# RYUK RANSOMWARE TEKNİK ANALİZİ

# İÇİNDEKİLER

# Giriş

Ryuk , ilk fidye yazılım ailelerinden biridir. Ryuk fidye yazılımı ilk olarak Ağustos 2018'de ortaya çıkmıştır. Ryuk zararlı yazılımı, hedefli saldırılarda kullanılmaktadır. Önemli ölçüde dosyaları şifrelemektedir. Diğer birçok kötü niyetli bilgisayar korsanlarının aksine, Ryuk kötü amaçlı yazılımı şifreleme yoluyla işe yaramaz hale getirdiği verileri serbest bırakmak için öncelikle fidye ödemesi istediği görülmektedir. Ryuk bir sistemin kontrolünü ele geçirdiğinde, saklanan verileri şifreler ve kurban tarafından izlenemez. Bitcoin olarak bir fidye ödenmediği sürece kullanıcıların verilerine erişmesine izin verilmemiştir. Çoğu zaman maksimum zararı verebilmek için büyük şifreleme gerçekleşmeden önce sisteme temel olarak eriştikten sonra günler içerisinde sisteme daha da fazla nüfuz etmektedir.Ryuk, ağ sürücülerini ve kaynaklarını da bulup şifrelediği için oldukça önüne geçilmesi zor bir zararlı yazılımdır. Ayrıca, dosyaların şifrelenmemiş durumlarına geri yüklenmesine izin verecek olan Microsoft Windows'un Sistem Geri Yükleme özelliğini de devre dışı bırakılmaktadır.

Ryuk, önemli miktarda para ödeyebilen büyük kuruluşları hedeflemektedir. FBI'a göre, 2018-2019 yıllarında Ryuk kötü amaçlı yazılım saldırıları nedeniyle 61 milyon dolardan fazla fidye ödenmiştir. Saldırının ardından, Ryuk "kimlik avı kampanyaları yoluyla faaliyet gösteren en tehlikeli fidye yazılımı gruplarından biri" olarak tanımlanmaktadır. Ryuk, ağ sürücülerini ve kaynaklarını tanımlama ve şifrelemenin yanı sıra uç noktada gölge kopyaları silme özelliğini içeren ilk fidye yazılım ailelerinden biri olmuştur. Bu, saldırganların daha sonra kullanıcılar için Windows Sistem Geri Yükleme'yi devre dışı bırakabileceği ve böylece harici yedeklemeler veya geri alma teknolojisi olmadan bir saldırıdan kurtulmayı imkansız hale getirebileceği anlamına gelmektedir.

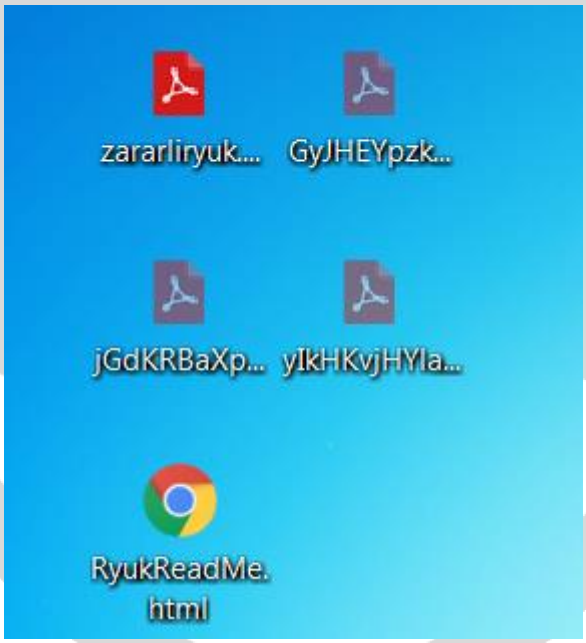
# Ön İzlenim

Bu sürümde klasik yayılımını sürdüren kötü amaçlı Ryuk'un bu sürümü posta kimlik avı yöntemi, ilk olarak 2021-03-17'de ortaya çıkmıştır. İnceleyeceğimiz kötü amaçlı dosyamızın adı '180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843.exe ' olarak bilinmektedir.

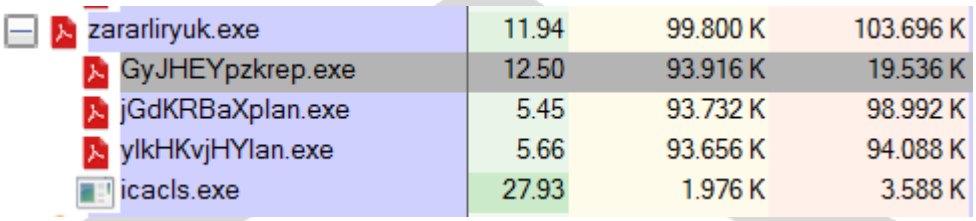
**Karbon Kopyaları**

Ryuk'un yürütme sırasında yaptığı ilk şey, masaüstüne veya kullanıcının dosyalarından birine yerleştirilen üç "gizli" dosyalarının oluşturulması olmaktadır. Ryuk, kötü amaçlı bir şifreleme yöntemi olarak RSA ve AES şifreleme yöntemlerini kullanmaktadırlar. Ryuk örneğinin yürütüldüğü yere bağlı olarak geçici dizinler oluşturmaktadır.

Ryuk, masaüstüne gizli dosyalar oluşturmaktadır.

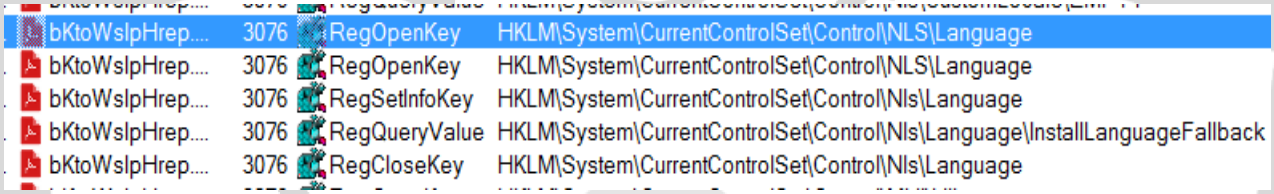


Ryuk, alt süreç (process) olarak çalıştırmaktadır.



| | | | |
|---|---|---|---|
| zararliryuk.exe | 11.94 | 99.800 K | 103.696 K |
| GyJHEYpzkrep.exe | 12.50 | 93.916 K | 19.536 K |
| jGdKRBaXplan.exe | 5.45 | 93.732 K | 98.992 K |
| ylkHKvjHYlan.exe | 5.66 | 93.656 K | 94.088 K |
| icacls.exe | 27.93 | 1.976 K | 3.588 K |

Ryuk zararlı yazılımı sistem dilini okumaktadır.



