Einladen Challenge

Sherlock Scenario
Our staff recently received an invite to the German embassy to bid farewell to the Germany Ambassador. We believe this invite was a phishing email due to alerts that fired on our organisation's SIEM tooling following the receipt of such mail. We have provided a wide variety of artifacts inclusive of numerous binaries, a network capture, DLLs from the host system and also a .hta file. Please analyse and complete the questions detailed below! Warning This is a warning that this Sherlock includes software that is going to interact with your computer and files. This software has been intentionally included for educational purposes and is NOT intended to be executed or used otherwise. Always handle such files in isolated, controlled, and secure environments. Once the Sherlock zip has been unzipped, you will find a DANGER.txt file. Please read this to proceed.

Task 1:
The victim visited a web page. The HTML file of the web page has been provided as 'downloader.html' sample file.The web page downloads a ZIP file named 'Invitation_Farewell_DE_EMB.zip'. What is the SHA-256 hash of the ZIP file?

I opened the "downloader.html" and downloaded the file "Invitation_Farewell_DE_EMB.zip" then I used HashMyFiles to get the SHA256

Answer: 5D4BF026FAD40979541EFD2419EC0B042C8CF83BC1A61CBCC069EFE0069CCD27

Task 2:
The downloaded ZIP file contains a HTA file, which creates multiple files. One of those files is a signed file by Microsoft Corporation. In HTA file, which variable's value was the content of that signed file?

I opened the "Invitation_Farewell_DE_EMB.hta" file with Notepad++ and scrolled down to the bottom

```
</script>
<script language="vbscript">
 CreateObject("WScript.Shell").Exec "C:\\windows\\tasks\\msoev.exe"
</script>
</script>
</head>
<body>
</body>
</html>
```

msoev.exe , according to spyshelter.com is: a process made by Microsoft itself to collect Telemetry information for the Microsoft Office software. The Telemetry helps Microsoft fix issues, and improve the Office software, like Word, Excel, or Outlook. 9 May 2024

Answer: msoev.exe

Task 3:

This answer can be found from the description

Sherlock Scenario
Our staff recently received an invite to the German embassy to bid farewell to the Germany Ambassador.

Also can be found from the "Invitation.pdf"

Auswärtiges Amt

The Embassy of Germany

requests the pleasure of your company
at a reception to bid farewell to
Ambassador of Germany

on Wednesday, 26 July 2023 at 18.30

German Residence

RSVP by 21 July
martine.carey@diplo.de

Answer: Germany

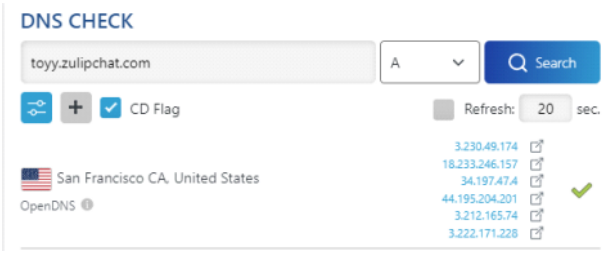
Task 4:
The malware communicated with a chatting platform domain. What is the domain name (inclusive of sub domain) the malware connects to?

I executed the malware inside Any Run sandbox and checked the DNS Requests

Answer: toyy.zulipchat.com

Task 5:
How many DNS A records were found for that domain?

