

New Yanluowang Ransomware Used in Targeted Attacks

New arrival to the targeted ransomware scene appears to be still in development.

The Symantec Threat Hunter Team, a part of <u>Broadcom Software</u>, has uncovered what appears to be a new ransomware threat called Yanluowang that is being used in targeted attacks.

In a recent attempted ransomware attack against a large organization, Symantec obtained a number of malicious files that, upon further investigation, revealed the threat to be a new, if somewhat underdeveloped, ransomware family.

The Threat Hunter Team first spotted suspicious use of AdFind, a legitimate command-line Active Directory query tool, on the victim organization's network. This tool is often abused by ransomware attackers as a reconnaissance tool, as well as to equip the attackers with the resources that they need for lateral movement via Active Directory. Just days after the suspicious AdFind activity was observed on the victim organization, the attackers attempted to deploy the Yanluowang ransomware.

Before the ransomware is deployed on a compromised computer, a precursor tool carries out the following actions:

- Creates a .txt file with the number of remote machines to check in the command line
- Uses Windows Management Instrumentation (WMI) to get a list of processes running on the remote machines listed in the .txt file
- Logs all the processes and remote machine names to processes.txt

```
.rdata:004558B8 ; CHAR aNetStopMssqlMs[]
.rdata:004558B8 aNetStopMssqlMs db 'net stop MSSQL$MSFW',0
                                                        ; DATA XREF: main_module+1581to
.rdata:00455888
.rdata:004558CC ; CHAR aNetStopSqlagen[]
.rdata:004558CC aNetStopSqlagen db 'net stop SQLAgent$ISARS',0
                                                       ; DATA XREF: main_module+1598to
.rdata:004558CC
.rdata:004558E4 ; CHAR aNetStopSqlagen_0[]
.rdata:004558E4 aNetStopSqlagen_0 db 'net stop SQLAgent$MSFW',0
.rdata:004558E4
                                                       ; DATA XREF: main_module+15AFto
.rdata:004558FB align 4
.rdata:004558FC ; CHAR aNetStopSqlbrow[]
.rdata:004558FC aNetStopSqlbrow db 'net stop SQLBrowser',0
.rdata:004558FC
.rdata:00455910 ; CHAR aNetStopReports[]
                                                       ; DATA XREF: main module+15C6to
.rdata:00455910 aNetStopReports db 'net stop ReportServer$ISARS',0
                                                       ; DATA XREF: main_module+15DDto
.rdata:00455910
.rdata:0045592C ; CHAR aNetStopSqlwrit[]
.rdata:0045592C aNetStopSqlwrit db 'net stop SQLWriter',0
.rdata:0045592C
                                                      ; DATA XREF: main_module+15F4to
.rdata:0045593F
                               align 10h
.rdata:00455940 ; CHAR aNetStopWindefe[]
.rdata:00455940 aNetStopWindefe db 'net stop WinDefend',0
.rdata:00455940
                                                        ; DATA XREF: main module+160Bto
.rdata:00455953
                               align 4
.rdata:00455954 ; CHAR aNetStopMr2kser[]
.rdata:00455954 aNetStopMr2kser db 'net stop mr2kserv',0
                                                      ; DATA XREF: main_module+1622to
.rdata:00455954
.rdata:00455966
                               align 4
.rdata:00455968 ; CHAR aNetStopMsexcha[]
.rdata:00455968 aNetStopMsexcha db 'net stop MSExchangeADTopology',0
                                                      ; DATA XREF: main_module+1639to
.rdata:00455968
.rdata:00455986
                               align 4
.rdata:00455988 ; CHAR aNetStopMsexcha_0[]
.rdata:00455988 aNetStopMsexcha_0 db 'net stop MSExchangeFBA',0
.rdata:00455988
                                                       ; DATA XREF: main module+1650to
.rdata:0045599F
                               align 10h
.rdata:004559A0 ; CHAR aNetStopMsexcha_1[]
.rdata:004559A0 aNetStopMsexcha_1 db 'net stop MSExchangeIS',0
.rdata:004559A0
                                                        ; DATA XREF: main module+1667to
.rdata:004559B6
                                align 4
```

Figure 1. Yanluowang stops multiple services on compromised computers The Yanluowang ransomware is then deployed and carries out the following actions:

- Stops all hypervisor virtual machines running on the compromised computer
- Ends processes listed in processes.txt, which includes SQL and back-up solution Veeam
- Encrypts files on the compromised computer and appends each file with the .yanluowang extension
- Drops a ransom note named README.txt on the compromised computer