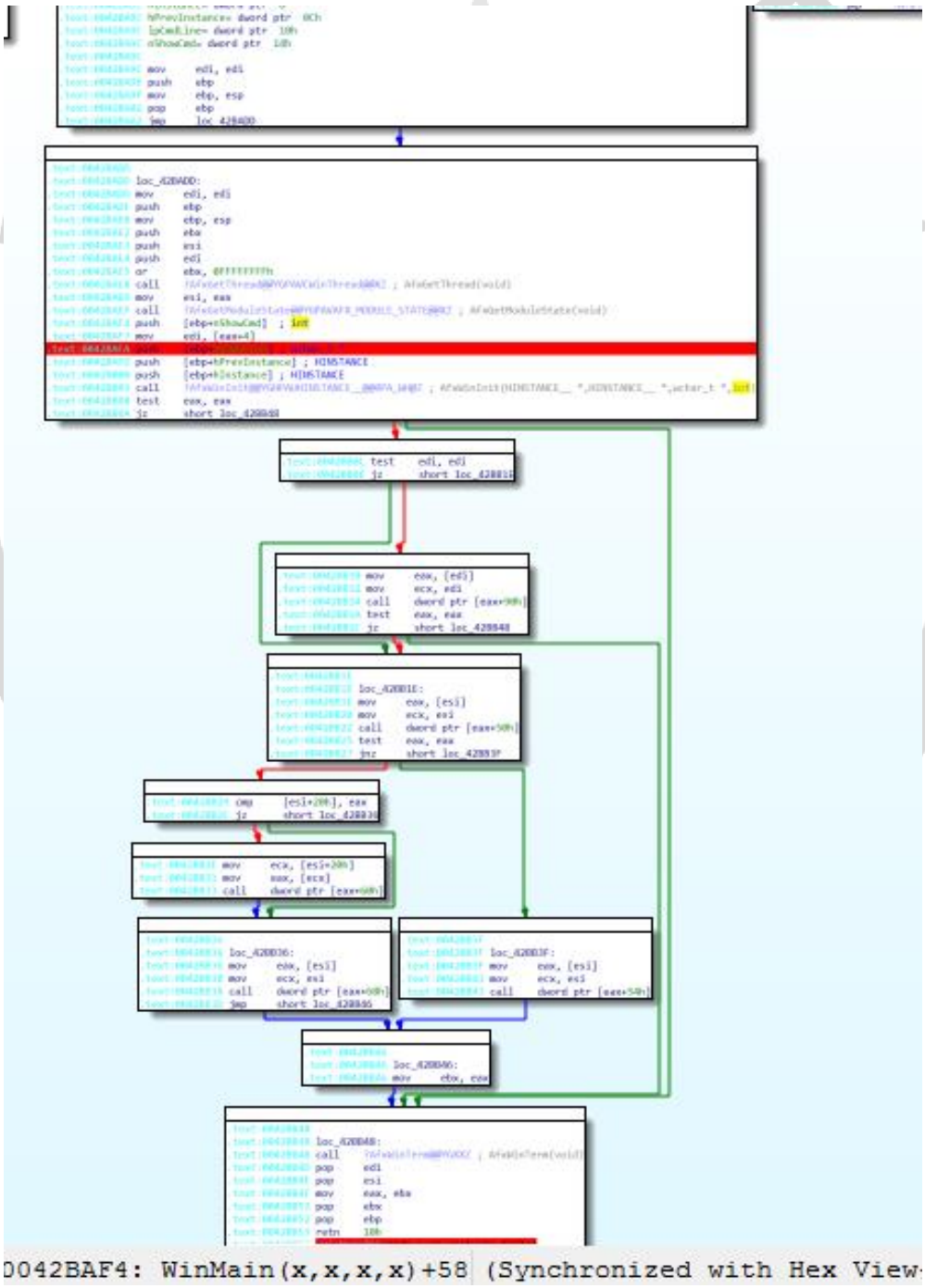
| | | | |
|---|---|---|---|
| bKtoWslpHrep.... | 3076 | RegOpenKey | HKLM\System\CurrentControlSet\Control\NLS\Language |
| bKtoWslpHrep.... | 3076 | RegOpenKey | HKLM\System\CurrentControlSet\Control\NLS\Language |
| bKtoWslpHrep.... | 3076 | RegSetInfoKey | HKLM\System\CurrentControlSet\Control\Nls\Language |
| bKtoWslpHrep.... | 3076 | RegQueryValue | HKLM\System\CurrentControlSet\Control\Nls\Language\InstallLanguageFallback |
| bKtoWslpHrep.... | 3076 | RegCloseKey | HKLM\System\CurrentControlSet\Control\Nls\Language |

```
31  v24 = a1;
32  v22 = a2;
33  lParam = 0;
34  Locale = 0;
35  hModule = GetModuleHandleA("kernel32.dll");
36  GetUserDefaultUILanguage = (LANGID (__stdcall *)())GetProcAddress(hModule, "GetUserDefaultUILanguage");
37  if ( GetUserDefaultUILanguage )
38  {
39    v3 = GetUserDefaultUILanguage();
40    lParam = v3;
41    Locale = v3 & 0x3FF;
42    v17 = ConvertDefaultLocale(Locale | (unsigned __int16)(v3 >> 10 << 10));
43    v18 = ConvertDefaultLocale(Locale);
44    Locale = 2;
45    GetSystemDefaultUILanguage = (LANGID (__stdcall *)())GetProcAddress(hModule, "GetSystemDefaultUILanguage");
46    if ( GetSystemDefaultUILanguage )
47    {
48      v5 = GetSystemDefaultUILanguage();
49      lParam = v5;
50      v6 = v5 & 0x3FF;
51      v19 = ConvertDefaultLocale(v6 | (unsigned __int16)(v5 >> 10 << 10));
52      v20 = ConvertDefaultLocale(v6);
53      Locale = 4;
54    }
00003DC2 ?AfxLoadLangResourceDLL@@YGPAUHINSTANCE__@@PBD0@Z:49 (4049C2)
```

# DOSYANIN ANALİZİ

| | |
|---|---|
| **DOSYA** | 180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843.exe |
| **MD5** | a563c50c5fa0fd541248acaf72cc4e7d |
| **SHA -1** | 602a43d4665ea83f3e1d0f1bc27ce83f515e6360 |

Anti-Debug yöntemi aşağıdaki fotoğrafta gösterildiği gibi AfxGetThread fonksiyonu ile başlamaktadır.