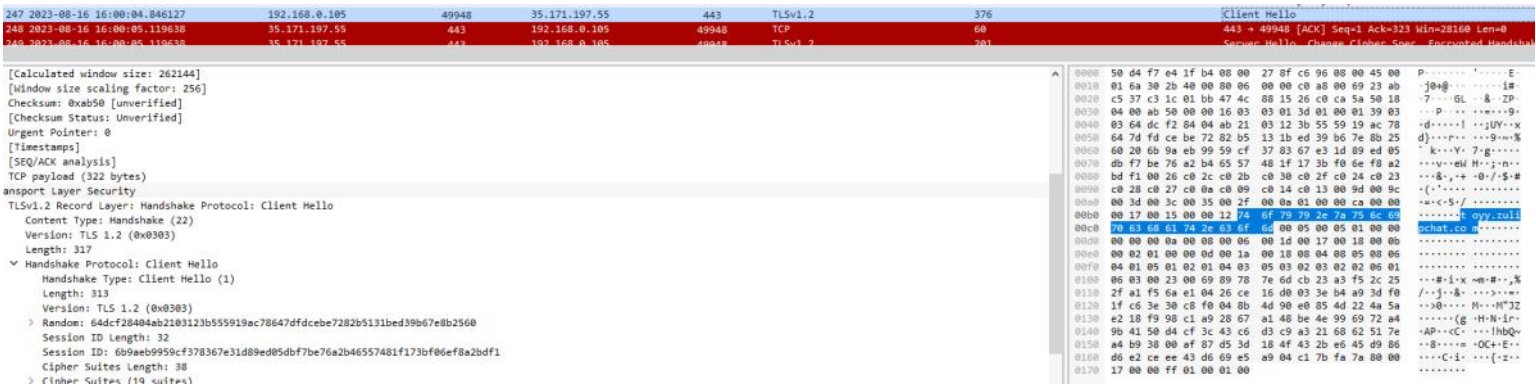
Same like task 4, 6 DNS.
Also checked in DNS Checker



Answer: 6

Task 6:
It seems like the chatting service was running on a very known cloud service using a FQDN, where the FQDN contains the IP address of the chatting domain in reversive format somehow. What is the FQDN?

I opened the Wireshark file msoev.pcapng and searched for the string "toyy.zulipchat.com"
Then I saw the "Client Hello" packet towards the destination IP 35.171.197.55 of the URL

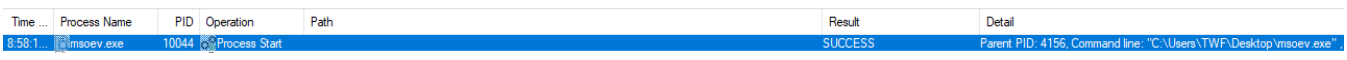


Then I checked the IP inside AbuseIPDB and found the hostname

Answer: ec2-35-171-197-55.compute-1.amazonaws.com

Task 7:
What was the parent PID (PPID) of the malware?

I opened the Logfile.PML which is a ProcMon file and found the PID inside the Detail tab



Answer: 4156

Task 8:
What was the computer name of the victim computer?

From same log in task 7, I clicked on Properties

Parent PID:	4156
Command line:	"C:\Users\TWF\Desktop\msoev.exe"
Current directory:	C:\Users\TWF\Desktop\
Environment:	

```
=::=::\
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\TWF\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-O88AN4O
```

Answer: DESKTOP-O88AN4O

Task 9:
What was the username of the victim computer?

Same like task 7 and 8 from same log

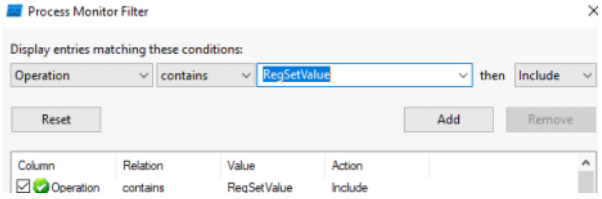
Parent PID:	4156
Command line:	"C:\Users\TWF\Desktop\msoev.exe"
Current directory:	C:\Users\TWF\Desktop\
Environment:	

Answer: TWF

Task 10:
How many times were the Windows Registry keys set with a data value?

I searched in the Procmon file for only the Registry events

Then I filtered for the operation "RegSetValue"



Time ...	Process Name	PID	Operation	Path	Result	Detail
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content\Cache...	SUCCESS	Type: REG_SZ, Length: 2, Data:
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies\Cache...	SUCCESS	Type: REG_SZ, Length: 16, Data: Cookie:
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History\CachePr...	SUCCESS	Type: REG_SZ, Length: 18, Data: Visited:
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
8:58:3...	msoev.exe	10044	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0

Answer: 11

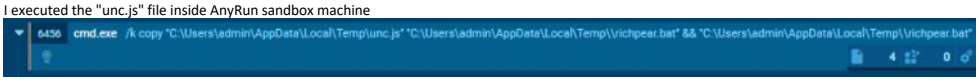
Task 11:
Did the malicious mso.dll load by the malware executable successfully?

