Taiwan Government Targeted by Multiple Cyberattacks in April 2020

medium.com/cycraft/taiwan-government-targeted-by-multiple-cyberattacks-in-april-2020-1980acde92b0

CyCraft Technology Corp January 31, 2022

CyCraft Technology Corp

Oct 8, 2020

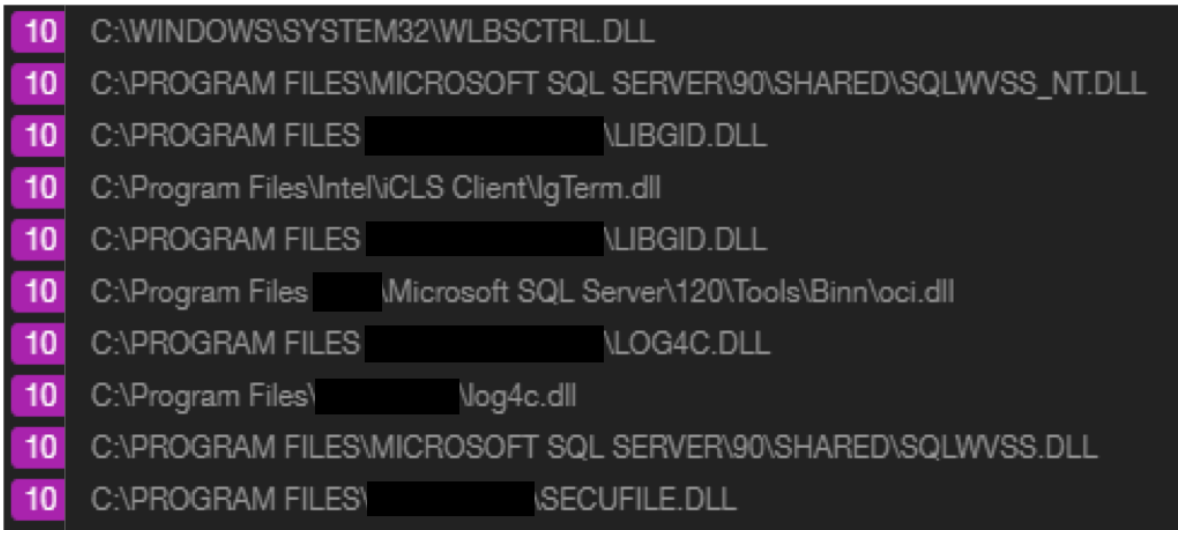
.

7 min read

Part 1: Waterbear Malware

In April 2020, highly malicious cyber activity was detected in several Taiwan government agencies. In one environment alone, out of the thousands of endpoints scanned, 30 endpoints were confirmed to be infected, and 10 high-risk endpoints were connected by these compromised endpoints. 10 key malware were discovered during these sophisticated targeted attacks — most of them were Waterbear Loader malware.

> This article is Part 1 of a series of articles. Click here to read Part 2: Owlproxy Malware.



CyCraft AIR assigns Threat Level 10 to the most severe and most damaging malware.

Highlighted Tactics

The attackers discovered and leveraged a weak point in trusted and commonly used data loss prevention (DLP) software in order to trigger malware and maintain persistence. The government agencies targeted for attack in April 2020 had already been compromised prior to the April attacks; however, CyCraft AIR (our automated detection and response platform) discovered that not all the malware from the previous attack was removed during another vendor's IR investigation, allowing the attackers to use the previously compromised endpoints yet again.

The discovered Waterbear Loader malware used several methods to evade defense. (Each method will be expanded upon later in the article.)

- DLL hijacking to stealthily trigger next stage malware
- Enlarging binary size to bypass scanning protocols
- Heaven's Gate to avoid antivirus detection
- Forcing DLLs to unload to obfuscate malware
- Padding memory with Kernel32 content to confuse analyses

Network Level Activity

The attackers first compromised a user's endpoint to harvest administrative credentials. The credentials were then utilized to RDP a web server. With the connectivity of the web server, the attackers "net use" through (proxying) the webserver, allowing them to distribute malware directly to other endpoints.