**Anti-Debug yönteminden sonra şifrelenmiş dizelerin çözümlenmiş hali aşağıdaki gibidir :**

- SCHTASKS /CREATE /NP /SC DAILY /TN \ “Print”
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
- SYSVOL
- C:\\Windows\\System32\\cmd.exe
- lsaas.exe
- \\Documents and Settings\\Default User\\sys
- taskkill
- boot
- RyukReadMe.html
- /C REG DELETE ”HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Ru n\” /v \”EV\” /f
- SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\
- cmd.exe /c \”bcdedit /set {default} recoveryenabled No & bcdedit /set {defalult}\”
- bin
- SUN
- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype)
- EnableUA
- sysrep
- HERMES
- encrypt
- cmd.exe /c \"wMIC.exe shadowcopy delete\
- SYSTEM\\CurrentControlSet\\Control\\Nls\\Language\\
- boot
- MON
- bind
- SYSVOL
- csrss.exe
- file
- socket

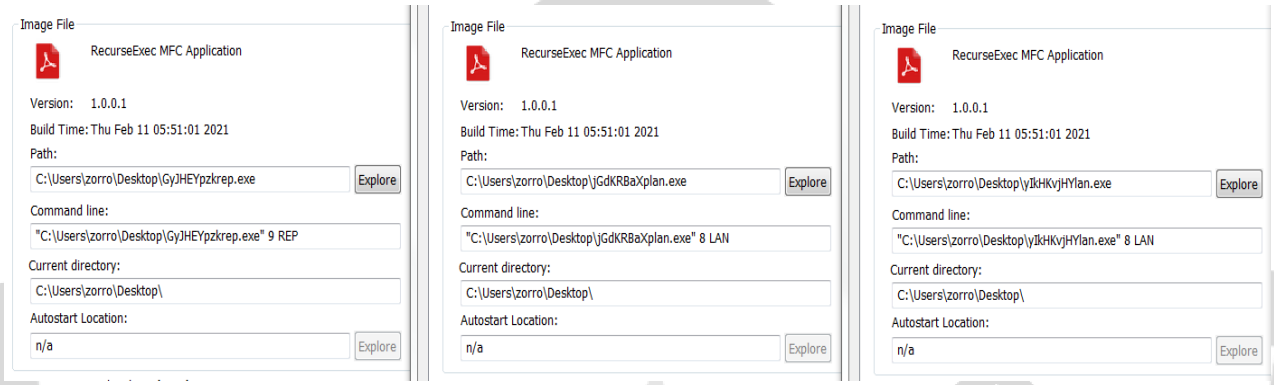
- Microsoft Base Cryptographic Provider v1.0
- RyukReadMe.html
- Mozilla
- netlogon
- inet_addr
- "\" /TR \"C:\\Windows\\System32\\cmd.exe /c for /l %x in (1,1,50) do start wordpad.exe /p
- cmd.exe /c \"bootstatuspolicy ignoreallfailures\
- NTDS
- "\" /grant Everyone:F /T /C /Q"
- WinExec
- "/C REG ADD \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows
- \\CurrentVersion\\Run\" /v \"EV\" /t REG_SZ /d \"
- "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\"
- " /sc once /st 00:00 /RL HIGHEST"
- InstallLanguage
- .RYK
- "cmd.exe /c \"vssadmin.exe Delete Shadows /all /quiet\"
- file
- \\\\192.168.59.132\\
- \\REGISTRY\\USER*\\SOFTWARE\\Classes
- Chrome
- cmd.exe /c \”vssadmin.exe Delete Shadows /all /quiet\”
- crss.exe

# ÇÖZÜMLENEN APİ ‘LAR

Ryuk kötü amaçlı işlemler  kullanılmak için şifreli olarak bulunan API’ ları çözümlemektedir. Çözümlenen API‘ lar aşağıdaki tabloda görülmektedir .

| | | |
|---|---|---|
| WSAStartup | socket | setsockopt |
| sendto | Closesocket | WSACleanup |
| INetNtopW | inet_ntop | GetTempPathW |
| CreateToolhelp32Snapshot | Process32FirstW | Process32NextW |
| VirtualFree | CryptExportKey | DeleteFileW |
| GetLastError | GetDriveTypeW | GetCommandLineW |
| GetStartupInfoW | FindNextFileW | VirtualAlloc |
| GetUserNameA | ExitProcess | Wow64RevertWow64FsRedirection |
| CreateProcessA | GetIpTable | GetVersionExW |
| Wow64DisableWow64FsRedirection | GetSystemDefaultLangID | GetUsernameW |
| ReadFile | RegQueryValueExW | RegCloseKey |
| CopyFileA | SetFileAttributesW | WinExec |
| CryptDeriveKey | CryptGenKey | Sleep |
| GetCurrentProcess | ShellExecuteW | GetFileSize |
| GlobalAlloc | FindClose | WaitForMultipleObjects |
| GetModuleFileNameA | ShellExecuteA | GetModuleHandleA |
| GetModuleFileNameW | CreateFileA | GetFileSizeEx |
| WriteFile | GetLogicalDrives | WNetEnumResourceA |
| WNetEnumResourceW | RegOpenKeyExW | WNetCloseEnum |
| GetWindowsDirectoryW | SetFileAttributesA | RegOpenKeyExA |
| SetFilePointer | GetTickCount | GetFileAttributesW |
| FindFirstFileW | CryptAcquireContextW | MoveFileExW |
| WNetOpenEnumA | WNetOpenEnumW | CoInitialize |
| CryptDecrypt | CryptImportKey | SetFilePointerEx |
| CopyFileW | FreeLibrary | CreateProcessW |
| CreateDirectoryW | CreateThread | CryptDestroyKey |
| CoCreateInstance | CreateFileW | GetFileAttributesA |
| CryptEncrypt | RegDeleteValueW | EnumServicesStatusW |
| GetTokenInformation | ImpersonateSelf | LookupPrivilegeValueW |
| OpenProcessToken | OpenSCManagerW | OpenThreadToken |
| AdjustTokenPrivileges | VirtualAllocEx | LookupAccountsidW |
| CommandLineToArgvW | WriteProcessMemory | VirtualFreeEx |
| CreateRemoteThread | GetAdaptersAddresses | IcmpCloseHandle |
| IcmpCreateFile | IcmpCreateFile | NTQueryInformationProcess |
| CloseServiceHandle | | |

