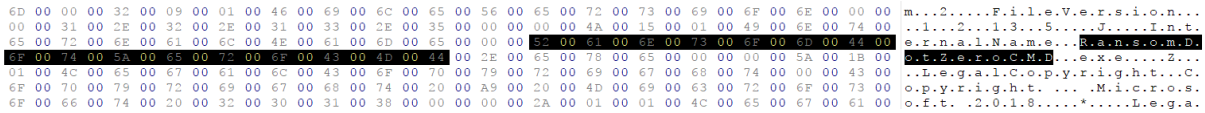
باسمه تعالی

تحلیل فنی باج افزار

DotZeroCMD.Ransom - v۱.۲ - RaaS

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت باج‌افزار - DotZeroCMD.Ransom - RaaS v۱.۲ خبر می‌دهد. این باج‌افزار برای نخستین بار در نیمه دوم ماه آوریل سال ۲۰۱۸ میلادی مشاهده گردید. براساس بررسی های صورت گرفته، باج‌افزار DotZeroCMD.Ransom یک Scareware است که جهت ترساندن کاربران به کار گرفته شده و به نظر می رسد که توسعه دهندگان آن قصد دارند با بروزرسانی این باج افزار در آینده حملات قابل ملاحظه‌ای انجام دهند. نکته جالب توجه در خصوص این باج افزار این است که پیغام باج‌خواهی آن دارای صفحه ای زرد رنگ مشابه با باج‌افزار GoldenEye (Petya-۳) می‌باشد.



مشخصات فایل اجرایی :

نام فایل	RansomDotZeroCMD.exe
MD۵	cc۹۸۹b۸٤cc٤b٥٦۸۸۹۳۱e۲۰cc٤a٥۱٥۸۸۷
SHA-۱	۲٥fe۷ffe۹۰۰f۸٤bc٦۷bb۹۰b۹ada٤۰٤۰a۳٥df۰٥f۲
SHA-۲٥٦	۹٤٦f۲c۱۹bdf٥edd٤۸bedf٥۰۷d٤٤٤٦٦da٦۷۸a۷b۲a٤٤cf۸٤۸e٤c۳٥d۹۲a۲۷۳۸f۱٦e
اندازه فایل	۱۱۲.٥ KB
کامپایلر	Microsoft visual C# vx.xDLL(managed)

فایل اجرایی این باج‌افزار دارای دو بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۳.۹۹	۸۱۹۲	۱۳۰٦٤	۱۳۳۱۲
.rsrc	۲٤٥۷٦	۲٤٥۷٦	۱۰۱۱۰۸	۱۰۱۳۷٦

تحلیل پویا :