As mentioned before, several malware was not removed from a previous IR investigation. One endpoint in the victim's private network was still compromised. The attackers used this previously compromised endpoint in the victim's private network as the C2 server for this attack.

System Level Activity

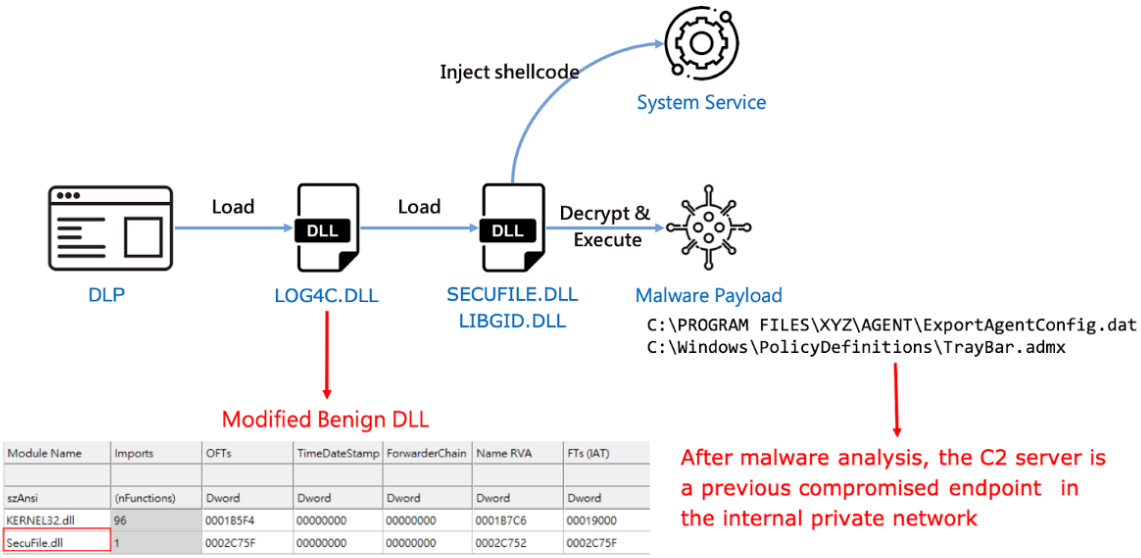
DLL Hijacking

One key feature of this attack was DLL Hijacking.

What is DLL Hijacking?

A DLL hijacking attack exploits the Windows search and load mechanism, allowing attackers to inject code into applications through disk manipulation. By simply injecting a DLL file in the right location, attackers can cause vulnerable applications to load malicious DLLs.