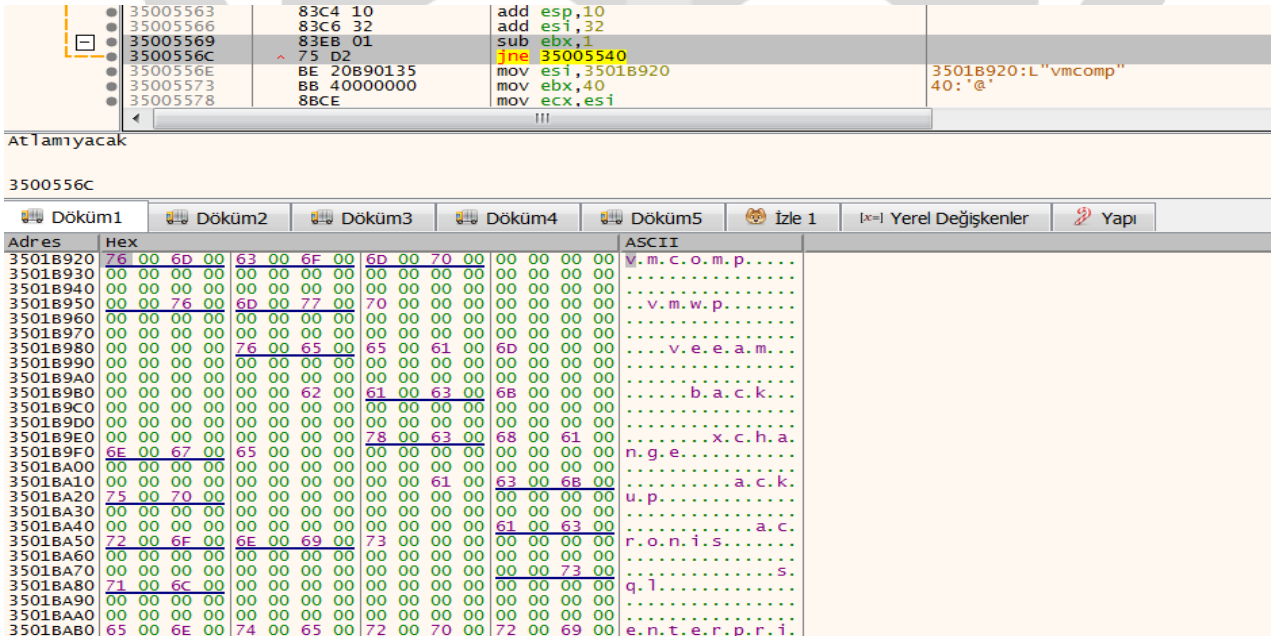
Dizelerin kod çözme işleminin ardından, zararlı yazılım "RyukReadme.html" dosyasını her dizine kopyalamaktadır.




İlk kopyası için mevcut dokuz rastgele harfin sonuna "9 REP" parametresi ile çalıştırır. Diğer kopyalanan yürütülebilir dosyanın adı ayrıca GetTickCount API kullanılarak, dokuz rastgele harflerin sonuna "lan.exe" dizesi eklenerek "8 LAN" parametresini çalıştırmaktadır.

Ryuk, kendisini kopyaladıktan sonra yeni dosyayı gizlemek için SetFileAttributesW API'sini kullanmaktadır. Masaüstüne yazılan dosyanın görünürlüğünü ayarladıktan sonra "8 LAN" parametresi ile çalıştırılır. Bu parametre alt süreçler yaratılmasını sağlamaktadır. Bu işlemi en az 3 defa tekrarladıktan sonra içerisinde "RyukReadMe.html" isimli bir dosya oluşturmaktadır.

Kötü amaçlı şifreleme işlemi sırasında sistemde çalışan işlemleri kontrol eder. **Kontrol edilen işlem adları aşağıda listelenmiştir :**



| | | | | |
|---|---|---|---|---|
| Vmcomp | Vmwp | Veeam | Backup | Xchange |
| Sql | Dbeng | Sofos | Calc | Ekrn |
| Zoolz | Encsvc | Excel | Firefoxconfig | İnfopath |
| Msaccess | Mspub | Mydesktop | Ocautopds | Ocomm |
| Ocssd | Onenote | Oracle | Outlook | Powerpnt |
| Sqbcoreservice | Steam | Tbirdconfig | Thebat | Thunderbird |
| Visio | Word | Xfssvccon | Tmlisten | PccNtMon |
| CNTAoSMgr | Ntrtscan | mbabtray | Synctime | |

## KOMUTLAR

Uses Windows utilities for basic functionality

**command**: "C:\Windows\System32\net.exe" stop "audioendpointbuilder" /y
**command**: net stop "audioendpointbuilder" /y
**command**: "C:\Windows\System32\net.exe" stop "samss" /y
**command**: net stop "samss" /y

**Komut sırası şu sırayla gerçekleşmektedir :**

- net.exe stop "audioendpointbuilder" /y

Bu komut, kurban sisteminde sesin arızalı olmasını sağlayan "ses uç noktası oluşturucu" Windows hizmetini durdurmaktadır.

- net.exe stop "samss" /y

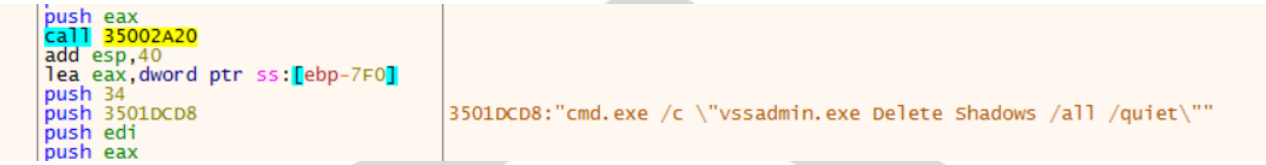
Güvenlik Hesapları Yöneticisi'ni durdurur. Bu teknik, güvenlik uyarılarının tetiklenmesini ve bir SIEM'e gönderilmesini önlemek için kullanılmaktadır.

- cmd.exe /c "WMIC.exe shadowcopy delete"

```
push eax
call 35002A20
push 27
push 3501D7D8                          3501D7D8:"cmd.exe /c \"WMIC.exe shadowcopy delete\""
lea eax,dword ptr ss:[ebp-7F0]
push edi
```

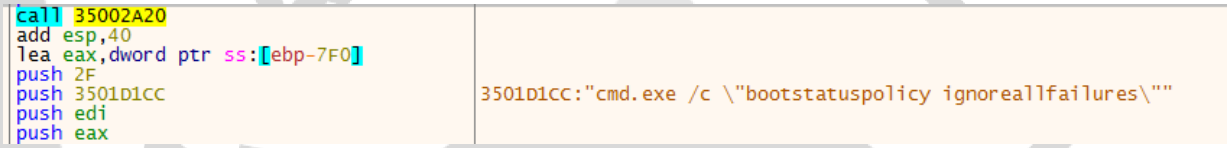
Bu komut, dosyaları kurtarmak için kullanılamayacakları Windows Birim Gölge Kopyası hizmetlerini temizlemektedir.

- cmd.exe /c "vssadmin.exe Delete Shadows /all /quiet"




Bu komut, dosyaların gölge kopyalarını kaldırmanın başka bir yöntemi olarak kullanmaktadır.

- cmd.exe /c "bcdedit /set {default} recoveryenabled No & bcdedit /set {default}"
- cmd.exe /c "bootstatuspolicy ignoreallfailures"




Bu komutlar, Windows error kurtarma ve ilişkili önyükleme seçeneklerini devre dışı bırakmak için kullanılır, bu nedenle sistemi kurtarmayı daha da zorlaştırmaktadır.