I searched the mso.dll in the ProcMon

Answer: yes

Task 12:
The JavaScript file tries to write itself as a .bat file. What is the .bat file name (name+extension) it tries to write itself as?

I executed the "unc.js" file inside AnyRun sandbox machine

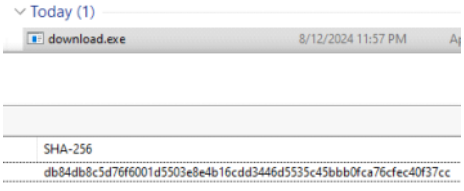


Answer: richpear.bat

Task 13:
The JavaScript file contains a big text which is encoded as Base64. If you decode that Base64 text and write its content as an EXE file. What will be the SHA256 hash of the EXE?

I copied the Base64 from the unc.js file and decode it in CyberChef

Then I downloaded it and saved it as .exe and used HashMyFiles



Answer: DB84DB8C5D76F6001D5503E8E4B16CDD3446D5535C45BBB0FCA76CFEC40F37CC

Task 14:
The malware contains a class Client.Settings which sets different configurations. It has a variable 'Ports' where the value is Base64 encoded. The value is decrypted using Aes256.Decrypt. After decryption, what will be its value (the decrypted value will be inside double quotation)?

I checked the Hash from task 13 - DB84DB8C5D76F6001D5503E8E4B16CDD3446D5535C45BBB0FCA76CFEC40F37CC in Virus total and inside the Behavior tab at the bottom of the page there is a "Decoded Text" with some ports from the question in the task

Answer: 666,777,111,5544

Task 15:
The malware sends a HTTP request to a URI and checks the country code or country name of the victim

machine. To which URI does the malware sends request for this?

Checking the malware EmpireClient in ILSpy, I found the GetCountryName() under Client.Helper - Antisng

```
internal class Antisng
{
    public class CountryConverter : JavaScriptConverter
    {...}

    public static void GetSNG()
    {...}

    public static string GetCountryName()
    {
        string requestUriString = "http://ip-api.com/json/";
        string input = string.Empty;
        try
        {
            HttpWebRequest obj = (HttpWebRequest)WebRequest.Create(requestUriString);
            obj.Method = "GET";
            obj.ContentType = "application/json";
            using (HttpWebResponse httpWebResponse = (HttpWebResponse)obj.GetResponse())
            {
                using StreamReader streamReader = new StreamReader(httpWebResponse.GetResponseStream());
                input = streamReader.ReadToEnd();
            }
            JavaScriptSerializer javaScriptSerializer = new JavaScriptSerializer();
            javaScriptSerializer.RegisterConverters(new CountryConverter[1]
            {
                new CountryConverter()
            });
            dynamic val = javaScriptSerializer.Deserialize<object>(input);
            return val["country"];
        }
        catch
        {
        }
        return "Unknown country";
    }

    public static string GetCountryCode()
    {...}
}
```

Answer: http://ip-api.com/json/

Task 16:
After getting the country code or country name of the victim machine, the malware checks some country codes and a country name. In case of the country name, if the name is matched with the victim machine's country name, the malware terminates itself. What is the country name it checks with the victim system?

Same like Task 15, at the Antisng - GetSNG() functions

```
public static void GetSNG()
{
    string countryCode = GetCountryCode();
    string countryName = GetCountryName();
    switch (countryCode)
    {
    default:
        if (!(countryName == "Russia"))
        {
            break;
        }
        goto case "RU";
    case "RU":
    case "AZ":
    case "AM":
    case "BY":
    case "KZ":
    case "KG":
    case "MD":
    case "TJ":
    case "TM":
    case "UZ":
        Environment.Exit(0);
        break;
    }
}
```

Answer: Russia

Task 17:
As an anti-debugging functionality, the malware checks if there is any process running where the process name is a debugger. What is the debugger name it tries to check if that's running?