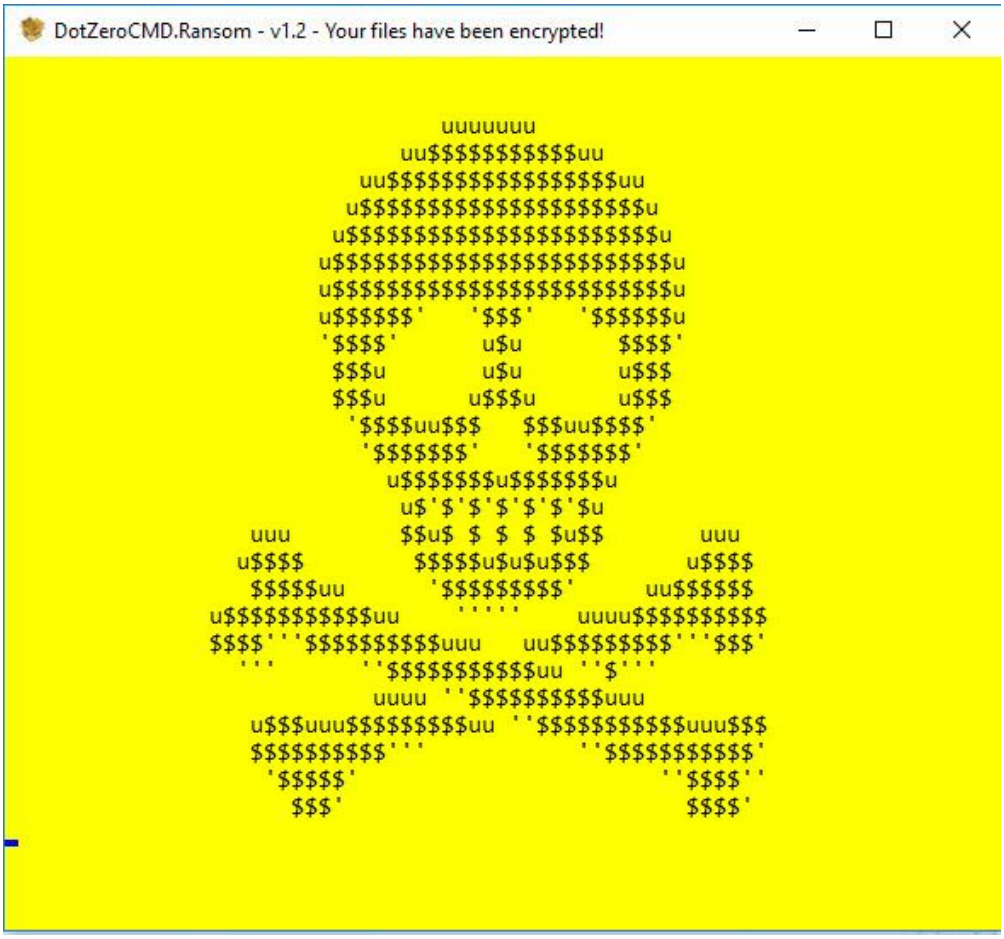
برای بررسی عمیق‌تر باج‌افزار DotZeroCMD.Ransom ، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم.

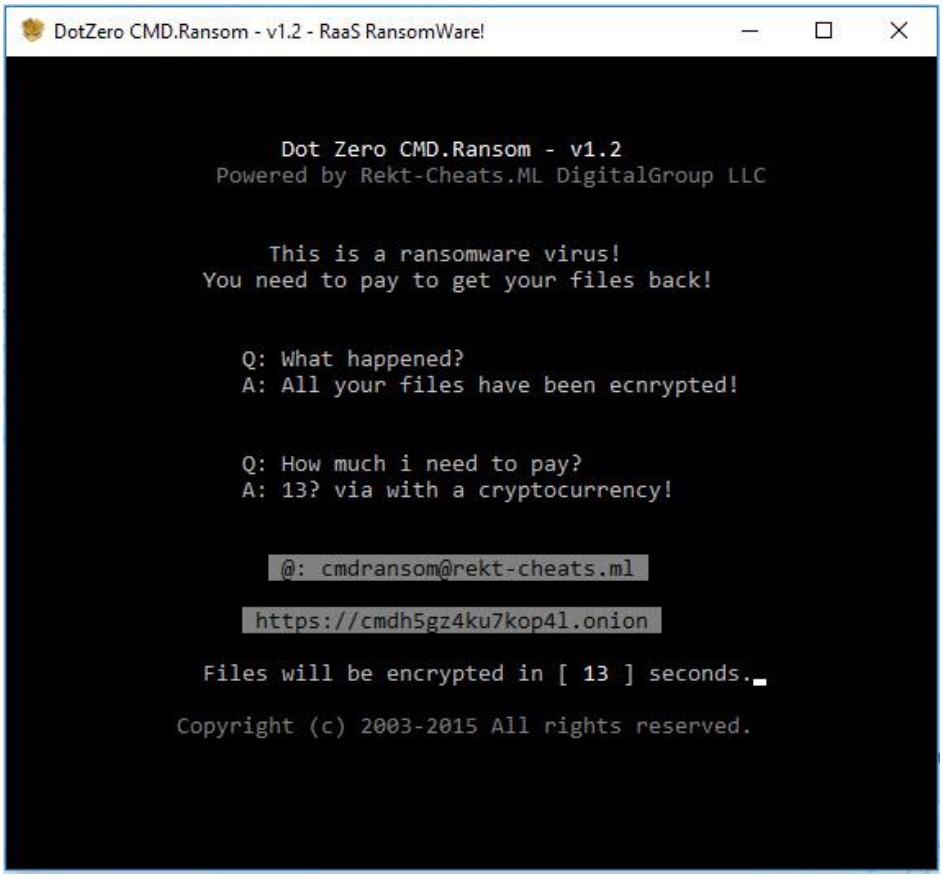
آیکن فایل اجرایی باج‌افزار DotZeroCMD.Ransom به صورت زیر می‌باشد :

