

# New Yanluowang Ransomware Found to be Code-Signed, Terminates Database-Related Processes

 [trendmicro.com/en\\_us/research/21//yanluowang-ransomware-code-signed-terminates-database-processes.html](https://trendmicro.com/en_us/research/21//yanluowang-ransomware-code-signed-terminates-database-processes.html)

December 10, 2021



## Ransomware

We analyzed new samples of the Yanluowang ransomware. One interesting aspect of these samples is that the files are code-signed. They also terminate various processes which are related to database and backup management.

By: Don Ovid Ladores December 10, 2021 Read time: ( words)

Content added to Folio



```
README.txt x
0 10 20 30 40 50 60 70 80 90 100 110 120 130 140 150 160
1 Hi, since you are reading this it means you have been hacked.
2 In addition to encrypting all your systems, deleting backups, we also downloaded 2 terabytes of confidential information.
3 Here's what you shouldn't do:
4 1) Contact the police, fbi or other authorities before the end of our deal
5 2) Contact the recovery company so that they would conduct dialogues with us. (This can slow down the recovery, and generally put our communication to naught)
6 3) Do not try to decrypt the files yourself, as well as do not change the file extension yourself !!! This can lead to the impossibility of their decryption.
7 4) Keep us for fools!)
8 We will also stop any communication with you, and continue DDoS, calls to employees and business partners.
9 In a few weeks, we will simply repeat our attack and delete all your data from your networks, WHICH WILL LEAD TO THEIR UNAVAILABILITY!
10 Here's what you should do right after reading it:
11 1) If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
12 2) If you are a CEO, or a specialist in the IT department, or another person who has weight in the company, you should contact us within 24 hours by email.
13 We are ready to confirm all our intentions regarding DDOS, calls, and deletion of the date at your first request.
14 As a guarantee that we can decrypt the files, we suggest that you send several files for free decryption.
15 Mails to contact us:
16 1) ██████████
17 2) ██████████
```

Figure 4. YanLuoWang ransomnote (README.txt)

## Digital signature, other features also found

It is important to highlight that the samples obtained are code-signed with a digital signature — and a valid one on that note, during the time of the analysis. The question remains whether this signature was stolen from a company or fraudulently signed.

Code signing is performed to validate the authenticity of a piece of software; thus, code-signed malware can appear legitimate and non-malicious, allowing it to bypass certain security measures.

