New Uyghur and Tibetan Themed Attacks Using PDF Exploits

By Igor Kuznetsov

Published: 2013-03-14 · Archived: 2026-04-05 17:36:44 UTC

On Feb 12th 2013, FireEye announced the discovery of an Adobe Reader 0-day exploit which is used to drop a previously unknown, advanced piece of malware. We called this new malware “ItaDuke” because it reminded us of Duqu and because of the ancient Italian comments in the shellcode copied from Dante Alighieri’s “Divine Comedy”.

Previously, we posted about another campaign hitting Governments and other institutions, named Miniduke, which was also using the same “Divine Comedy” PDF exploits.

In the meantime, we’ve come by other attacks which piggyback on the same high level exploit code, only this time the targets are different: Uyghur activists.

Together with our partner at AlienVault Labs, we analyzed these new exploits. For their blog, which includes Yara rules and industry standard IOC’s, please read [here]. For our analysis, please read below.

The new attacks

A few days ago, we observed several PDF files which carry the CVE-2013-0640/641 (ItaDuke) exploits. Some of the MD5s and filenames include:

7005e9ee9f673edad5130b3341bf5e5f 2013-Yilliq Noruz Bayram Merik isige Teklip.pdf
d00e4ac94f1e4ff67e0e0dfcf900c1a8 .pdf (joint_letter.pdf)
ad668992e15806812dd9a1514cfc065b arp.pdf

The Kaspersky detection name for these exploits is Exploit.JS.Pdfka.gjc.

If the exploit is successful, the PDFs show a clean, “lure” document to the user:

Noruz Bayram Merikisige Teklip

En'eniwiy milli bayrimimiz bolghan "Noruz" Ejdatlirimizning bizge qaldurghan bibaha-qimmetlik teweruklirining birsidur. Ejdat rohini xosh qilish, Ejdat iradisige warisliq qilish, Ejdat izidin méngish her bir Uyghur bashliq Türkiy perzentlirining bash tartip bolmaydighan muqeddes burchidur. Her yer qérindashlarning hemkarliqida ta bu yilgha kelgiche bolghan 5 yil jeryanida noruz bayrimining ayighini üzüldürmey türlük meniwi paaliyetler bilen tebriklep kelduq.

Bu yil, yeni 2013-yili 3-ayning 20-kuni(charshembe) "2013-Yilliq NORUZ BAYRAM MUBAREK" namida xas milli tüske ige, Uyghur bashliq Türkiy qerindashlirinila asas qilghan, yéngiche mezmungha mol bolghan katta merike qilishni pilanliduq. Barliq qérindashlarning qimmetlik waxtini ajritip, ariliqni yiraq dimey, qizghinliq bilen qatniship, sahipxan hem mihman bolup kitishini ümüt qilimiz.

Noruz teshkillesh hey'etlirining keng dairilik meslihetlishishi arqisida, bu yilqi noruzgha Müchenluq dostlirimiz teklip qilinmaydighan boldi. Qérindashlarning toghra chüshinishini ümid qilimiz.

Milliy bayrimimizgha téximu hösun qoshush, kelgusi izbasarlirimizgha bolghan yüksek mes'uliyetchanliqimizni közde tutup, imkan qeder milliche kiyim, imkan bolmighanda retlik kiyinip kélishinglarni soraymiz.

"Noruz bayram Merikisi" asasliq mezmuni

1. NORUZ mezmunigha xas bolghan tebrikname, xalisane biyit, qoshaq, yinik tenherket wekazalar
2. Sen'et péshiwaliri we heweskarlirining orunlishida naxsha-muzika, usul-neghme nawalar
3. Kelgusi izbasar smur-balilar mehsus NORUZ bezmisi Merike Küni:

2013-yili 3-ayning 20-küni (charshembe)