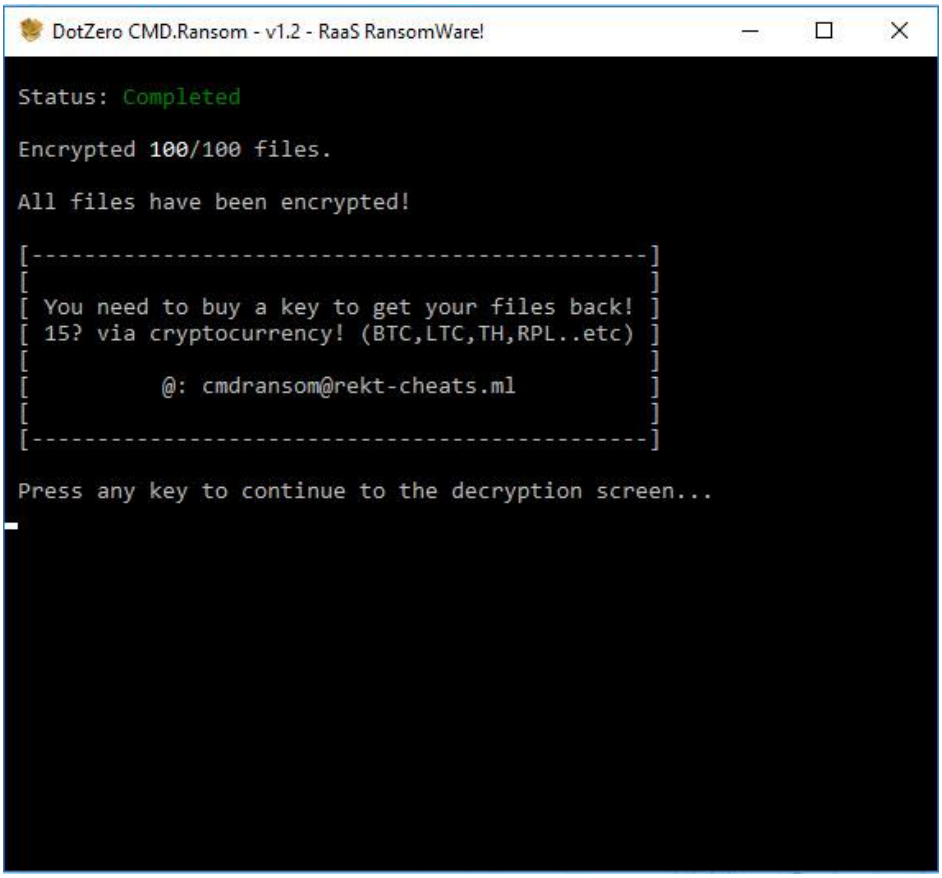
نتایج حاصل از این بررسی نشان داد تنها کاری که باج افزار انجام می‌دهد نمایش پیغام باج‌خواهی تحت عنوان زیر برای قربانی می باشد.

