New Yanluowang Ransomware Used in Targeted Attacks

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/yanluowang-targeted-ransomware





Threat Hunter TeamSymantec

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$MSFW',0
.rdata:004558B8
                                                        ; DATA XREF: main module+1581to
.rdata:004558CC ; CHAR aNetStopSqlagen[]
.rdata:004558CC aNetStopSqlagen db 'net stop SQLAgent$ISARS',0
.rdata:004558CC
                                                        ; DATA XREF: main module+1598to
.rdata:004558E4 ; CHAR aNetStopSqlagen 0[]
.rdata:004558E4 aNetStopSqlagen_0 db 'net stop SQLAgent$MSFW',0
.rdata:004558E4
                                                       ; DATA XREF: main_module+15AFto
.rdata:004558FB
.rdata:004558FC ; CHAR aNetStopSqlbrow[]
.rdata:004558FC aNetStopSqlbrow db 'net stop SQLBrowser',0
.rdata:004558FC
                                                        ; DATA XREF: main module+15C6fo
.rdata:00455910 ; CHAR aNetStopReports[]
.rdata:00455910 aNetStopReports db 'net stop ReportServer$ISARS',0
.rdata:00455910
                                                        ; DATA XREF: main module+15DDto
.rdata:0045592C ; CHAR aNetStopSqlwrit[]
.rdata:0045592C aNetStopSqlwrit db 'net stop SQLWriter',0
.rdata:0045592C
                                                       ; DATA XREF: main module+15F4to
.rdata:0045593F
.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+1622fo
.rdata:00455954
.rdata:00455966
                               align 4
.rdata:00455968 ; CHAR aNetStopMsexcha[]
.rdata:00455968 aNetStopMsexcha db 'net stop MSExchangeADTopology',0
.rdata:00455968
                                                       ; DATA XREF: main module+1639to
.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
                                align 10h
.rdata:0045599F
.rdata:004559A0 ; CHAR aNetStopMsexcha_1[]
.rdata:004559A0 aNetStopMsexcha_1 db 'net stop MSExchangeIS',0
.rdata:004559A0
                                                        ; DATA XREF: main module+1667to
.rdata:00455986
                                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

```
[ebp+var 40], 0
mov
        offset aVeeam; "veeam"
push
        ecx, [ebp+var 40]
lea
        [ebp+var 30], 0
mov
        [ebp+var_2C], 7
mov
mov
        word ptr [ebp+var 40], ax
        sub D59320
call
        [ebp+var 4], 0
mov
        ecx, [ebp+var 28]
lea
push
xor
        eax, eax
        [ebp+var_28], 0
mov
        offset aSql ; "sql"
push
        [ebp+var 18], 0
mov
        [ebp+var_14], 7
mov
        word ptr [ebp+var_28], ax
mov
call
        sub D59320
push
        0 ; th32ProcessID
        OFh ; dwFlags
push
mov
        [ebp+var 4], 1
        ds:CreateToolhelp32Snapshot
call
        esi, eax
mov
        [ebp+var_28C], esi
mov
        esi, OFFFFFFFh
cmp
        loc D55646
jz
  mov
                         eax, ds:OpenProcess
                lea
                         edi, [ebp+var 40]
                mov
                         ecx, ds:Process32FirstW
                         [ebp+openProcess], eax
                mov
                         eax, ds:TerminateProcess
                mov
                         [ebp+TerminateProcess], eax
                mov
                mov
                         eax, ds:CloseHandle
                         [ebp+CloseHandle], eax
                mov
                         eax, ds:Process32NextW
                mov
                         [ebp+var 278], 0
                mov
                         [ebp+var 27C], edi
                mov
                         [ebp+Process32FirstW], ecx
                mov
                mov
                         [ebp+Process32NextW], eax
                         66h. 66h
                db
```

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

```
push eax ; pnProv

call ds:CryptAcquireContextW

lea eax, [ebp+phKey]

push eax ; phKey

push edi : pInfo
```

```
; dwCertEncodingType
push
        1
push
                        ; hCryptProv
        [ebp+phProv]
call
        ds:CryptImportPublicKeyInfo
        esi, ds:CryptEncrypt
mov
        eax, [ebp+pdwDataLen]
lea
push
        20h ; '
                         ; dwBufLen
push
                         ; pdwDataLen
        eax
push
                         ; pbData
        0
                         ; dwFlags
push
        0
                         ; Final
push
        1
                         ; hHash
push
        0
push
        [ebp+phKey]
                         ; hKey
        [ebp+var 1118], 20h;
mov
        [ebp+pdwDataLen], 20h; '
mov
        esi ; CryptEncrypt
call
push
        [ebp+pdwDataLen]
        ?? U@YAPAXI@Z ; operator new[](uint) Figure 3.
call
        ecx, [ebp+var 13B0]
mov
add
        esp, 4
        [ebp+pbBinary], eax
mov
movups xmm0, xmmword ptr [ecx]
movups xmmword ptr [eax], xmm0
movups xmm0, xmmword ptr [ecx+10h]
        ecx, [ebp+var 1118]
lea
movups
        xmmword ptr [eax+10h], xmm0
        [ebp+pdwDataLen]; dwBufLen
push
push
                         ; pdwDataLen
        ecx
push
                         ; pbData
      eax
push
        0
                         ; dwFlags
                         ; Final
push
        1
push
        0
                         ; hHash
push
       [ebp+phKey]
                         ; hKev
call
        esi ; CryptEncrypt
        eax, [ebp+pbEncoded]
lea
        edi, edi
xor
                         ; pcchString
push
        eax
                         ; pszString
push
        edi
push
                         ; dwFlags
        1
```

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.

```
is, since you are reading this it means you have been hacked.
In addition to encrypting all your systems, deleting backups, we also downloaded ? terabytes of confidential information.

| Contact the police, fbi or other authorities before the end of our deal
| 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)
| 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)
| 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)
| Contact the recovery company so that they would contact us well as do not change the file extension yourself!!! This can lead to the impossibility of their decryption.
| Contact us will also stop any communication with you, and continue DOOS, calls to employees and business partners.
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
| If you are an ordinary employee, send our message to the CEO o
```

Figure 4. Yanluowang ransom note

Protection

File based:

Ransom. Yanluowang

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

Indicators of Compromise

- d11793433065633b84567de403c1989640a07c9a399dd2753aaf118891ce791c
- 49d828087ca77abc8d3ac2e4719719ca48578b265bbb632a1a7a36560ec47f2d
- 2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27770e04

BroadcomSymantec Enterprise Blogs
You might also enjoy



Threat Intelligence3 Min Read

The Ransomware Threat in 2021

New research from Symantec finds that organizations face an unprecedented level of danger from targeted ransomware attacks as the number of adversaries multiply alongside an increased sophistication in tactics.



About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?