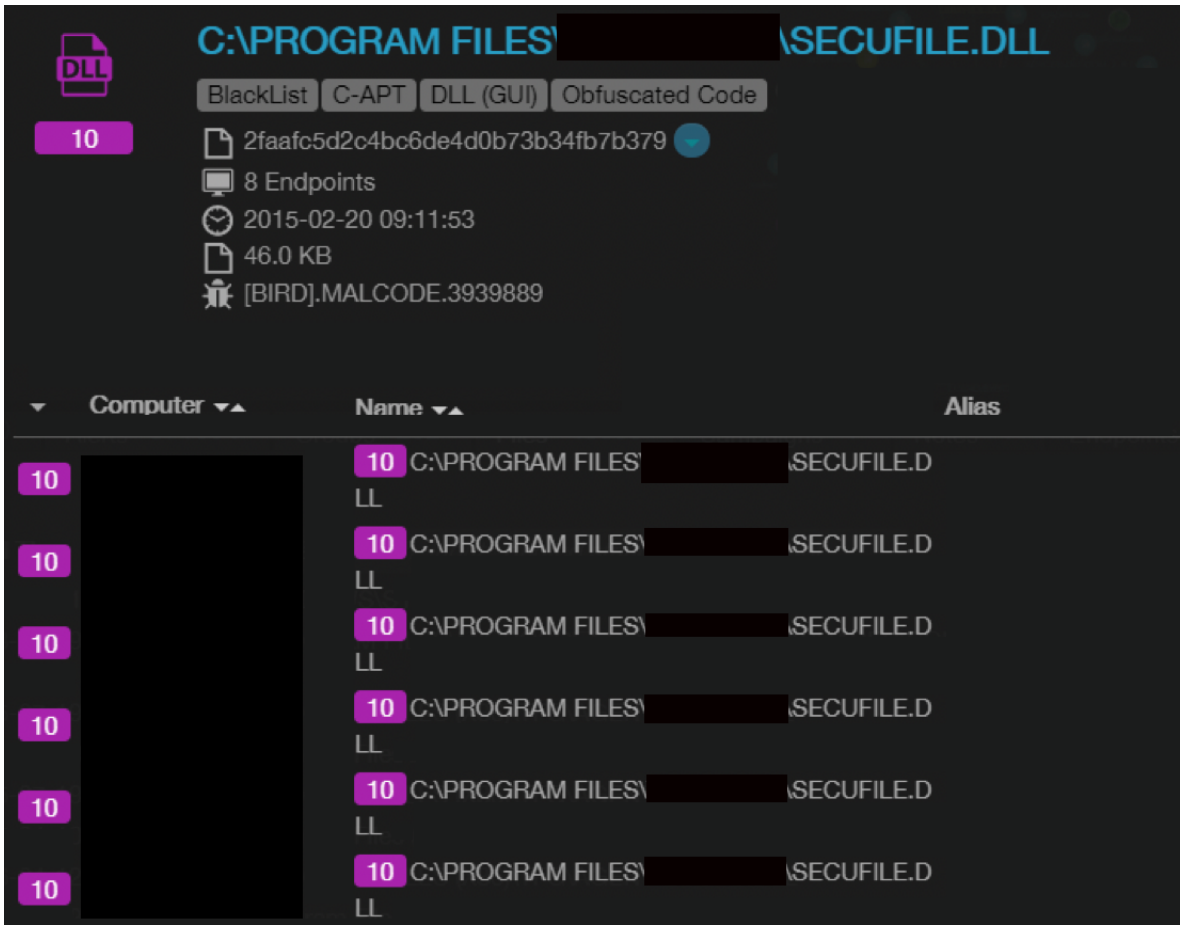
The attackers leveraged a DLL hijacking vulnerability in the DLP software to enlarge its defensive evasion capability and to persistently trigger next-stage malware. However, the DLP software failed to verify the integrity of their loaded DLLs. Thus the DLP software loaded the malicious DLL with high privilege.



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	96	0001B5F4	00000000	00000000	0001B7C6	00019000
SecuFile.dll	1	0002C75F	00000000	00000000	0002C752	0002C75F