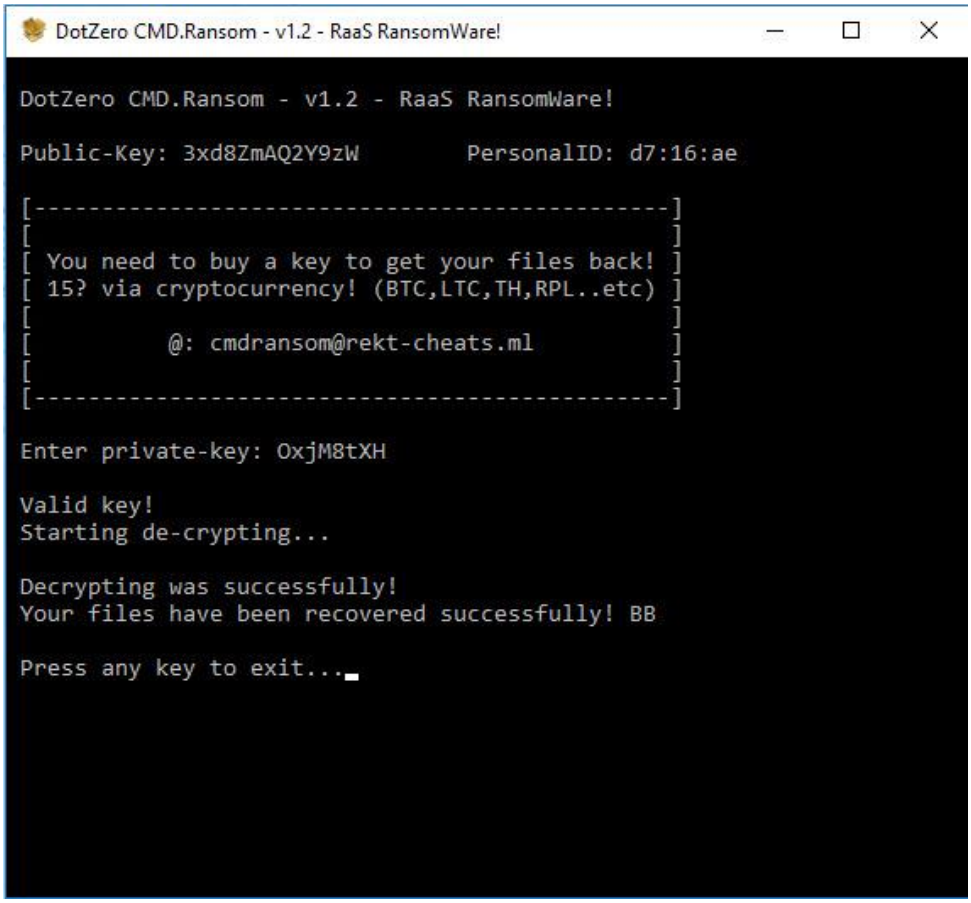
DotZeroCMD.Ransom - v۱.۲ - your files have been encrypted!

پس از اجرای باج افزار، تصاویر زیر به ترتیب برای قربانی به نمایش در می آیند.


DotZeroCMD.Ransom - v1.2 - Your files have been encrypted!


DotZero CMD.Ransom - v1.2 - RaaS RansomWare!
Dot Zero CMD.Ransom - v1.2
Powered by Rekt-Cheats.ML DigitalGroup LLC
This is a ransomware virus!
You need to pay to get your files back!
Q: What happened?
A: All your files have been ecnrypted!
Q: How much i need to pay?
A: 13? via with a cryptocurrency!
@: cmdransom@rekt-cheats.ml
https://cmdh5gz4ku7kop4l.onion
Files will be encrypted in [13] seconds.
Copyright (c) 2003-2015 All rights reserved.


DotZero CMD.Ransom - v1.2 - RaaS RansomWare!
Status: Completed
Encrypted 100/100 files.
All files have been encrypted!
[--]
[You need to buy a key to get your files back!]
[15? via cryptocurrency! (BTC,LTC,TH,RPL..etc)]
[@: cmdransom@rekt-cheats.ml]
[--]
Press any key to continue to the decryption screen...


DotZero CMD.Ransom - v1.2 - RaaS RansomWare!
DotZero CMD.Ransom - v1.2 - RaaS RansomWare!
Public-Key: 3xd8ZmAQ2Y9zW PersonalID: d7:16:ae
[--]
[You need to buy a key to get your files back!]
[15? via cryptocurrency! (BTC,LTC,TH,RPL..etc)]
[@: cmdransom@rekt-cheats.ml]
[--]
Enter private-key: OxjM8tXH
Valid key!
Starting de-crypting...
Decrypting was successfully!
Your files have been recovered successfully! BB
Press any key to exit...

در این پیغام به این مطلب اشاره شده است که تمامی فایل‌ها پس از گذشت ۱۲ ثانیه رمزگذاری خواهند شد. در صورتی که پس از گذشت این زمان هیچ تغییری بر روی فایل‌ها صورت نمی‌گیرد.