- icacls "C:" /grant Everyone:F /T /C /Q
- icacls "D:" /grant Everyone:F /T /C /Q
- icacls "Z: " /grant Everyone:F /T /C /Q

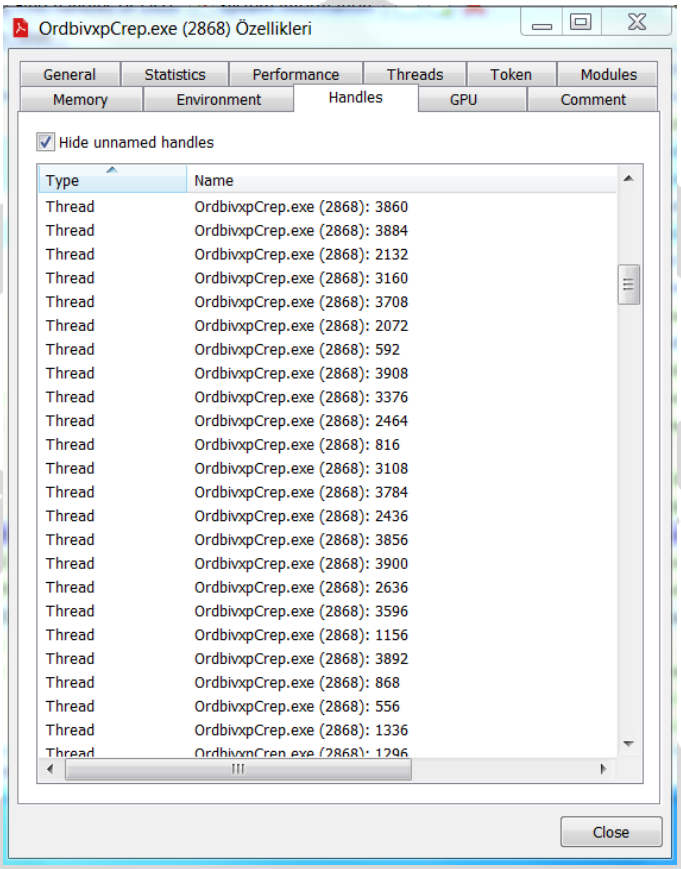
Bu komutlar, C, D ve Z sürücülerine Everyone grubu tam izinlerini atamaya çalışır. Bu, şifreleme işlemi başlamadan önce, Ryuk'un dosyaları değiştirme izinlerine sahip olduğundan emin olmak için kullanmaktadır.

- cmd.exe " /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "EV" /t REG_SZ /d "\"

Bu komut Kayıt Defteri kalıcılığı sağlamak için kullanılır. Temel olarak amacı Ryuk zararlısının bu örneğinde sistem önyüklemesi sırasında tekrar çalışmasını sağlayabilmektir. Ancak Ryuk dosyaları yalnızca bir kez şifrelenmektedir.

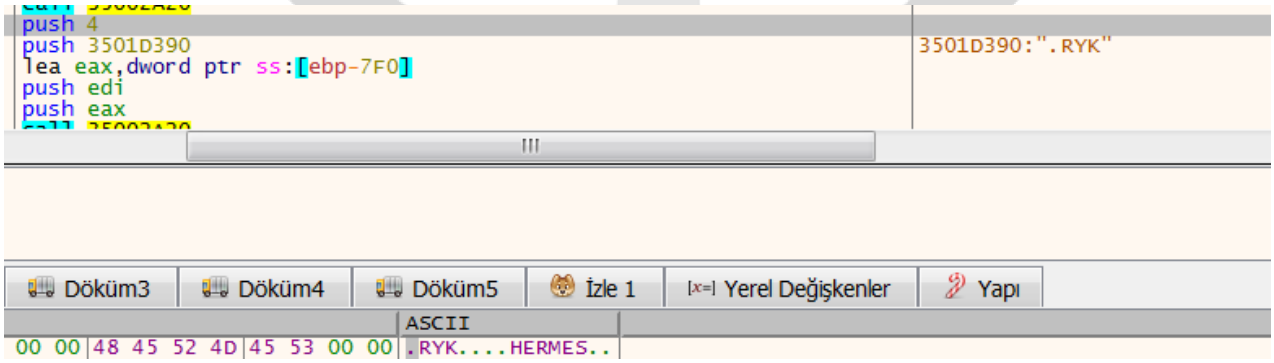
Yukarıdaki komut satırı komutları çalıştırıldıktan sonra dosya şifreleme işlemi çalıştırmaktadır. Daha önce de belirtildiği gibi, Ryuk dosya sistemini birden fazla iş parçacığı kullanarak şifrelemekte, Ryuk çalıştırabilir dosyası ve karbon kopyası alınan gizli çalıştırabilir dosyalar, Ryuk'un enjekte edebildiği işlemler arasında yayılmaktadır. Ryuk şifrelenen her dosya için yeni bir iş parçacığı oluşturmaktadır.

**Ryuk şifreleme iş parçacıkları :**



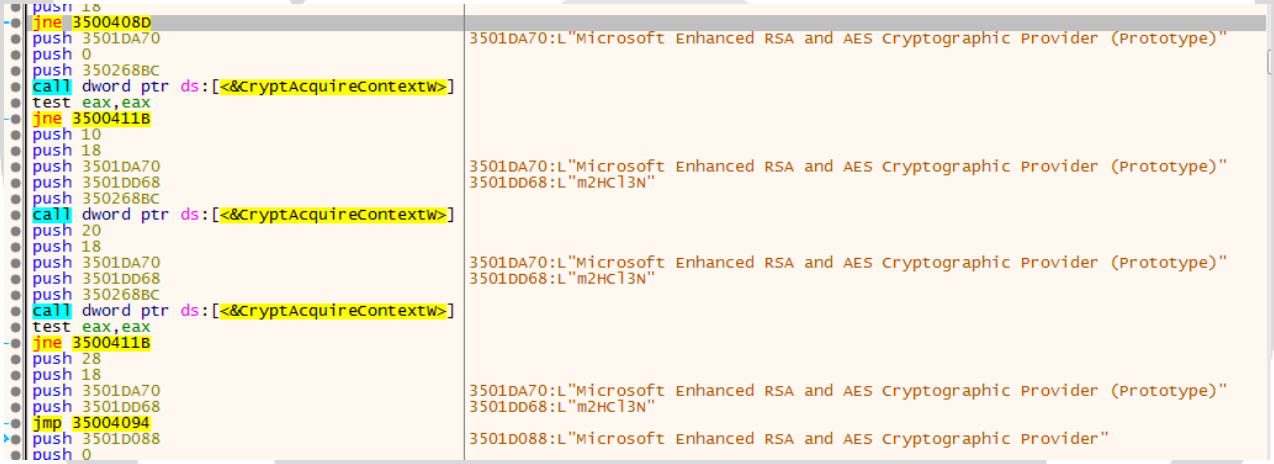

Ryuk, kurban sistemindeki dosyalar arasında yineleme yapmak için FindFirstFileW ve FindNextFileW işlevlerini kullanmaktadır. Bir dosya bulunduktan sonra, Ryuk yeni bir şifreleme iş parçacığı başlatmak için CreateThread'i çağırmaktadır. Ryuk'un kurban sistemindeki dosyaları ne kadar hızlı numaralandırması ve şifrelemesi dikkat çekmektedir. Ağa bağlı sürücülerdeki dosyalar da dahil olmak üzere 120 saniye içinde şifrelenmektedir.

