باسمه تعالی

تحلیل فنی باج افزار CSGO

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام CSGO خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در اواسط ماه آوریل سال ۲۰۱۸ میلادی شروع شده است. همزمان با انتشار این باج‌افزار، باج‌افزار دیگری به نام Minecraft نیز شروع به فعالیت نمود که شباهت بسیار زیادی در کدمنبع و نوع فعالیت آن با باج‌افزار CSGO دارد و احتمالاً هر دوی این باج‌افزارها توسط یک گروه توسعه داده شده‌اند. این باج‌افزار نام خود را از نام یک بازی به نام Counter-Strike Global Offensive به ارث برده است و به نظر می‌رسد همانند باج‌افزارPUBG، قربانیان جهت رمزگشایی فایل‌ها، می‌بایست به انجام بازی بپزدازند. اما این گونه نیست و برخلاف باج‌افزار PUBG، این باج‌افزار قادر به رمزگذاری هیچ یک از فایل‌ها نیست و پس از اجرا فقط یک پنجره به نمایش می‌گذارد و کار خاصی از پیش نمی‌برد. به نظر می‌رسد این باج‌افزار و باج‌افزار Minecraft در حال توسعه می‌باشند و بیشتر جهت جلب توجه رسانه‌ها ارائه شده‌اند.

مشخصات فایل اجرایی باج‌افزار CSGO :

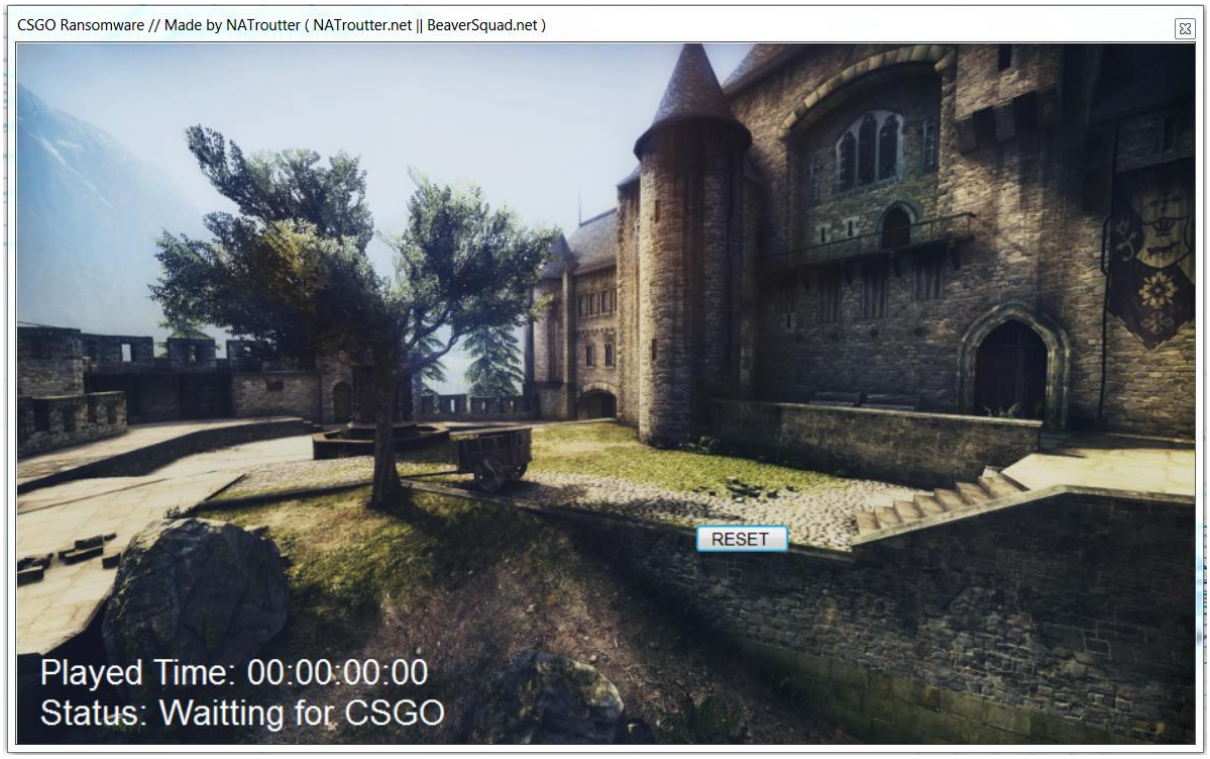
نام فایل	CSGO Ransomware.exe
MD۵	۱۹۵۰٤eb۱c۵d۲۱d۸۹٦d۷e۲۱۷f٦٦۰۳۱b۷b
SHA-۱	۹۰cb٤ef٤٤cfd۹b۳۸۱e٤۲٦۰۷۲٤d۸ec۵۱۲۹ea۵d٦۰۳
SHA-۲۵٦	۸۵۲۲f۰a۵٤٦fe۵٦٦۵۲۹f٤۸b٦۷c۸d۹۲d۵cab۸۲fe٦۷٤۷۱۲٤۹۰۹۷b۳b۰b۰۹۵fe۱a۱۵٤
اندازه فایل	۲.٦۸ MB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی باج افزار CSGO دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۹۱	۸۱۹۲	۲۸۰۲۳٤۰	۲۸۰۲٦۸۸
.rsrc	٤.۱۸	۲۸۱۸۰٤۸	۱۵۰۰	۱۵۳٦
.reloc	۰.۱	۲۸۲٦۲٤۰	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار CSGO، فایل اجرایی آن‌ها را در محیط آزمایشگاهی اجرا نمودیم تا عملکرد آن‌ها را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از بررسی‌ها نشان می‌دهد که احتمالا این باج‌افزار در حال توسعه می‌باشد و در حال حاضر قادر به رمزگذاری فایل‌ها نمی‌باشد و تنها پس از اجرا یک پنجره به نمایش می‌گذارد و فعالیت دیگری انجام نمی دهد.