با وجود اینکه هیچ رمزگذاری صورت نگرفته، اما سازنده از قربانی می خواهد پس از ارسال مبلغ ۱۳ یورو در واحد پول Bitcoin ،Ethereum و... به ایمیل cmdransom@rekt-cheats.ml کلید خصوصی را دریافت کند.

تحلیل ایستا:

با بررسی بیشتر کدهای باج‌افزار به نتایج زیر دست یافتیم.

قطعه کد مربوط به پیغام باج‌خواهی باج افزار را در تصاویر زیر مشاهده می کنید.

```
Console.Clear();
Console.BackgroundColor = ConsoleColor.Black;
Console.ForegroundColor = ConsoleColor.Gray;
Console.BackgroundColor = ConsoleColor.Yellow;
Console.ForegroundColor = ConsoleColor.Black;
Console.Clear();
Console.WriteLine("\n");
Console.WriteLine("                                uuuuuuu");
Console.WriteLine("                            uu$$$$$$$$$$uu");
Console.WriteLine("                         uu$$$$$$$$$$$$$$$$uu");
Console.WriteLine("                        u$$$$$$$$$$$$$$$$$$$$u");
Console.WriteLine("                       u$$$$$$$$$$$$$$$$$$$$$$u");
Console.WriteLine("                      u$$$$$$$$$$$$$$$$$$$$$$$$u");
Console.WriteLine("                      u$$$$$$$$$$$$$$$$$$$$$$$$u");
Console.WriteLine("                      u$$$$$$'   '$$$'   '$$$$$$u");
Console.WriteLine("                       '$$$$'      u$u       $$$$'");
Console.WriteLine("                        $$$u       u$u       u$$$");
Console.WriteLine("                        $$$u      u$$$u      u$$$");
Console.WriteLine("                         '$$$$uu$$$   $$$uu$$$$'");
Console.WriteLine("                          '$$$$$$$'   '$$$$$$$'");
Console.WriteLine("                            u$$$$$$$u$$$$$$$u");
Console.WriteLine("                             u$'$'$'$'$'$'$u");
Console.WriteLine("                  uuu        $$u$ $ $ $ $u$$       uuu");
Console.WriteLine("                 u$$$$        $$$$$u$u$u$$$       u$$$$");
Console.WriteLine("                  $$$$$uu      '$$$$$$$$$'     uu$$$$$$");
Console.WriteLine("                u$$$$$$$$$$uu     ''''     uuuu$$$$$$$$$");
Console.WriteLine("                $$$$'''$$$$$$$$$$uuu   uu$$$$$$$$$'''$$$'");
Console.WriteLine("                 '''       ''$$$$$$$$$$uu ''$'''");
Console.WriteLine("                           uuuu ''$$$$$$$$$uuu");
Console.WriteLine("                  u$$$uuu$$$$$$$$$uu ''$$$$$$$$$$uuu$$$");
Console.WriteLine("                  $$$$$$$$$'''           ''$$$$$$$$$$'");
Console.WriteLine("                   '$$$$$'                    ''$$$$''");
Console.WriteLine("                     $$$'                       $$$$'");
Thread.Sleep(95);
Console.Clear();
Console.ForegroundColor = ConsoleColor.Yellow;
```

```
Console.WriteLine("Powered by Rekt-Cheats.ML DigitalGroup LLC");
Console.BackgroundColor = ConsoleColor.Black;
Console.ForegroundColor = ConsoleColor.Gray;
Console.SetCursorPosition(20, 7);
Console.WriteLine("This is a ransomware virus!");
Console.SetCursorPosition(15, 8);
Console.WriteLine("You need to pay to get your files back!");
Console.SetCursorPosition(18, 11);
Console.WriteLine("Q: What happened?");
Console.SetCursorPosition(18, 12);
Console.WriteLine("A: All your files have been ecnrypted!");
Console.SetCursorPosition(18, 15);
Console.WriteLine("Q: How much i need to pay?");
Console.SetCursorPosition(18, 16);
Console.WriteLine("A: 13€ via with a cryptocurrency!");
Console.SetCursorPosition(20, 19);
Console.BackgroundColor = ConsoleColor.DarkGray;
Console.ForegroundColor = ConsoleColor.Black;
Console.WriteLine(" @: cmdransom@rekt-cheats.ml ");
Console.SetCursorPosition(18, 21);
Console.BackgroundColor = ConsoleColor.DarkGray;
Console.ForegroundColor = ConsoleColor.Black;
Console.WriteLine(" https://cmdh5gz4ku7kop4l.onion ");
Console.SetCursorPosition(15, 23);
Console.BackgroundColor = ConsoleColor.Black;
Console.ForegroundColor = ConsoleColor.Gray;
Console.Write("Files will be encrypted in [ ");
Console.ForegroundColor = ConsoleColor.White;
Console.Write("{0} ", 13);
Console.ForegroundColor = ConsoleColor.Gray;
Console.Write("] seconds.");
Console.SetCursorPosition(13, 25);
Console.ForegroundColor = ConsoleColor.DarkGray;
Console.WriteLine("Copyright (c) 2003-2015 All rights reserved.");
```