Şifrelenmiş bazı dosyaların uzantısını ". RYK" yapmaktadır.



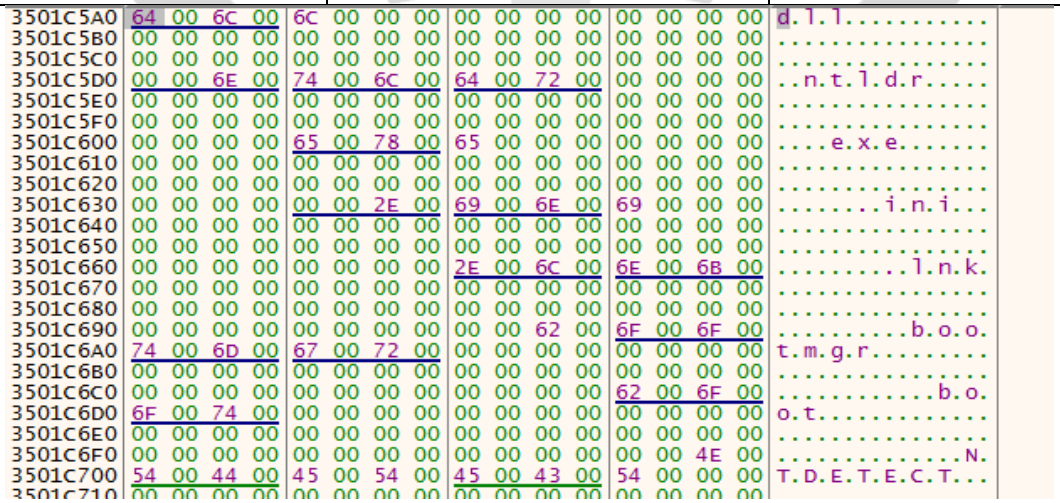
Bir dosyayı şifrelemeden önce kötü amaçlı yazılım, dosyanın zaten şifrelenmiş olup olmadığını kontrol etmektedir. Eğer eski şifrelenmemiş hali ise RYUKTM kelimesini aramaktadır veya şifrelenmiş haliyse HERMES kelimesini aramaktadır, bulduğunda şifrelemeyi durdurmaktadır.


Ryuk ransomware, "Microsoft Enhanced RSA ve AES Cryptographic" hizmetini kullanarak dizinleri şifrelemektedir.



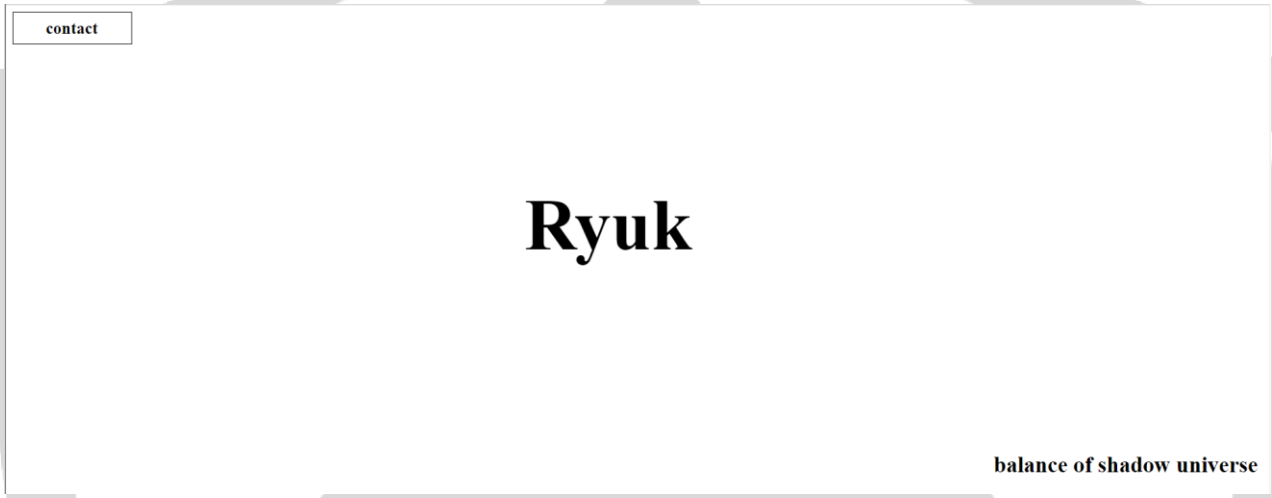

Kötü amaçlı yazılım ayrıca, dosya uzantısı aşağıdakilerden herhangi birini içeriyorsa dosyaları şifrelemez. **Bu uzantılar şunlardır:**

| | | |
|---|---|---|
| boot | dll | ntldr |
| exe | ini | lnk |
| bootmgr | NTDETECT | |

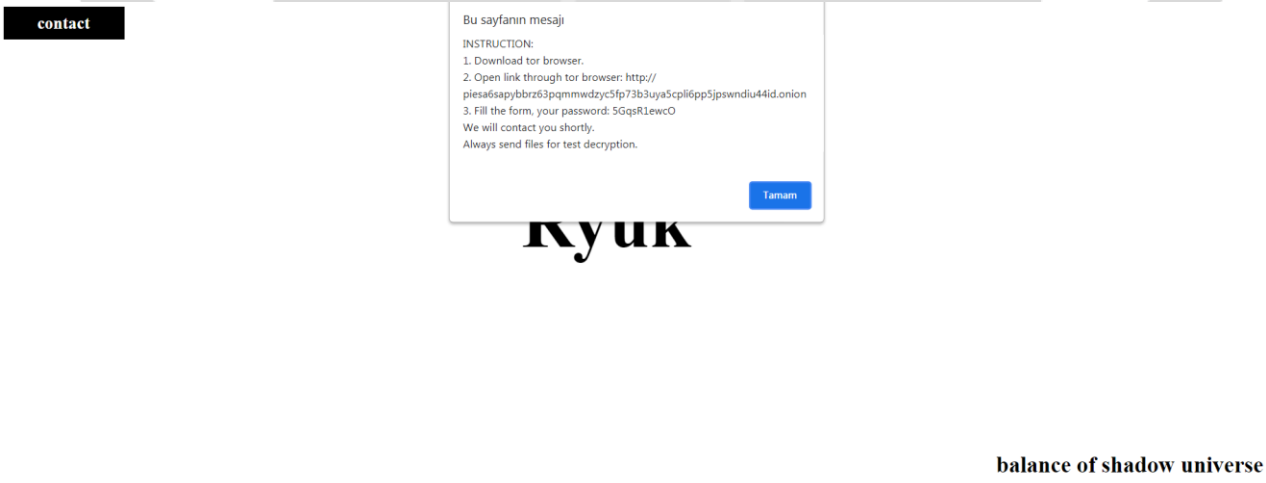


# BENİ OKU DOSYASI

Ryuk ayrıca şifreli dosyalar içeren her dizinde bir "beni oku" dosyası (RyukReadme.html) oluşturmaktadır. Bu benioku dosyası, kurbana fidyenin nasıl ödenecekleri hakkında daha fazla talimat uygulatabilmek için iletişim butonu bulunmaktadır.




