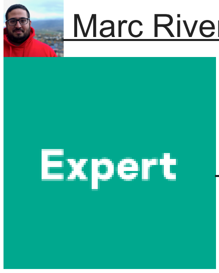
How to recover files encrypted by Yanluowang

securelist.com/how-to-recover-files-encrypted-by-yanlouwang/106332/

Authors

- Marc Rivero
- 

 Yanis Zinchenko

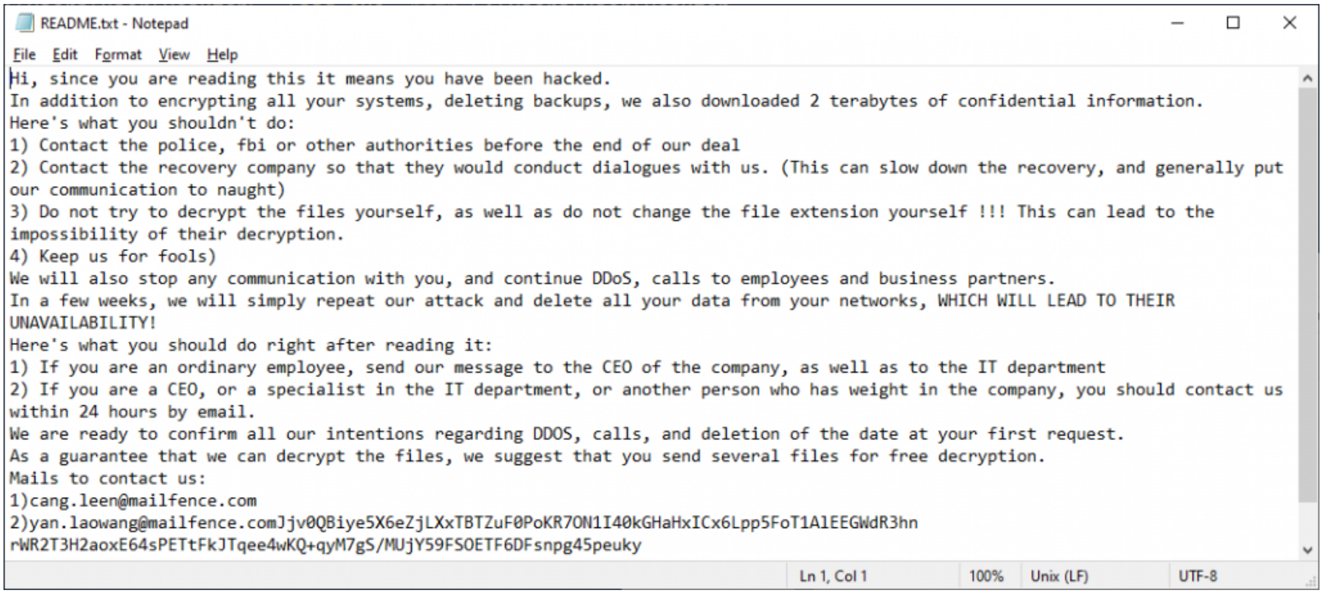
Yanluowang is a type of targeted ransomware discovered by the Symantec Threat Hunter team as they were investigating an incident on a large corporate network. Kaspersky experts have found a vulnerability in the Yanluowang encryption algorithm and created a free decryptor to help victims of this ransomware with recovering their files.

Yanluowang description

The ransomware is relatively recent, its name a reference to the Chinese deity Yanluo Wang, one of the Ten Kings of Hell. Unfortunately, we do not know much about the victims. According to Kaspersky Security Network data, attacks have been carried out in the United States, Brazil, Turkey and a few other countries. The low number of infections is due to the targeted nature of the ransomware: threat actors prepare and implement attacks on specific companies only.