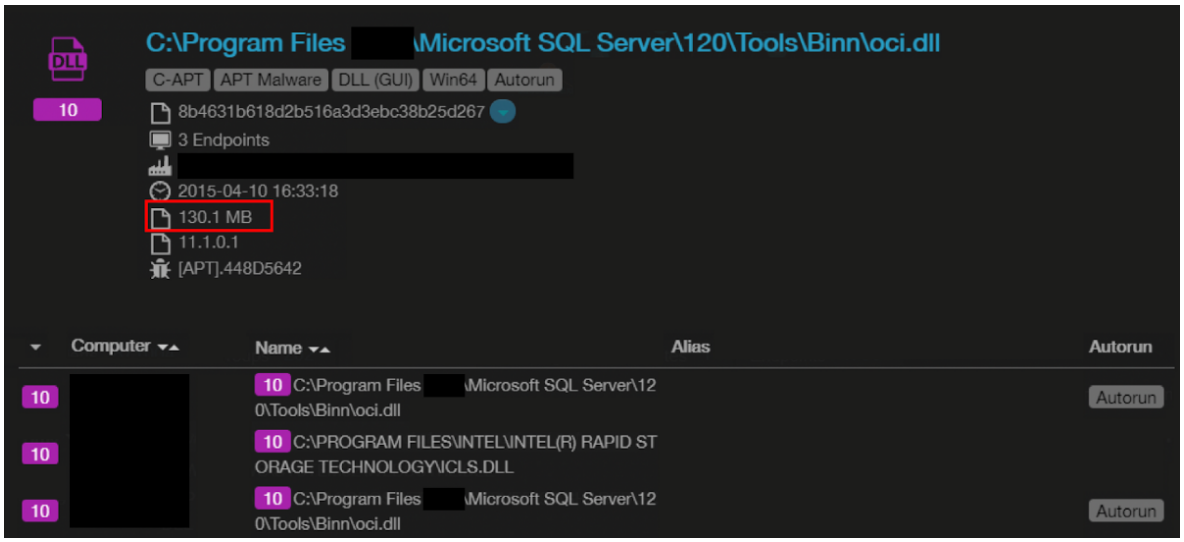
The attacker modified LOG4C.DLL to implant a new entry in the import table. The new entry will enforce the DLP software to load the malicious SecureFile.dll (or LIBDIG.dll). The loaded DLL then injects shellcode to system services, including Winmgmt, sens, Wuauserv and LanmanServer. Then, the next-stage malware payload is invoked to communicate to the C2 server.

```
Next-Stage MalwareC[:]\PROGRAM
FILES\XYZ\AGENT\ExportAgentConfig[.]datC[:]\Windows\PolicyDefinitions\TrayBar.admx
```



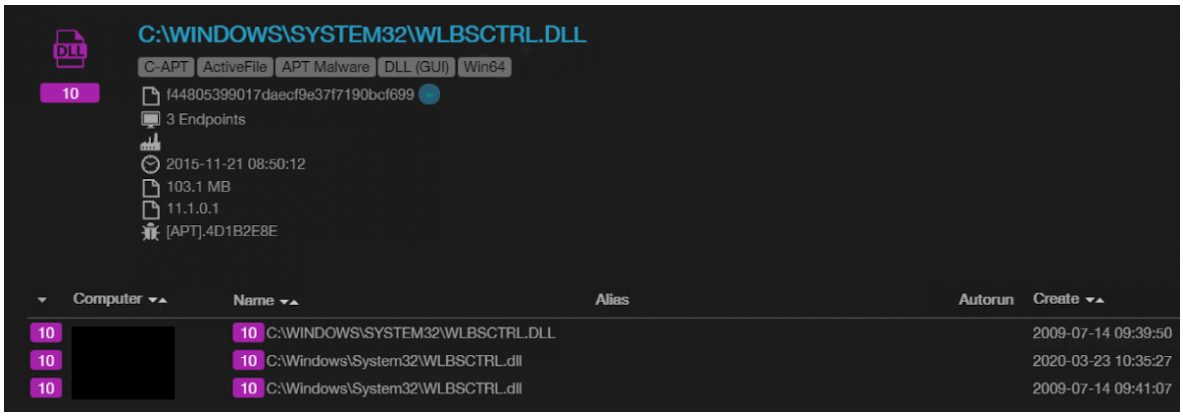
Increased Size

File-based scanners sometimes skip the scanning of larger files to maintain performance. The attackers enlarged the file size to bypass scanning altogether. The original size of file oci[.]dll is 66.5 KB however, as the above screenshot of CyberTotal demonstrates, oci[.]dll had been enlarged to 130 MB. Thus allowing it to be ignored by numerous security scanning tools.



Windows IKEEXT Service Abuse

The threat actor made use of Windows IKEEXT Service to load even more malware into memory — WLBSCTRL.DLL. Windows IKEEXT Service is a service for APN authentication that is disabled in the default Windows setting. This service is widely abused by attackers we observe.