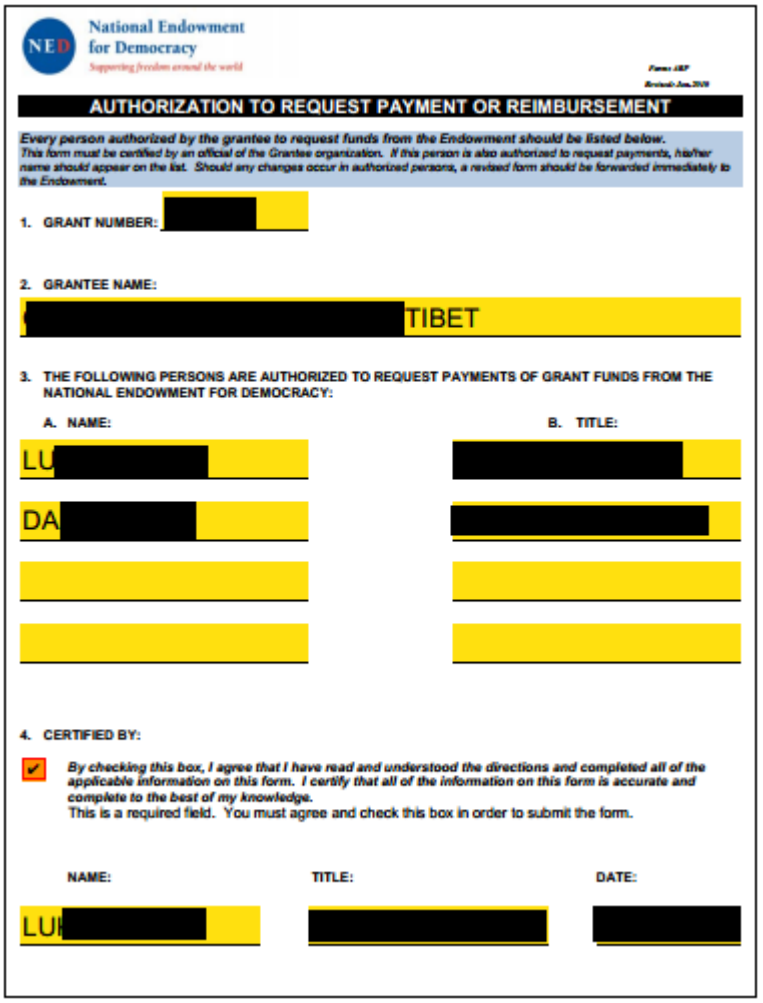
Waxti:

12:00 ~ 17:00

Hörmet Bilen:

"2013-Yilliq Noruz Bayram Merikisi "Teshkillesh Hey'etliki

2013-Yil 3-Ayning 1-Kuni



National Endowment for Democracy
Supporting freedom around the world

AUTHORIZATION TO REQUEST PAYMENT OR REIMBURSEMENT

Every person authorized by the grantee to request funds from the Endowment should be listed below. This form must be certified by an official of the Grantee organization. If this person is also authorized to request payments, his/her name should appear on the list. Should any changes occur in authorized persons, a revised form should be forwarded immediately to the Endowment.

1. GRANT NUMBER:

2. GRANTEE NAME:

TIBET

3. THE FOLLOWING PERSONS ARE AUTHORIZED TO REQUEST PAYMENTS OF GRANT FUNDS FROM THE NATIONAL ENDOWMENT FOR DEMOCRACY:

A. NAME:	B. TITLE:
LU	
DA	

4. CERTIFIED BY:

☑ *By checking this box, I agree that I have read and understood the directions and completed all of the applicable information on this form. I certify that all of the information on this form is accurate and complete to the best of my knowledge.*
This is a required field. You must agree and check this box in order to submit the form.

NAME:	TITLE:	DATE:
LU		

The first document (2013-Yilliq Noruz Bayram Merik isige Teklip.pdf) refers to a New Years party invitation. The second one, “arp.pdf”, is an authorization to request a reimbursement, for a Tibetan activist group.