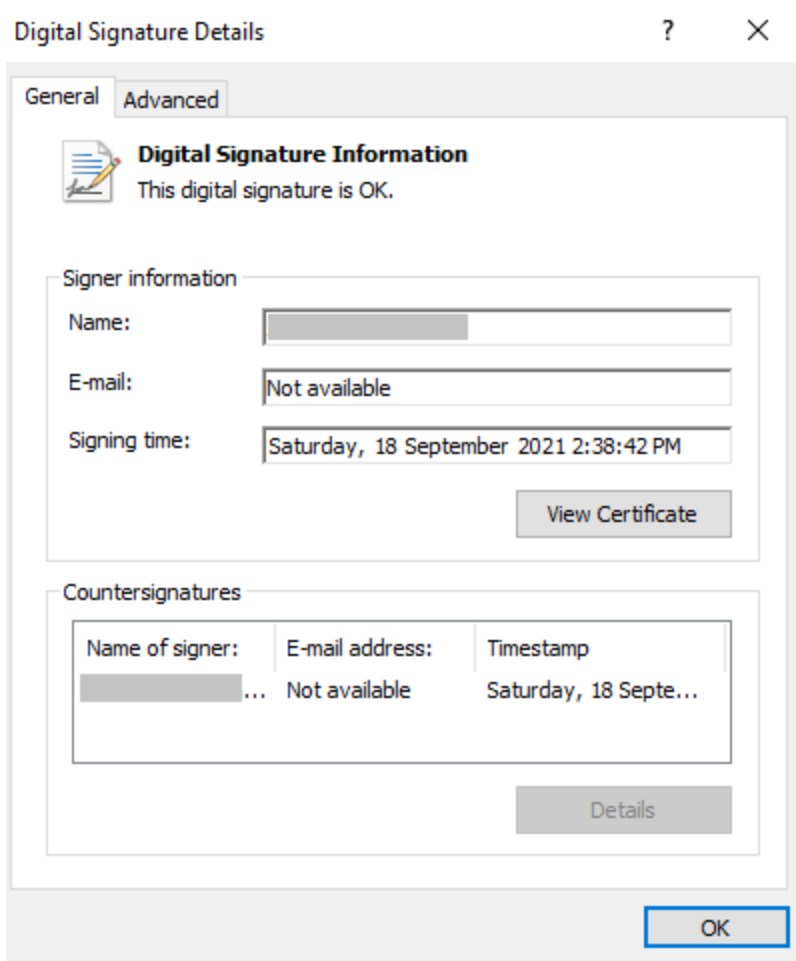


Figure 5. Digital signature found

with Yanluowang ransomware samples

Upon execution, the ransomware also terminates the following processes, which are related to managing databases and backups, through Windows API:

- Veeam
- SQL

The termination of database-related processes could potentially lead to loss of access to backup files, which then places additional pressure on ransomware victims to pay up to retrieve their files.

01345393	50	PUSH EAX	
01345394	8045 F4	PUSH EAX	
01345397	64:A3 00000000	LEA EAX, DWORD PTR SS:[EBP-C]	
01345399	6A 05	MOV DWORD PTR FS:[0],EAX	
0134539F	33C0	PUSH 5	
013453A1	C745 C0 000000	XOR EAX,EAX	
013453A8	68 84573901	MOV DWORD PTR SS:[EBP-40],0	
013453AD	8040 C0	PUSH d1179343.01395794	UNICODE "veeam"
013453B0	C745 D0 000000	LEA ECX, DWORD PTR SS:[EBP-40]	
013453B7	C745 D4 070000	MOV DWORD PTR SS:[EBP-30],0	
013453BE	66:8945 C0	MOV DWORD PTR SS:[EBP-2C],7	
013453C2	E8 593F0000	MOV WORD PTR SS:[EBP-40],AX	
013453C7	C745 FC 000000	CALL d1179343.01349320	
013453CE	8040 D8	MOV DWORD PTR SS:[EBP-4],0	
013453D1	6A 03	LEA ECX, DWORD PTR SS:[EBP-28]	
013453D3	33C0	PUSH 3	
013453D5	C745 D8 000000	XOR EAX,EAX	
013453DC	68 90573901	MOV DWORD PTR SS:[EBP-28],0	
013453E1	C745 E8 000000	PUSH d1179343.01395790	UNICODE "sql"
013453E8	C745 EC 070000	MOV DWORD PTR SS:[EBP-18],0	
013453EF	66:8945 D8	MOV DWORD PTR SS:[EBP-10],0	
013453F3	E8 283F0000	MOV WORD PTR SS:[EBP-28],AX	
013453F8	E8 283F0000	CALL d1179343.01349320	
013455B2	8085 B8FDFFFF	LEA EAX, DWORD PTR SS:[EBP-248]	
013455B8	50	PUSH EAX	
013455B9	E8 623D0000	CALL d1179343.01349320	
013455BE	33C9	XOR ECX,ECX	
013455C0	C645 FC 01	MOV BYTE PTR SS:[EBP-4],1	
013455C4	E8 C7FBFFFF	CALL <d1179343.string_compare>	
013455C9	83C4 30	ADD ESP,30	
013455CC	83F8 FF	CMP EAX,-1	
013455CF	74 26	JE SHORT d1179343.013455F7	
013455D1	FFB5 9CFDFFFF	PUSH DWORD PTR SS:[EBP-264]	
013455D7	6A 00	PUSH 0	
013455D9	6A 01	PUSH 1	
013455DB	FF95 7CFDFFFF	CALL DWORD PTR SS:[EBP-284]	
013455E1	8BF0	MOV ESI,EAX	
013455E3	85F6	TEST ESI,ESI	
013455E5	74 10	JE SHORT d1179343.013455F7	
013455E7	6A 09	PUSH 9	
013455E9	56	PUSH ESI	
013455EA	FF95 78FDFFFF	CALL DWORD PTR SS:[EBP-288]	Open_proc
013455F0	56	PUSH ESI	
013455F1	FF95 80FDFFFF	CALL DWORD PTR SS:[EBP-280]	terminate_proc
013455F7	8BB5 74FDFFFF	MOV ESI, DWORD PTR SS:[EBP-28C]	
013455FD	8085 94FDFFFF	LEA EAX, DWORD PTR SS:[EBP-26C]	

Figures 6-7.