İletişim butonuna tıklandığında Ryuk Ransomware notu karşımıza çıkmaktadır.



Tor Browser indirmemizi ve linke ulaşmamız istenmektedir. Linke ulaştığımızda karşımıza şu şekilde bir ekran gelmektedir:

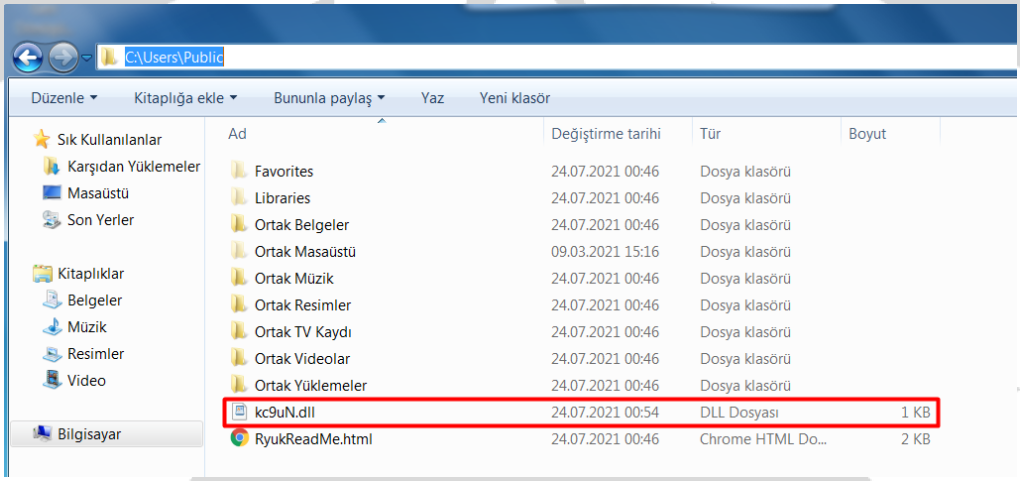

**balance of shadow universe**

Bu bölümden gönderdiğiniz iletişim içeriğine karşılık cevap dönerek sizden yüksek miktarlarda bitcoin üzerinden fidye istenmektedir.

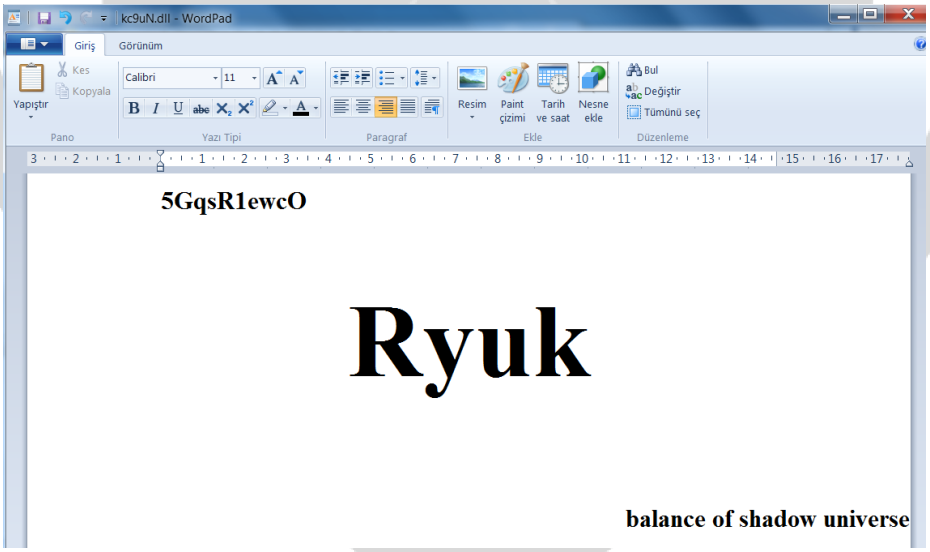
# YAZDIRMA İŞLEMİ

Dosyaların şifrelenmesinden sonra, ryuk kötü amaçlı yazılımı sistemde varsayılan fidye notunun 50 kopyasını yazdırmayı amaçlayan bir görev komutunu kullanmaktadır.

Genel dizine bırakılan “kc9uN.dll” ile bu komut çalıştırılmaktadır.



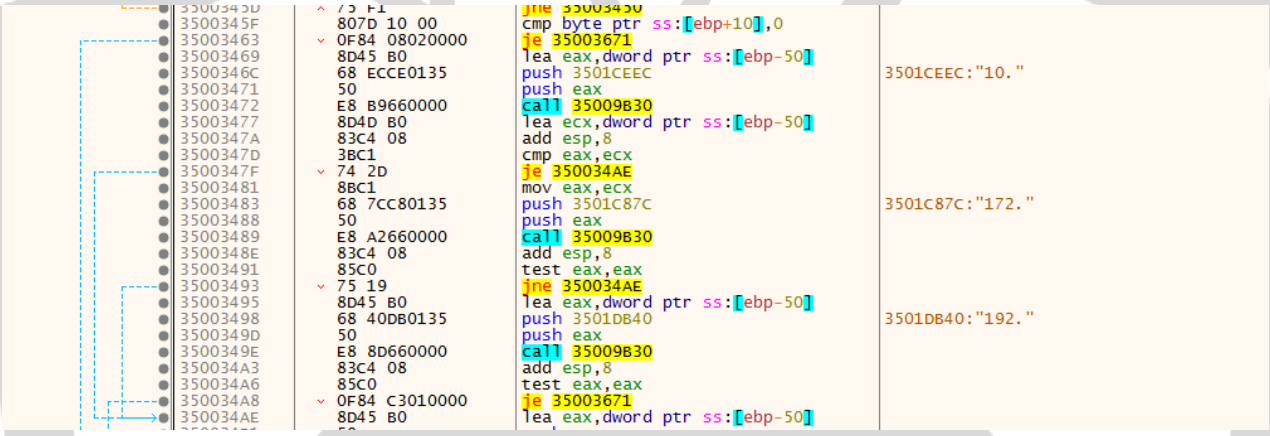

```
SCHTASKS /CREATE /NP /SC DAILY /TN “PrintvE” /TR
“C:\Windows\System32\cmd.exe /c for /l %x in (1,1,50) do start
wordpad.exe /p C:\users\Public\kc9uN.dll” /ST 10:25 /SD 05/18/2021
/ED 05/25/2021
```



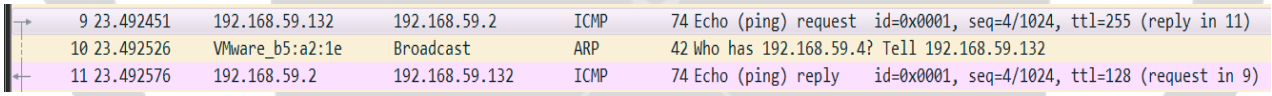

Haftanın belirli bir zamanında tanımlanan görev, fidye notunu 50 sayfaya yazdırmayı amaçlamaktadır. Aynı zamanda kötü amaçlı yazılıma eklenen yeni bir baskı sürecidir. Kurbanın sisteminde kaos yaratmayı ve onlara fidye bedelini ödemeleri için baskı yapmayı amaçlamaktadır.

