Recorded Future

RedAlpha: New Campaigns Discovered Targeting the Tibetan Community

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 widerr
        $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
}
```