Waterbear Loader Malware Analysis

File Metadata

> filename: libgid.dll
> md5: e3be074e0da9ba0c3201ceea4dd972d6
> sha1: cd8f49e467cf2f630c7f3b38a2e4c30e7bac6466
> sha256: e69690e4f94a60678aefc3adb80eef484bb5ca4285a2d3aabc1bb8d975fb7610
> filetype: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
> family: Waterbear Loader

Indicator

> file_path: C[:]\Windows\PolicyDefinitions\TrayBar.admx

RICH Header

```
Target machine: x32
@comp.id   id version count   description
000e1c83    e   7299     1
00041f6f    4   8047     2
00010000    1      0    30 [---] Unmarked objects
005d0fc3   5d   4035     5
000b2636    b   9782     4 [C++] VS98 (6.0) SP6 build 8804
000420ff    4   8447     1 [LNK] VC++ 6.0 SP5 imp/exp build 8447
```

The Waterbear Loader malware resurrected a 10-year-old antivirus evasion technique known as Heaven's Gate. In this particular case, the attackers applied Heaven's Gate to inject shellcode into the 64-bit system service from 32-bit WoW64.

Just as 64-bit and 32-bit programs are quite different, so are analysis mechanisms. Malware equipped with Heaven's Gate contains both 64-bit and 32-bit parts. Therefore, some monitor/analysis systems will only apply 32-bit analysis and will fail the 64-bit part; thus, this approach will break some monitor/analysis mechanisms.

Waterbear Loader forced itself to be unloaded, allowing it to evade detection from some memory forensic tools.

What is Heaven's Gate?

> This antivirus evasion technique permits 32-bit malware to hide API calls by switching to a 64-bit environment. Malware typically remains hidden inside the loader making it difficult for the AV to detect.
>
> While Heaven's Gate was first considered to be an advanced technique, over the last decade the Heaven's Gate exploit has been observed in more and more rootkits as well as other malware, such as the infamous Emotet trojan.
>
> Even though usage of the Heaven's Gate spread, Microsoft's release of Control Flow Guard (CFG) in Windows 10 immediately hindered the exploit's effectiveness as CFG prevented code jumps from WoW64 32-bit execution to native 64-bit code execution space. However, like most exploits, attackers still equip them when targeting legacy systems and the like — further demonstrating the need for organizations to update defenses early and update them often.

Behavior

```
void __cdecl DecodeData(LPVOID a1, DWORD a2)
{
  int v2; // eax
  int *v3; // ecx
  int v4; // edx




  v2 = (signed int)a2 / 4;
  if ( (signed int)a2 / 4 > 0 )
  {
    v3 = (int *)a1;
    do
    {
      v4 = *v3;
      ++v3;
      --v2;
      *(v3 - 1) = v4 ^ 0x781C362A;
    }
    while ( v2 );
  }
}
```

1. Waterbear Loader first checks whether the current execution context is WoW64, and looks for Winmgmt, sens, Wuauserv, LanmanServer to inject the shellcode.
2. Then, Waterbear Loader uses xor to decrypt strings in file with key 0x2a361c78
3. Waterbear Loader reads the encrypted payload. In this case: C:\Windows\PolicyDefinitions\TrayBar.admx
4. Then uses RC4 to decrypt it with key: 690c402f435878175d454028455a751b5372791e4358750c4359720b76626e1953747d0a0457781552361c78
5. In an attempt to further confuse analysis, Waterbear Loader padded contents from Kernel32.dll in front of and behind their shellcode.
6. Used x64_InjectShellcode to inject shellcode to the previously found service by Heaven's Gate.
7. In the end, the LdrData data is modified and forced to free the library by FreeLibraryAndExitThread.

```
int __stdcall StartAddress(LPVOID lpThreadParameter)
{
  int result; // eax
  int Pid; // esi
  unsigned int RetryCounter; // ecx
  bool PidFound; // zf
  int Size; // [esp+0h] [ebp-8h]
  LPVOID Shellcode; // [esp+4h] [ebp-4h]
```

```
  Size = 0;
  result = CheckWow64Process2();
  if ( result )
  {
    while ( 1 )
    {
      Sleep(1000u);
      Pid = FindServicePid();
      RetryCounter = Size + 1;
      PidFound = Pid == 0;
      ++Size;
      if ( Pid )
        break;
      if ( RetryCounter >= 20 )
      {
        PidFound = 1;
        break;
      }
    }
    if ( PidFound )
    {
      Shellcode = 0;
      if ( LoadShellcode(&Shellcode, &Size) )
      {
        x64_InjectShellcode(Shellcode, Size, Pid);
        memset(Shellcode, 0, Size);
        VirtualFree(Shellcode, 0, 0x8000u);
      }
    }
    ForceFreeLibrary(hInst);
    result = 0;
  }
  return result;
}
```