The Javascript exploit code has a large comment block prepended, which was probably included to avoid detection by certain anti-malware programs.

```
%PDF-1.7
1 0 obj
<<
        /Pages 2 0 R
        /NeedsRendering true
        /AcroForm 4 0 R
        /Perms <<
                /UR3 8 0 R
        >>
        /Type /Catalog
        /OpenAction <<
                /JS (\n0 >> 0 >> 0 >> 0 >> 0 >> 0;\n
```

```
<!--
cWKQmZlaVVVVVVVVVVVcwSdcjKz85m7JVm7JFxkZmZmRDcZXAsmZmZzBJ1ys/(
yP1mrKmZmZnBEtmVEtGVEogS2KnzmxLkkc7JccKZmZkcWe2dElNyfhLYgckSwaWa
WhLB4cHJmkES0oUSyrkSwr2aUZpJmkESq8HJmmnzmGbslc9xupmZmRxZ7ZEaW50a
WptyesGqS/8Silh7m5pTmpjAxsfCEnzEW5GZzBJ1yMrLqlCqQqpLEtyRE4kZU/ma
Q0h6mtyJE5EdUHl3qlkS1JWiQO2Y2cPCwBJ8xFuVmRLcZcbHwhJ8xFpVVVVVVVV
zBJ1GuSVmeyCEtyJyfOZEtSREsiFZkvJEtyREtGBZkhyhHKCEsyJyxLclcnzmRLU
kRLIhWZLyRLckRLRjWZIxFpVVVVVVVVVVVVVVVVXMEnUadY0S3I0S0Z0Q1GkS
zI0SmxLUjRKIli7TjRTNkYEQzHVe3GWZmZmZcosS3GUaWZgQ3GUS1HUaWLEQ1HUS
zI0Sm5Yu0Z+g1GWWFDCZmZkSzHUa44mZ7NYS3IkS0aEQ1G0a5G2Z56fznfGZiZmZ
EsxtyxLcdRLUaZrRlcgSzJES271mSRDcYRLUdRLMYRDIkRLcbcnzmRLUYcgSzJES
24lmSRpdlXId853xmYmZmRLUdRLIicsS3HUS1Gma0ZXIEsyREtu9ZkkQ3GES1HUS
vInLEtx1EtSVmtGNvBLMYcsS3JES0ZVmSBpdlRLMdRLcYRDbkXCqZmZmEnzEWlVV
```

The comment block and the exploit is exactly the same among all analyzed PDF files. Interestingly, the “sHOGG” string obfuscation function from Itaduke has been removed. In addition, some of the obfuscation for variable initialization has been removed as well:

	New exploit (no obfuscation)	ItaDuke (obfuscated assignments)

JS code	ROP_ADD_ESP_4 = 0x20c680bb;
	bENEDETTO = 0x20d76e3d;
	cARPONE = 0x20cfd14d;
	sENTIRSI = 0x20cf54d4;
	rICINGHE = 0x20ce7272;
	aPPARENZA = 0x209be728;
	fISAMENTE = 0x20cfb4d5;
	pRESUNSI = 0x20801039;
	oRDERED = 0x20ce58a6;
	cOCOLLE = 0x2087d453;
		ROP_ADD_ESP_4 = 7*5*15710857;
		bENEDETTO = 127*11*394409;
		cARPONE = 83*73*5*3*3*3*673;
		sENTIRSI = 7*5*2*2*3931847;
		rICINGHE = 113*23*19*2*5573;
		aPPARENZA = 11*2*2*2*6216911;
		fISAMENTE = 59*7*1332889;
		pRESUNSI = 545263673;
		oRDERED = 3*2*91732337;
		cOCOLLE = 3*3*3*20213801;

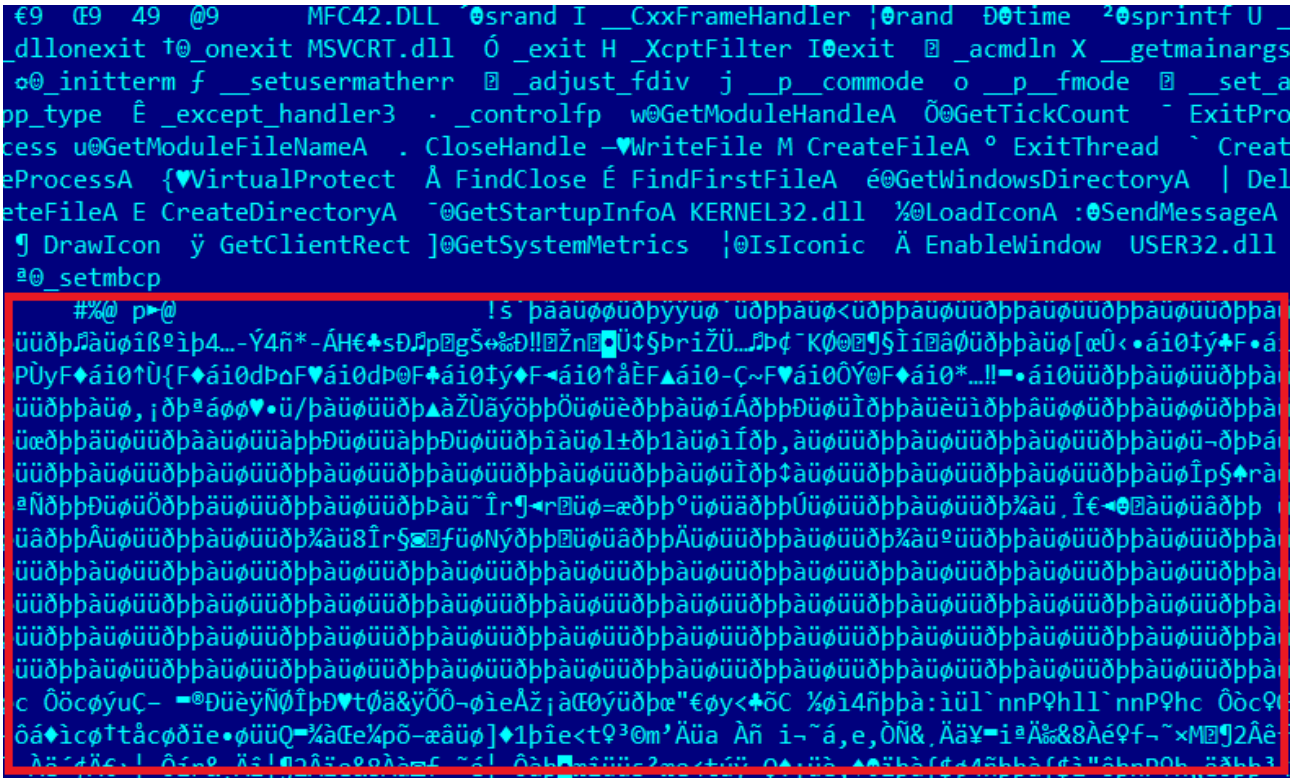
All documents drop the same malware, detected by Kaspersky as Trojan.Win32.Agent.hwoo and Trojan.Win32.Agent.hwop, which is interesting: this is one of the rare cases when the same threat actor hits both