همانطور که گفته شد این باج‌افزار از الگوریتم رمزگذاری استفاده نمی‌کند و تنها مقادیری را جهت شبیه‌سازی فرایند رمزگذاری چاپ می‌کند. که در تصویر زیر قابل مشاهده است.

```
for (int i = 1; i <= 100; i++)
{
    Thread.Sleep(100);
    Console.SetCursorPosition(1, 3);
    Console.BackgroundColor = ConsoleColor.Black;
    Console.ForegroundColor = ConsoleColor.Gray;
    Console.Write("Encrypted ");
    Console.ForegroundColor = ConsoleColor.White;
    Console.Write("{0}", i);
    Console.ForegroundColor = ConsoleColor.Gray;
    Console.Write("/100 files.");
    bool flag3 = i == 100;
    if (flag3)
    {
        Console.SetCursorPosition(1, 5);
        Console.Write("All files have been encrypted!");
    }
}
a = "comp";
bool flag4 = a == "enc";
if (flag4)
{
    Console.ForegroundColor = ConsoleColor.DarkRed;
    Console.SetCursorPosition(9, 1);
    Console.Write("Encrypting ");
}
else
{
    bool flag5 = a == "comp";
    if (flag5)
    {
        Console.ForegroundColor = ConsoleColor.DarkGreen;
        Console.SetCursorPosition(9, 1);
        Console.Write("Completed ");
    }
}
```

بررسی ها نشان می دهد که تابع رمزگشایی این باج‌افزار حاوی کلید خصوصی می‌باشد که پس از وارد کردن آن پیغام موفقیت‌آمیز بودن عملیات رمزگشایی نمایش داده می‌شود!

```
public static void Decrypt()
{
    string b = "3xd8ZmAQ2Y9zW";
    string b2 = "OxjM8tXH";
    int num = 13;
    int num2 = num - 1;
    Console.Clear();
    Console.BackgroundColor = ConsoleColor.Black;
    Console.ForegroundColor = ConsoleColor.Gray;
    Console.WriteLine("\n DotZero CMD.Ransom - v1.2 - RaaS RansomWare!");
    Console.WriteLine(" ");
    Console.WriteLine(" Public-Key: 3xd8ZmAQ2Y9zW \t  PersonalID: d7:16:ae \n");
    Console.WriteLine(" [-----------------------------------------------]");
    Console.WriteLine(" [                                               ]");
    Console.WriteLine(" [ You need to buy a key to get your files back! ]");
    Console.WriteLine(" [ 15€ via cryptocurrency! (BTC,LTC,TH,RPL..etc) ]");
    Console.WriteLine(" [                                               ]");
    Console.WriteLine(" [          @: cmdransom@rekt-cheats.ml          ]");
    Console.WriteLine(" [                                               ]");
    Console.WriteLine(" [-----------------------------------------------]");
    Console.Write("\n Enter private-key: ");
    string a = Console.ReadLine();
```

```
    bool flag = a == b2;
    if (flag)
    {
        Thread.Sleep(3100);
        Console.WriteLine("\n Valid key! \n Starting de-crypting...");
        Thread.Sleep(1500);
        Console.WriteLine("\n Decrypting was successfully! \n Your files have been recovered
          successfully! BB");
        Console.Write("\n Press any key to exit...");
        Console.ReadKey();
        Environment.Exit(0);
    }
    else
    {
        bool flag2 = a == b;
        if (flag2)
        {
            Console.WriteLine(" Invalid key! This is the public key -,-' \t {0} tries
              left!", num2);
            Console.ReadKey();
            Console.Clear();
            Program.Decrypt();
        }
        else
        {
            Thread.Sleep(2100);
            Console.WriteLine(" Invalid key! \t {0} tries left!", num2);
            Console.ReadKey();
            Console.Clear();
            Program.Decrypt();
        }
    }
while (a != b2);
```