MITRE ATT&CK®

The following MITRE ATT&CK techniques were observed in this attack.

Persistence

T1547.001 Registry Run Keys/ Startup FolderT1574.001 DLL Search Order Hijacking

Privilege Escalation

T1574.001 DLL Search Order Hijacking

Defense Evasion

T1574.001 DLL Search Order HijackingT1027.002 Software PackingT1070.006 Timestop

Lateral Movement

T1021.001 Remote Desktop Protocol

IOCs

```
30DDEFC3093AFD7075A74BE30A381A3D     SQLWVSS.DLLC6EE3CEED5ADA7EE23FEB0E0CEA95193
IGTERM.DLL8B4631B618D2B516A3D3EBC38B25D267     OCI.DLL2FAAFC5D2C4BC6DE4D0B73B34FB7B379     SECUFILE.DLL
E3BE074E0DA9BA0C3201CEEA4DD972D6     LIBGID.DLL F44805399017DAECF9E37F7190BCF699     WLBSCTRL.DLL
F10034D1D8F90F36FEA602A4128BAEBC     SQLWVSS_NT.DLL 49D6C7FD1D47F345F64EEA6DA8591084     LOG4C.DLL
AE63EBAE30678DA8A7314A9427747BBE     LIBGID.DLL 48AA2A38E5125C4E0E4A069C473F67FC     LOG4C.DLL
```

Mitigation

1. Add listed IOCs to preventative solution blacklists.

2. Adjust detection and response solutions to detect listed IOCs.

3. Meticulously tracking down the root cause of the attack (not just the endpoint) and thoroughly removing malware is not only paramount in an IR investigation but could also prevent future attacks.

4. As DLP software is widely deployed in sensitive organizations, is daily-used software, and often has high privilege, DLP vendors and customers both need to constantly be striving on hardening security to maintain resilience even in the worst of situations.

5. Do not rely on a one-solution security policy. Preventative solutions (e.g., firewalls, antivirus) and DLP solutions are no longer enough to maintain resilience during an attack of this sophistication. AI-driven detection and response solutions, such as our award-winning CyCraft AIR, not only reduce mean dwell time but also increase SOC efficiency, automate investigations, and reduce alert fatigue.

> This article is Part 1 of a series of articles. Click here to read Part 2: Owlproxy Malware.

Follow Us

When you join CyCraft, you will be in good company. CyCraft secures government agencies, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, and SMEs.

We power SOCs with our proprietary and award-winning AI-driven MDR (managed detection and response), SOC (security operations center) operations software, TI (threat intelligence), Health Check, automated forensics, and IR (incident response), and Secure From Home services.

Additional Related Resources

- Learn how we targeting Taiwan's high-tech ecosystem. Read our full analysis and malware reversal.
-
-
-
-
- , and CyCraft Global Project Manager, Chad Duffy, speak on the latest MITRE ATT&CK Evaluations. Read their thoughts on our results and the philosophy powering CyCraft.
- Has your organization shifted to a Work From Home environment? Learn how to receive .
- drops your mean dwell time down from 197 days to under 1 day without false positives or false negatives. Know with confidence if hackers have penetrated your enterprise.

READY FOR A DEMO?

Contact us directly for more details: contact@cycraft.com