Tibet and Uyghur activists at exactly the same time. It is possible this was done in regards to a human rights conference which is taking place in Geneva between 11-13 March, 2013.

The backdoor

The PDF malware dropper creates a file named “C:Documents and SettingsAdministratorLocal SettingsTempAcroRd32.exe” and runs it. AcroRd32.exe has a PE compilation timestamp of “Wed Jul 11 05:39:45 2012”.

“AcroRd32.exe” contains an encrypted block with the final payload, an 8KB backdoor, which is dropped as “clbcatq.dll” and run via Windows Update. The block can be easily noticed inside the backdoor by a trained eye:



The block is encrypted with a simple xor + add algorithm. Here’s the decryption algorithm for the final payload:

```
char key[]=”0l23kj@nboxu”;

a=key[i&7] + 6;
buf[i]=(buf[i]^a) + a;
```

The final backdoor (clbcatq.dll) is 9728 bytes in size. It was compiled on “Wed Jul 11 05:39:39 2012”. The backdoor connects to its C&C server and requests further data using HTTP GET requests. The response from the server is expected to be a slightly encrypted DLL, which is then loaded and called by exports “InfectFile” and “GetWorkType”.

Sample	C2 server 'A'	C2 server 'B'
7005e9ee9f673edad5130b3341bf5e5f	ly.micorsofts.net (60.211.253.28)	ip.micrsofts.com (60.211.253.28)
d00e4ac94f1e4ff67e0e0dfcf900c1a8	xdx.hotmal1.com (60.211.253.28)	ip.micrsofts.com (60.211.253.28)
ad668992e15806812dd9a1514cfc065b	hy.micrsofts.com (60.211.253.28)	ip.micrsofts.com (60.211.253.28)

For all the servers, the malware makes a request to "/news/show.asp", using a custom agent string of "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)".

At the moment, all the domains point to the same IP address: 60.211.253.28. The server is located in China, in Shandong province:

IP Information for 60.211.253.28

IP Location:	China Jinan China Unicom Shandong Province Network
ASN:	AS4837 CHINA169-BACKBONE CNCGROUP China169 Backbone
IP Address:	60.211.253.28 W R P D T
Whois Server	whois.apnic.net

```
inetnum:        60.208.0.0 - 60.217.255.255
netname:        UNICOM-SD
descr:          China Unicom Shandong province network
descr:          China Unicom
country:        CN
```

The domains "micrsofts.com" and "hotmal1.com" appear to have been registered by the same person, although with very small differences in the registration data:

Registrant Contact:
GW SY
li wen li wen (lcb_jn@sina.com)
zq dj
jiningshi, shandongsheng, cn 272000
P: +86.05372178000 F: +86.05372178000

Registrant Contact:
GW SY
li wen li wen (lcb_jn@sina.com)
zq dj
shixiaqu, beijingshi, cn 272000
P: +86.02227238836601 F: +86.02227238836601