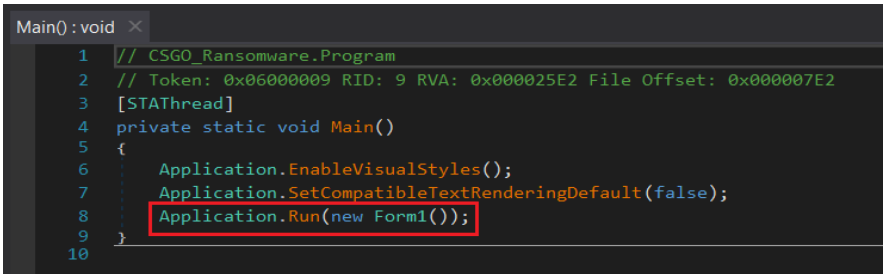
پنجره مربوط به اجرای باج‌افزار CSGO

طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ این باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

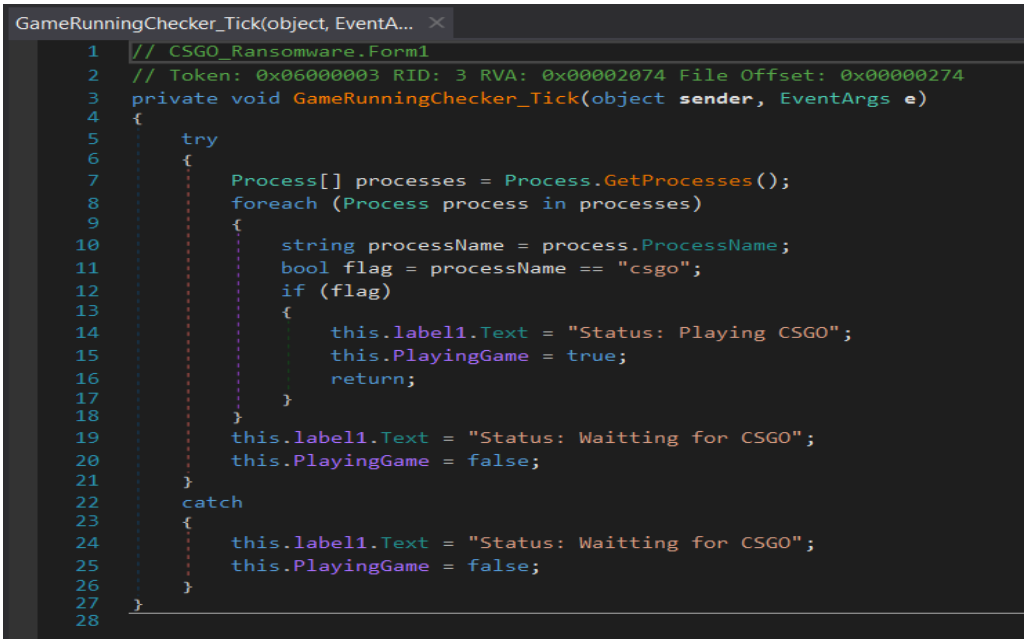
تحلیل ایستا:

