باسمه تعالی

تحلیل فنی باج افزار Minecraft

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام Minecraft 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 CSGO نیز شروع به فعالیت نمود که شباهت بسیار زیادی در کدمنبع و نوع فعالیت آن با باج‌افزار Minecraft دارد و به نظر می‌رسد هر دوی این باج‌افزارها توسط یک گروه توسعه داده شده‌اند. این باج‌افزار نام خود را از نام یک بازی به نام Minecraft به ارث برده است و احتمالاً همانند باج‌افزارPUBG، قربانیان جهت رمزگشایی فایل‌ها، می‌بایست به انجام بازی بپردازند. 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 CSGO در حال توسعه می‌باشند و بیشتر جهت جلب توجه رسانه‌ها ارائه شده‌اند.

مشخصات فایل اجرایی باج‌افزار Minecraft :

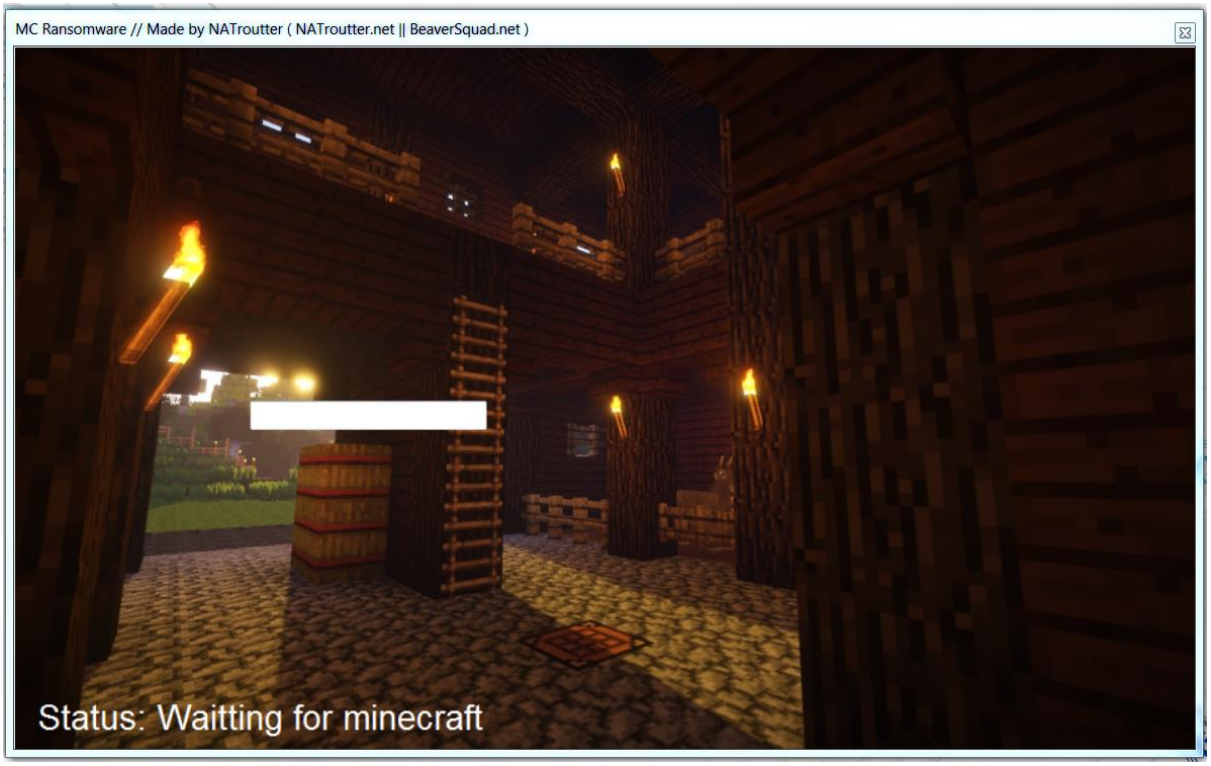
نام فایل	MC Ransomware.exe
MD۵	cd۲c۷۲de۱f۳۶۲۶۵۱۲٤۲۹۲۰۳۱b۲۰۸۵۹df
SHA-۱	۸f۳a٤۷۲cc۸۱۸a۰۵٤d۷۱c۷a٤e۲d٤۰bbe۰c۱۱۲۲۸٦d
SHA-۲۵٦	۲d۱eb۵۷۹۷b۸fbcbea۸٤٦۲b٤۷۰da۳٤۳ba۹۵d۵٤۵۸۰۸d۸۳f۷۱b۸۷٦۳e۱daf۷٦٤۸b۱٤
اندازه فایل	۲۹۵ KB
کامپایلر	Microsoft visual C# v۷.۰ / Basic .NET