Under the Client.Helper function I saw the Anti_Analysis with the process running

```
public static void RunAntiAnalysis()
{
    if (DetectManufacturer() || DetectDebugger() || DetectSandboxie() || IsSmallDisk() || IsXP() || IsProcessRunning("dnSpy") || CheckWMI())
    {
        Environment.FailFast(null);
    }
}
```

Answer: dnSpy

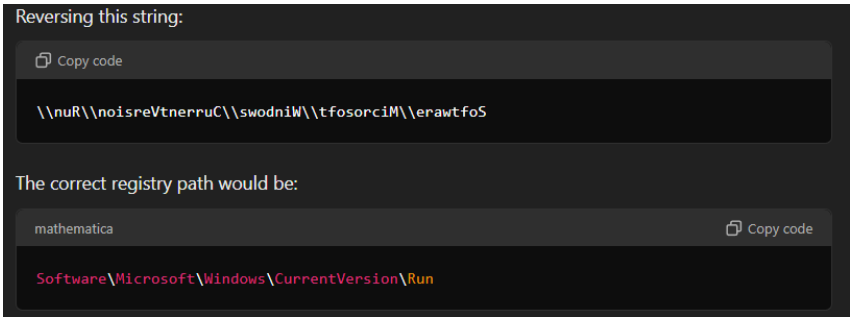
Task 18:
For persistence, the malware writes a Registry key where the registry key is hardcoded in the malware in reversed format. What is the registry key after reversing?

Checking the ILSpy under Client.Install - NormalStartup I saw the scheduled task and right after it the

Registry key in reverse

```
    }
}
if (Methods.IsAdmin())
{
    ProcessStartInfo processStartInfo = new ProcessStartInfo();
    processStartInfo.FileName = "cmd";
    processStartInfo.Arguments = "/c schtasks /create /f /sc onlogon /rl highest /tn \"" + Path.GetFileNameWithoutExtension(text) + "\" /tr \"" + text + "\" & exit";
    processStartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    processStartInfo.CreateNoWindow = true;
    Process.Start(processStartInfo);
}
else
{
    using RegistryKey registryKey = Registry.CurrentUser.OpenSubKey(Strings.StrReverse("\\nuR\\noisreVtnerruC\\swodniW\\tfosorciM\\erawtfoS"), RegistryKeyPermissionCheck.ReadWriteSubTree);
    registryKey?.SetValue(Path.GetFileNameWithoutExtension(text), "\"" + text + "\"");
```

I copied the string to ChatGPT



Then I found the HKCU under the Client.Helper - SetRegistry

```
private static readonly string ID = "Software\\" + Settings.Hwid;

public static bool SetValue(string name, byte[] value)
{
    try
    {
        Registry.SetValue("HKEY_CURRENT_USER\\" + ID, name, value, RegistryValueKind.Binary);
        return true;
    }
    catch (Exception ex)
    {
        Packet.Error(ex.Message);
        return false;
```

Answer: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\

Task 19:
The malware sets a scheduled task. What is the Run Level for the scheduled task/job it sets?

In the ILSpy under the Client.Install - NormalStartup function, I saw a filename "cmd" with the arguments of "/c schtasks /create /f /sc onlogon /rl highest /tn \"

```
ProcessStartInfo processStartInfo = new ProcessStartInfo();
processStartInfo.FileName = "cmd";
processStartInfo.Arguments = "/c schtasks /create /f /sc onlogon /rl highest /tn \"" + Path.GetFileNameWithoutExtension(text) + "\" /tr \"" + text + "\" & exit";
processStartInfo.WindowStyle = ProcessWindowStyle.Hidden;
processStartInfo.CreateNoWindow = true;
Process.Start(processStartInfo);
```

The Run Level for the scheduled task or job set by the malware is **highest**.
This means the scheduled task will run with the highest privileges available, typically as an administrator.

Answer: highest