پس از تحلیل کد باج‌افزار CSGO به نتایج زیر دست پیدا کردیم.

تصویر زیر کدمنبع تابع Main باج‌افزار CSGO می‌باشد که برای اجرا تابع Form۱() را فراخوانی می‌کند :



قطعه کد زیر مربوط به بررسی انجام بازی در باج‌افزار CSGO می‌باشد :



باج‌افزار CSGO در پنجره‌ی مربوط به خود یک تایمر به نمایش می‌گذارد که نشان می‌دهد قربانی چه مدتی بازی نموده است، این مورد یکی از تفاوت‌های این باج‌افزار و باج‌افزار Minecraft می‌باشد، در تصویر زیر می‌توان این قطعه کد را مشاهده نمود :

PlayingTime_Tick(object, EventArgs) : void

```
// CSGO_Ransomware.Form1
// Token: 0x06000004 RID: 4 RVA: 0x00002120 File Offset: 0x00000320
private void PlayingTime_Tick(object sender, EventArgs e)
{
    bool playingGame = this.PlayingGame;
    if (playingGame)
    {
        int num = Settings.Default.PlayTime;
        num++;
        Settings.Default.PlayTime = num;
        Settings.Default.Save();
        TimeSpan timeSpan = TimeSpan.FromMilliseconds((double)num);
        string text = ((double)timeSpan.Milliseconds / 15.6).ToString();
        string[] array = text.Split(new char[]
        {
            ','
        });
        this.label2.Text = num + string.Format(" - Played Time: {0}:{1}:{2}:{3}", new object[]
        {
            timeSpan.Hours,
            timeSpan.Minutes,
            timeSpan.Seconds,
            array[0]
        });
    }
}
```

باج‌افزار CSGO فقط از کتابخانه ویندوزی زیر به همراه یک تابع از آن، استفاده می‌کند.

mscoree.dll
_CorExeMain

تحلیل ترافیک شبکه :

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

شناسایی :

در حال حاضر تعداد ۳۱ مورد از ۵۹ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی باج‌افزار CSGO و آن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.GameChecker.1137F...	AegisLab	Gen.Heur.Ransom!c
AhnLab-V3	Trojan/Win32.Occamy.R225999	ALYac	Trojan.Ransom.CSGORansom
Arcabit	Generic.Ransom.GameChecker.1137F...	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	JOKE/csgo.Agent.2683
AVware	Trojan.Win32.Generic!BT	BitDefender	Generic.Ransom.GameChecker.1137F...
CAT-QuickHeal	Trojan.Tiggre	Comodo	.UnclassifiedMalware
Cyren	W32/Trojan.JTRT-5298	Emsisoft	Generic.Ransom.GameChecker.1137F... (B)
eScan	Generic.Ransom.GameChecker.1137F...	ESET-NOD32	a variant of Generik.EBVHCWN
F-Secure	Generic.Ransom.GameChecker.1137F...	Fortinet	PossibleThreat
GData	Win32.Trojan-Ransom.Filecoder.P@gen	K7AntiVirus	Trojan (00531ec71)
K7GW	Trojan (00531ec71)	MAX	malware (ai score=95)
Microsoft	Trojan:Win32/Tiggre!rfn	NANO-Antivirus	Trojan.Win32.Ric.fcbnbc
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.935
Sophos AV	Mal/Generic-S	Sophos ML	heuristic
Symantec	Trojan Horse	Tencent	Win32.Trojan.Generic.Dygm
VIPRE	Trojan.Win32.Generic!BT	Antiy-AVL	Clean