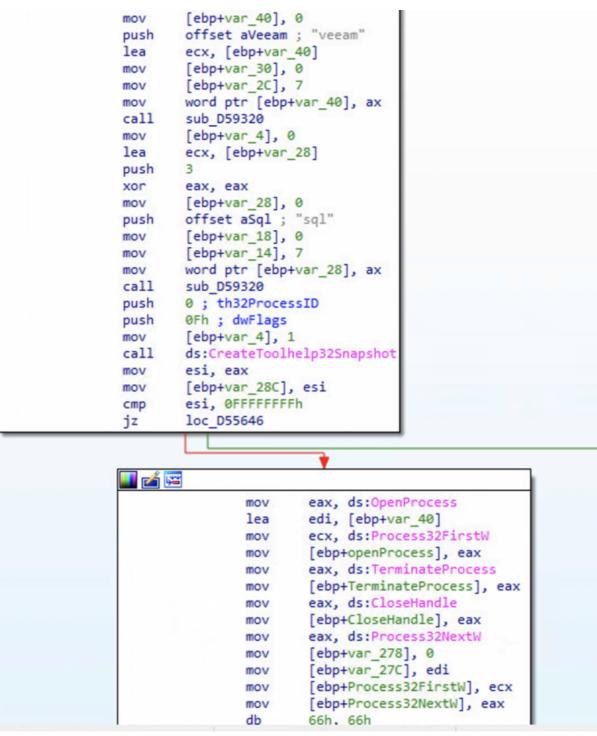


Figure 2. Yanluowang ends the SQL and Veeam processes before encryption

```
eax
pusn
                         ; pnprov
call
        ds:CryptAcquireContextW
lea
        eax, [ebp+phKey]
                         ; phKey
push
        eax
        edi
push
                         ; pInfo
        1
push
                        ; dwCertEncodingType
        [ebp+phProv]
push
                        ; hCryptProv
call
        ds:CryptImportPublicKeyInfo
mov
        esi, ds:CryptEncrypt
lea
        eax, [ebp+pdwDataLen]
                         ; dwBufLen
        20h ; '
push
push
        eax
                         ; pdwDataLen
push
        0
                         ; pbData
        0
                         ; dwFlags
push
                         ; Final
push
        1
push
        0
                         ; hHash
                         ; hKey
push
        [ebp+phKey]
        [ebp+var_1118], 20h ;
mov
        [ebp+pdwDataLen], 20h ; ' '
mov
call
        esi ; CryptEncrypt
push
        [ebp+pdwDataLen]
call
        ?? U@YAPAXI@Z ; operator new[](uint)
        ecx, [ebp+var 13B0]
mov
add
        esp, 4
        [ebp+pbBinary], eax
mov
movups
        xmm0, xmmword ptr [ecx]
movups
        xmmword ptr [eax], xmm0
        xmm0, xmmword ptr [ecx+10h]
movups
lea
        ecx, [ebp+var 1118]
        xmmword ptr [eax+10h], xmm0
movups
        [ebp+pdwDataLen] ; dwBufLen
push
                         ; pdwDataLen
push
        ecx
                        ; pbData
push
        eax
push
        0
                         ; dwFlags
                         ; Final
        1
push
push
                         ; hHash
        0
push
        [ebp+phKey]
                         ; hKey
call
        esi ; CryptEncrypt
lea
        eax, [ebp+pbEncoded]
xor
        edi, edi
                         ; pcchString
push
        eax
                        ; pszString
push
        edi
push
        1
                         ; dwFlags
```

Figure 3.

Yanluowang uses the Windows API for encryption

The ransom note dropped by Yanluowang warns victims not to contact law enforcement or ransomware negotiation firms. If the attackers' rules are broken the ransomware operators say they will conduct distributed denial of service (DDoS) attacks against the victim, as well as make "calls to employees and business partners." The criminals also threaten to repeat the attack "in a few weeks" and delete the victim's data.

i, since you are reading this it means you have been hacked.
in addition to encrypting all your systems, deleting backups, we also downloaded 2 terabytes of confidential information.
iere's what you shouldn't do:
) Contact the police, fbi or other authorities before the end of our deal
) 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)
) 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.
Keep us for fools)
e will also stop any communication with you, and continue DOoS, calls to employees and business partners.
in a few weeks, we will simply repeat our attack and delete all your data from your networks, WHICH WILL LEAD TO THEIR UNAVAILABILITY!
ere's what you should do right after reading it:
) If you are an ordinary employee, and our message to the CEO of the company, as well as to the IT department
) 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.
e are ready to confirm all our intentions regarding DOOS, calls, and deletion of the date at your first request.
is a guarantee that we can decrypt the files, we suggest that you send several files for free decryption.
ails to contact us:
,
The tay of second s

Figure 4. Yanluowang ransom note **Protection**

File based:

• Ransom.Yanluowang

For the latest protection updates, please visit the <u>Symantec Protection</u> <u>Bulletin</u>.

Indicators of Compromise

- d11793433065633b84567de403c1989640a07c9a399dd2753aaf11889 1ce791c
- 49d828087ca77abc8d3ac2e4719719ca48578b265bbb632a1a7a36560 ec47f2d
- 2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27 770e04