### Terminating processes

The ransomware also attempts to terminate a few more processes through the command prompt if they match the following strings:

- mysql\*
- dsa\*
- veeam\*
- chrome\*
- iexplore\*
- firefox\*
- outlook\*
- excel\*
- taskmgr\*
- tasklist\*

- Ntrtscan\*
- ds\_monitor\*
- Notifier\*
- putty\*
- ssh\*
- TmListen\*
- iVPAgent\*
- CNTAoSMgr\*
- IBM\*
- bes10\*
- black\*
- robo\*
- copy\*
- sql
- store.exe
- sql\*
- vee\*
- wrsa\*
- wrsa.exe
- postg\*
- sage\*

Aside from processes, the malware will also forcefully stop (through net stop command line) the following services:

- MSSQLServerADHelper100
- MSSQL\$ISARS
- MSSQL\$MSFW
- SQLAgent\$ISARS
- SQLAgent\$MSFW
- SQLBrowser
- ReportServer\$ISARS
- SQLWriter
- WinDefend
- mr2kserv
- MExchangeADTopology
- MExchangeFBA
- MExchangeIS
- MExchangeSA
- ShadowProtectSvc
- SPAdminV4
- SPTimerV4
- SPTraceV4

- SPUserCodeV4
- SPWriterV4
- SPSearch4
- IISADMIN
- firebirdguardiandefaultinstance
- ibmiasrw
- QBCFMonitorService
- QBVSS
- QBOSDBServiceV12
- \"IBM Domino Server (CProgramFilesIBMDominodata)\"
- \"IBM Domino Diagnostics (CProgramFilesIBMDomino)\"
- \"Simply Accounting Database Connection Manager\"
- QuickBooksDB1
- QuickBooksDB2
- QuickBooksDB3
- QuickBooksDB4
- QuickBooksDB5
- QuickBooksDB6
- QuickBooksDB7
- QuickBooksDB8
- QuickBooksDB9
- QuickBooksDB10
- QuickBooksDB11
- QuickBooksDB12
- QuickBooksDB13
- QuickBooksDB14
- QuickBooksDB15
- QuickBooksDB16
- QuickBooksDB17
- QuickBooksDB18
- QuickBooksDB19
- QuickBooksDB20
- QuickBooksDB21
- QuickBooksDB22
- QuickBooksDB23
- QuickBooksDB24
- QuickBooksDB25

Lastly, it will forcefully terminate running virtual machines (VMs) through the following command line:

```
powershell -command \"Get-VM | Stop-VM -Force\"
```

```

-----
.text:00406BC0          ; -----
.text:00406BC2          push     0 ; lpDirectory
.text:00406BC7          push     offset Parameters ; "/c powershell -command \"Get-UM | Stop-\"...
.text:00406BCC          push     offset File ; "cmd.exe"
.text:00406BD1          push     offset Operation ; "open"
.text:00406BD5          mov     byte ptr [ebp+var_4], 15h
.text:00406BD8          mov     edi, ds:ShellExecuteA
.text:00406BDD          push     0 ; hwnd
.text:00406BDF          call    edi ; ShellExecuteA
.text:00406BE1          push     0 ; nShowCmd
.text:00406BE3          push     0 ; lpDirectory
.text:00406BE8          push     offset aNetStopMssqlse ; "net stop MSSQLServerADHelper100"
.text:00406BED          push     offset File ; "cmd.exe"
.text:00406BF2          push     offset Operation ; "open"
.text:00406BF4          push     0 ; hwnd
.text:00406BF6          call    edi ; ShellExecuteA
.text:00406BF8          push     0 ; nShowCmd
.text:00406BFA          push     0 ; lpDirectory
.text:00406BFF          push     offset aNetStopMssqlIs ; "net stop MSSQL$ISARS"
.text:00406C04          push     offset File ; "cmd.exe"
.text:00406C09          push     offset Operation ; "open"
.text:00406C0B          push     0 ; hwnd
.text:00406C0D          call    edi ; ShellExecuteA
.text:00406C0F          push     0 ; nShowCmd
.text:00406C11          push     0 ; lpDirectory
.text:00406C16          push     offset aNetStopMssqlIms ; "net stop MSSQL$MSFW"
.text:00406C1B          push     offset File ; "cmd.exe"
.text:00406C20          push     offset Operation ; "open"
.text:00406C22          push     0 ; hwnd
.text:00406C24          call    edi ; ShellExecuteA
.text:00406C26          push     0 ; nShowCmd
.text:00406C28          push     0 ; lpDirectory
.text:00406C2D          push     offset aNetStopSqlagen ; "net stop SQLAgent$ISARS"
.text:00406C32          push     offset File ; "cmd.exe"
.text:00406C37          push     offset Operation ; "open"
.text:00406C39          push     0 ; hwnd
.text:00406C39          call    edi ; ShellExecuteA

