44738d5bf9d8a8ecf53c3108c

Notable Strings:
x86_GmRemote.dll
Mark
D:\Project\GTProject\Public\List\ListManager.cpp

Footnote

[1] Surtr is a fire giant in Norse Mythology. We chose Surtr as this malware family's namesake because the malware creates a

folder named ‘Burn’

Post a Comment

Your email is *never* shared. Required fields are marked *

Name *

Email *

Website

Comment

Post Comment