فایل اجرایی باج افزار Minecraft دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۷.۹٦	۸۱۹۲	۲۹۹۱۹٦	۲۹۹۵۲۰
.rsrc	٤.۱۳	۳۱۱۲۹٦	۱٤۸٤	۱۵۳٦
.reloc	۰.۱	۳۱۹٤۸۸	۱۲	۵۱۲

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار Minecraft، فایل اجرایی آن را در محیط آزمایشگاهی اجرا نمودیم تا عملکرد آن 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 می‌گذارند و فعالیت دیگری انجام نمی‌دهد.



پنجره مربوط به اجرای باج‌افزار Minecraft

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 Minecraft به نتایج زیر دست پیدا کردیم.

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

Main() : void

```
// MC_Ransomware.Program
// Token: 0x06000006 RID: 6 RVA: 0x0000233D File Offset: 0x0000053D
[STAThread]
private static void Main()
{
    Application.EnableVisualStyles();
    Application.SetCompatibleTextRenderingDefault(false);
    Application.Run(new Main());
}
```

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

GameOnlineChecker_Tick(object, EventAr...

```
// MC_Ransomware.Main
// Token: 0x06000003 RID: 3 RVA: 0x0000206C File Offset: 0x0000026C
private void GameOnlineChecker_Tick(object sender, EventArgs e)
{
    try
    {
        Process[] processes = Process.GetProcesses();
        foreach (Process process in processes)
        {
            string processName = process.ProcessName;
            bool flag = processName != "MinecraftLauncher";
            if (flag)
            {
                bool flag2 = processName.Contains("Minecraft");
                if (flag2)
                {
                    this.label1.Text = "Status: Playing minecraft";
                    this.textBox1.Text = processName;
                    return;
                }
            }
        }
        this.label1.Text = "Status: Waitting for minecraft";
    }
    catch
    {
        this.label1.Text = "Status: Waitting for minecraft";
    }
}
```

باج‌افزار Minecraft 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 Minecraft نشدیم.

شناسایی :

در حال حاضر تعداد ۳۹ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی باج‌افزار Minecraft وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Generic.Ransom.GameChecker.6E502...	AegisLab	Gen.Heur.Ransom!c
AhnLab-V3	Trojan/Win32.Tiggre.R225982	ALYac	Trojan.Ransom.MCRansom
Arcabit	Generic.Ransom.GameChecker.6E502...	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	JOKE/Minecraft.Agent.2951
AVware	Trojan.Win32.Generic!BT	BitDefender	Generic.Ransom.GameChecker.6E502...
CAT-QuickHeal	Trojan.Tiggre	Comodo	UnclassifiedMalware
CrowdStrike Falcon	malicious_confidence_70% (W)	Cybereason	malicious.e1f362
Cyren	W32/Trojan.UGKQ-4151	Emsisoft	Generic.Ransom.GameChecker.6E502... (B)
eScan	Generic.Ransom.GameChecker.6E502...	ESET-NOD32	a variant of Generik.FIMHNM
F-Secure	Generic.Ransom.GameChecker.6E502...	Fortinet	PossibleThreat
GData	Win32.Trojan-Ransom.Filecoder.P@gen	Ikarus	Trojan.SuspectCRC
K7AntiVirus	Trojan (0052fb651)	K7GW	Trojan (0052fb651)
MAX	malware (ai score=96)	McAfee	RDN/Ransom-MC
McAfee-GW-Edition	RDN/Ransom-MC	Microsoft	Trojan:Win32/Occamy.B
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.Ransom.935
Rising	Malware.Undefined!8.C (TFE:C:zW4xjPNluhM)	Sophos AV	Troj/Ransom-EYC
Sophos ML	heuristic	Symantec	Trojan Horse
Tencent	Win32.Trojan.Generic.Szbo	TrendMicro	TROJ_GEN.R011C0ODL18
TrendMicro-HouseCall	TROJ_GEN.R011C0ODL18	VIPRE	Trojan.Win32.Generic!BT
Yandex	Trojan.Agent!zhmMLNH0rs8	Antiy-AVL	Clean