# NETWORK ANALİZİ

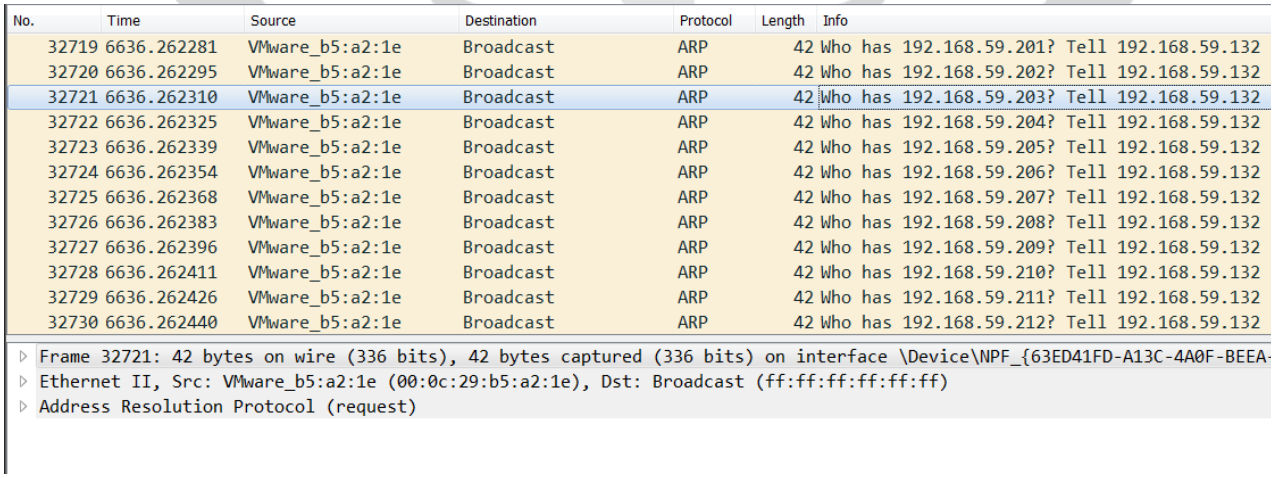
Ryuk, ağ bağdaştırıcısı IP adreslerini (GetAdapterAddresses apisini kullanarak) kurban sisteminden bilgisini alır ve onları harekete geçirmek için bu sistemlere WOL (WakeOn-LAN) paketleri göndermeye çalışır. Ryuk WOL paketlerini yalnızca 10, 172 veya 192 ile başlayan adreslere göndermektedir.




Ryuk ARP tablosunu kullarak (GetIpNetTable apisini kullanarak) ip adresini almaktadır ve açık olup olmadıklarını kontrol etmek için aldığı iplere istek atmaya çalışmaktadır.




Sonrasında Ryuk fidye yazılımı, yerel ağdaki bir ip yanıt verdiğinde, oraya yerleşmeyi ve çalışmayı amaçlamaktadır. O ip'deki ağ sürücülerine erişir ve şifrelemeye başlamaktadır.



# ÇÖZÜM ÖNERİLERİ

- Sistemlerde ve sunucularda güncel antivürüs programları kullanılması gerekmektedir.
- Gelen e-postalar dikkatli okunmalı, güvenmeden e-posta içerisindeki ekler açılmamalı veya cevap verilmemelidir.
- İnternette gezinirken phishing sitelerine dikkat edilmelidir.
- İşletim sistemi güncel tutulmalıdır.
- Şüphenilen bir durumda ağın izlenmesi ve duruma göre müdahale edilmesi gerekmektedir.

# MITRE ATT&CK TABLOSU

| Teknik ID | Teknik Açıklama | Gözlemlenen durum |
|---|---|---|
| T1059.003 | Windows Command Shell | Ryuk **cmd.exe** kullanarak yazma işlemi gerçekleştirmektedir. |
| T1083 | File and Directory Discovery | Ryuk sistemdeki dosyaları numaralandırabilmek için **FindFirstFileW** ve **FindNextFileW** API'sini kullanmaktadır. |
| T1222.001 | Windows File and Directory Permission Modification | Ryuk izinleri değiştirmek için **icacls "C:" /grant Everyone:F /T /C /Q** komutunu kullanmaktadır. |
| T1205 | Traffic Signaling | Ryuk **Wake-on-lan** methodunu kullanmaktadır. |
| T1016 | System Network Configuration Discovery | Ryuk **GetIpTable** apisini kullanarak arp tablosuna ulaşmaktadır. |
| T1057 | Process Discovery | Ryuk **CreateToolhelp32Snapshot** apisini kullanarak süreçlerin ilk kısmını başlatmaktadır. |
| T1053.005 | Scheduled Task | Ryuk fidye notunu **yazdırabilmek** için zamanlanmış görev oluşturmaktadır. |

# YARA KURALI

```
import "hash"
rule Ryuk_Ransomware
{
 meta:
 author = "ZAYOTEM - Emre Dogan"
 description = "Ryuk Ransomware Technical Analysis"
 strings:
 $str1 = "MON"
 $str2 = "RyukReadMe.html"
 $lan = "lan.exe"
 $enc = "encrypt"
 $dec = "decrypt"
 $task = "taskkill"
 $hermes = "HERMES"
 $ryk = ".RYK"
 $com1 = "cmd.exe /c \"bcdedit /set {default} recoveryenabled No & bcdedit /set
{default}\"" fullword ascii
 $com2 = "\" /TR \"C:\\Windows\\System32\\cmd.exe /c for /l %x in (1,1,50) do start
wordpad.exe /p " fullword ascii
 $com3 = "cmd.exe /c \"vssadmin.exe Delete Shadows /all /quiet\"" fullword ascii
 $com4 = "cmd.exe /c \"WMIC.exe shadowcopy delete\"" fullword ascii
 $com5 = "/grant Everyone:F /T /C /Q"
 $com6 = "Cmd.exe /c \"bootstatuspolicy ignoreallfailures\""
 $path = "\\Documents and Settings\\Default User\\sys"
 condition:
 hash.md5(0, filesize) == "a563c50c5fa0fd541248acaf72cc4e7d" or all of them

}
```

**HAZIRLAYAN**

# EMRE DOĞAN

**https://www.linkedin.com/in/emreefedogan/**