Stage 2

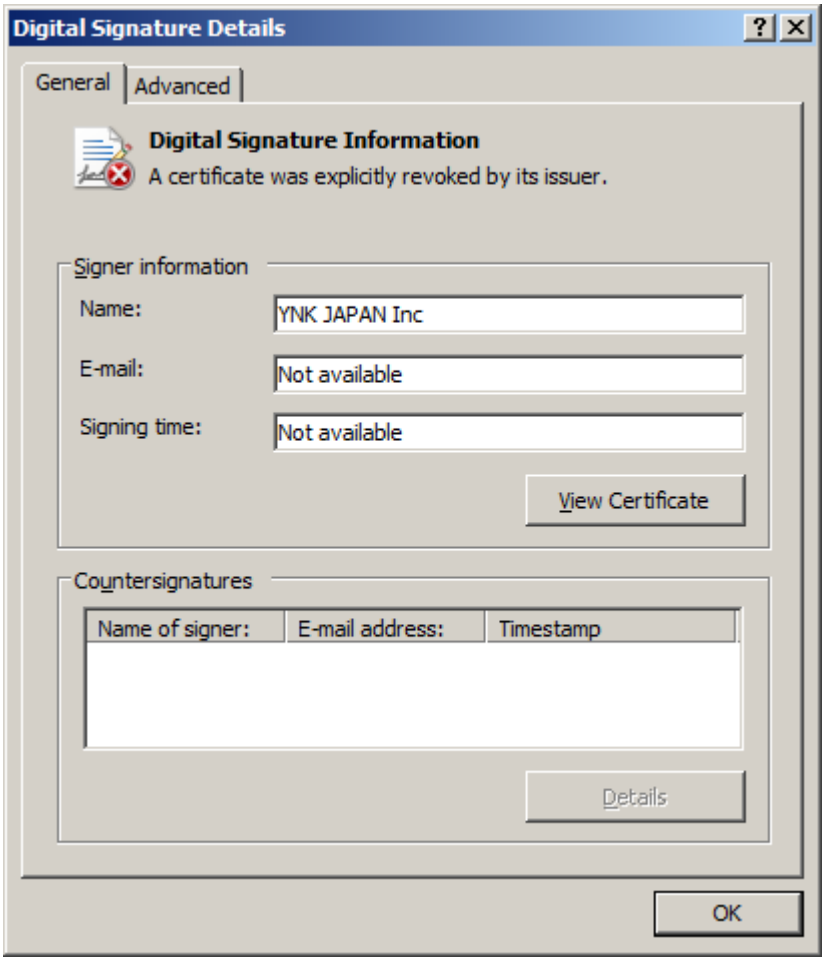
The command and control server will reply with a 300K backdoor, which is sent in encrypted form. Here's how it looks as sent by server:

The encryption is a sub 0x11 followed by a xor 0x11. Once decrypted, we get the malware dropper, which was compiled on "Wed Jul 11 06:52:48 2012". This "stage 2" malware dropper is heuristically detected by Kaspersky products as HEUR:Trojan.Win32.Generic.

The stage 2 dropper will install two files in system32wbem:

4BA5E980.PBK – 204,932 bytes (MD5 varies)
MSTD32.DLL – 31,880 bytes (MD5: 92f15c2b82e81e8ae47e361b3ecb5add)

MSTD32.DLL is signed by "YNK JAPAN Inc", with a certificate that was revoked by the issuer:



This technique reminds us of the method used by the malware from the Tilded platform (Duqu, Stuxnet) for starting up (small signed loader which reads and executes main body kept in encrypted form).

Our colleagues from Norman have previously written (http://blogs.norman.com/2011/security-research/invisible-ynk-a-code-signing-conundrum) about this compromised certificate in relation to Hupigon and other malware.

The final stage malware is known by our products as Trojan.Win32.Swisyn and has pretty extensive functionality for data stealing.

Conclusions

We have previously published blogs about targeted attacks against Tibetan and Uyghur activists.

The threat actors behind these attacks are very active and continuously use new methods and new exploits to attack their victims. We have previously seen the use of CVE-2013-0158 or CVE-2010-3333, in addition to exploits for Mac OS X, taking advantage of CVE-2009-0563.

The PDF exploit originally discovered by FireEye is the first known exploit capable of bypassing the Adobe Reader X sandbox. Due to this advanced capability, it is extremely valuable to any attacker. Although it was probably developed for (or by) use of a nation state originally, we now see it being copied and reused by other threat actors. This is becoming a common procedure nowadays and we can expect more such piggybacking or exploit stealing in the future.