```

Figure 8. Terminating services

We will continue to monitor events related to the Yanluowang ransomware and share any updates.

## Strengthening defenses against ransomware

As new ransomware families continue to emerge, we foresee in our [2022 security predictions report](#) that ransomware operators will use more modern and sophisticated methods of extortion. Moving forward, enterprises must then take extra caution in applying preventive measures.

It would also help enterprises to establish frameworks that would help them with ransomware defense. Here are some of the best practices that they can include in their frameworks:

- Audit and take inventory of assets and data, authorized and unauthorized devices and software, and logs of events and incidents.
- Configure and monitor hardware and software configurations, and only grant admin privileges and access when absolutely necessary to an employee's role.
- Patch and update for operating systems and applications, perform regular vulnerability assessments, and conduct patching or virtual patching for operating systems and applications.
- Protect and recover essential information and files by enforcing stringent data protection, backup, and recovery measures.

- Perform security skills assessment and training regularly and conduct red-team exercises and penetration tests.
- Secure and defend systems by employing the latest version of security solutions to all layers of the system, including email, endpoint, web, and network.

Trend Micro Vision One™ offers multilayered protection and behavior detection, allowing for the detection of and blocking ransomware early on before it can do any real damage to the system. This is done by identifying questionable behavior that might otherwise seem benign when viewed from only a single layer.

Trend Micro Cloud One™ – Workload Security defends systems against both known and unknown threats that exploit vulnerabilities through techniques such as virtual patching and machine learning. It also leverages the latest in global threat intelligence to provide timely, real-time protection.

Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block ransomware before it gets into the system, blocking phishing emails that can be used by ransomware as entry points.

Trend Micro Apex One™ provides a closer inspection of endpoints through next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware.

## Indicators of Compromise (IoCs)

---

View the full list of IOCs [here](#).

We analyzed new samples of the Yanluowang ransomware, a recently discovered ransomware family. One interesting aspect of these samples is that the files are code-signed using a valid digital signature, which was either stolen or fraudulently signed. They also terminate various processes including Veeam and SQL, which are related to database and backup management.

After being uncovered a few weeks ago, the Yanluowang ransomware (named after the Chinese deity Yanluo Wang) has since been associated with campaigns, and its operators are said to launch targeted attacks on US corporations since at least August this year.

## Yanluowang ransomware initial analysis

---

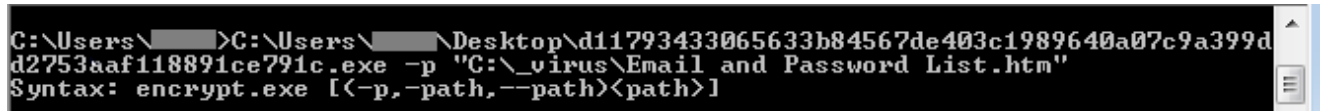
The Yanluowang ransomware samples we analyzed still have only a few detections as of this writing. Just looking at the files themselves shows very little about where or how they arrived at a user's system. But since the samples require certain arguments for proper execution, it appears that the most likely scenario for their execution is through remote desktop tools.



We also believe that the files analyzed here are merely part of a toolkit used by operators once they have compromised their victims' machines.

From our initial analysis, the ransomware checks for the following arguments that are primarily used to specify the directory where it would do its encryption:

- -h/--help
- -p/-path/--path
- -pass



```
C:\Users\>C:\Users\\Desktop\d11793433065633b84567de403c1989640a07c9a399d
d2753aaf118891ce791c.exe -p "C:\_virus\Email and Password List.htm"
Syntax: encrypt.exe [<-p,-path,--path><path>]
```

Figure 1. Checking for arguments (path)