باج افزار DotZeroCMD خود را باج افزار به عنوان یک سرویس (RaaS) معرفی می کند. آدرس موجود در پیغام باج خواهی نیز گویای این مطلب می باشد. اما بررسی ها نشان می دهد آدرس اشاره شده در حال حاضر خارج از سرویس بوده و در دسترس نمی باشد.

[https://cmdh٥gz٤kuvkop٤l.onion]

```
[assembly: AssemblyTitle("Ransom DotZero CMD Ransom")]
[assembly: AssemblyDescription("RaaS RansomWare")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("Rekt-Cheats.ML DigitalGroup LLC")]
[assembly: AssemblyProduct("Ransom DotZero CMD.Ransom")]
[assembly: AssemblyCopyright("Copyright © Microsoft 2018")]
```

تغییرات رجیستری:

کلید رجیستری زیر که مربوط به نمایش پیغام باج‌خواهی می‌باشد توسط باج‌افزار در سیستم عامل باز می‌شود:

HKU\S-۱-۵-۲۱-٤١٦٣٥٦٠٣١٩-١٦٥١٥٥٠٦٧٥-٣٥٢٦٨٢٢٤٩٠-
١٠٠٠\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\١\ApplicationVie
wManagement\W٣٢:٠٠٠٠٠٠٠٠٠١٢٠٢٧٨

تحلیل ترافیک شبکه :

پس از بررسی و انجام آزمایشات مختلف بر روی این باج‌افزار، هیچ‌گونه ترافیک http و یا درخواست DNS توسط باج‌افزار DotZeroCMD.Ransom مشاهده نگردید.

شناسایی :

در حال حاضر تعداد ٢٦ مورد از ٦٧ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

20180425	Trojan.Joke.PXH	Ad-Aware
20180425	Hoax.Win64.Gen!c	AegisLab
20180425	Trojan.Ransom.DotZeroCMD	ALYac
20180425	Trojan.Joke.PXH	Arcabit
20180425	Win64:Malware-gen	Avast
20180425	Win64:Malware-gen	AVG
20180425	JOKE/RedCap.mrsrx	Avira (no cloud)
20180425	Trojan.Joke.PXH	BitDefender
20180425	W64/Joke.MTMQ-0315	Cyren
20180425	Joke.Runsom.1	DrWeb
20180425	Trojan.Joke.PXH (B)	Emsisoft
20180425	Trojan.Joke.PXH	F-Secure
20180425	Riskware!FakeRansom.A!tr	Fortinet
20180425	Trojan.Joke.PXH	GData
20180425	Trojan-Ransom.DotZero	Ikarus
20180121	heuristic	Sophos ML
20180425	Hoax.Win64.FakeRansom.a	Kaspersky
20180425	Artemis!CC989B84CC4B	McAfee
20180425	Artemis!Trojan	McAfee-GW-Edition
20180425	Trojan.Joke.PXH	eScan
20180425	Trj/CI.A	Panda
20180425	Troj/DotZero-A	Sophos AV
20180425	Trojan.Cridex	Symantec
20180425	Ransom_DOTZERO.THDBCAH	TrendMicro
20180425	Ransom_DOTZERO.THDBCAH	TrendMicro-HouseCall
20180425	Hoax.Win64.FakeRansom.a	ZoneAlarm by Check Point