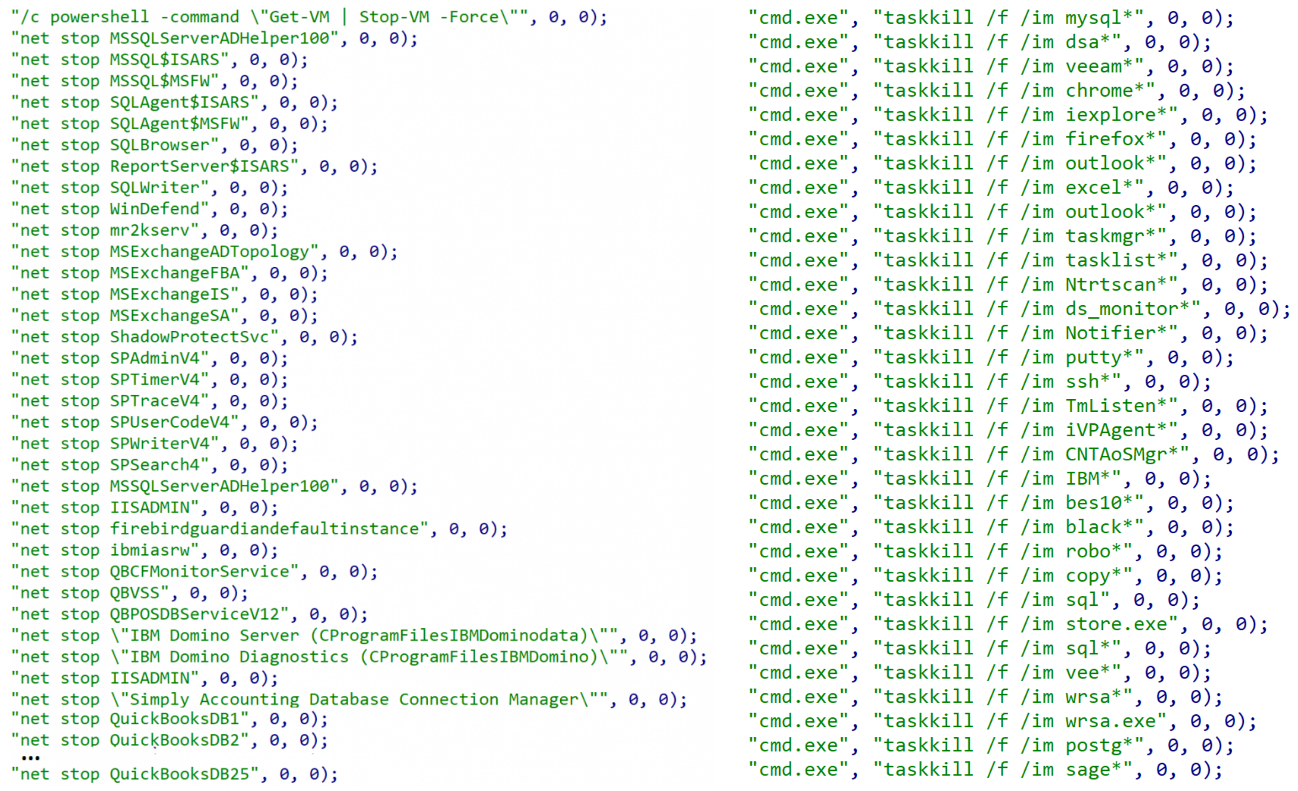
Geography of the Yanluowang attacks, December 4th, 2021 – April 8th, 2022 (download)

In the ransom note, the cybercriminals demand not to contact law enforcement and not ‘keep them for fools’:



```
Hi, 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.
Here's what you shouldn't do:
1) Contact the police, fbi or other authorities before the end of our deal
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)
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.
4) Keep us for fools)
We will also stop any communication with you, and continue DDoS, 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!
Here's what you should do right after reading it:
1) If you are an ordinary employee, send our message to the CEO of the company, as well as to the IT department
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.
We are ready to confirm all our intentions regarding DDOS, calls, and deletion of the date at your first request.
As a guarantee that we can decrypt the files, we suggest that you send several files for free decryption.
Mails to contact us:
1)cang.leen@mailfence.com
2)yan.laowang@mailfence.comJjv0QBiye5X6eZjLXxTBTZuF0PoKR7ON1I40kGHaHxICx6Lpp5FoT1AlEEGWdR3hn
rWR2T3H2aoxE64sPETtFkJTqee4wKQ+qyM7gS/MUjY59FSOETF6DFsnpg45peuky
```

The ransomware program has the functionality to terminate virtual machines, processes and services. This is necessary to make files used by other programs available for encryption. The main parts of stopped services and processes include databases, email services, browsers, programs for working with documents, security solutions, backups and shadow copy services.



```
"/c powershell -command \"Get-VM | Stop-VM -Force\"", 0, 0);
"net stop MSSQLServerADHelper100", 0, 0);
"net stop MSSQL$ISARS", 0, 0);
"net stop MSSQL$MSFW", 0, 0);
"net stop SQLAgent$ISARS", 0, 0);
"net stop SQLAgent$MSFW", 0, 0);
"net stop SQLBrowser", 0, 0);
"net stop ReportServer$ISARS", 0, 0);
"net stop SQLWriter", 0, 0);
"net stop WinDefend", 0, 0);
"net stop mr2kserv", 0, 0);
"net stop MSExchangeADTopology", 0, 0);
"net stop MSExchangeFBA", 0, 0);
"net stop MSExchangeIS", 0, 0);
"net stop MSExchangeSA", 0, 0);
"net stop ShadowProtectSvc", 0, 0);
"net stop SPAdminV4", 0, 0);
"net stop SPTimerV4", 0, 0);
"net stop SPTraceV4", 0, 0);
"net stop SPUserCodeV4", 0, 0);
"net stop SPWriterV4", 0, 0);
"net stop SPSearch4", 0, 0);
"net stop MSSQLServerADHelper100", 0, 0);
"net stop IISADMIN", 0, 0);
"net stop firebirdguardiandefaultinstance", 0, 0);
"net stop ibmiasrw", 0, 0);
"net stop QBCFMonitorService", 0, 0);
"net stop QBVSS", 0, 0);
"net stop QBPOSDBServiceV12", 0, 0);
"net stop \"IBM Domino Server (CProgramFilesIBMDominodata)\"", 0, 0);
"net stop \"IBM Domino Diagnostics (CProgramFilesIBMDomino)\"", 0, 0);
"net stop IISADMIN", 0, 0);
"net stop \"Simply Accounting Database Connection Manager\"", 0, 0);
"net stop QuickBooksDB1", 0, 0);
"net stop QuickBooksDB2", 0, 0);
 ...
"net stop QuickBooksDB25", 0, 0);
```

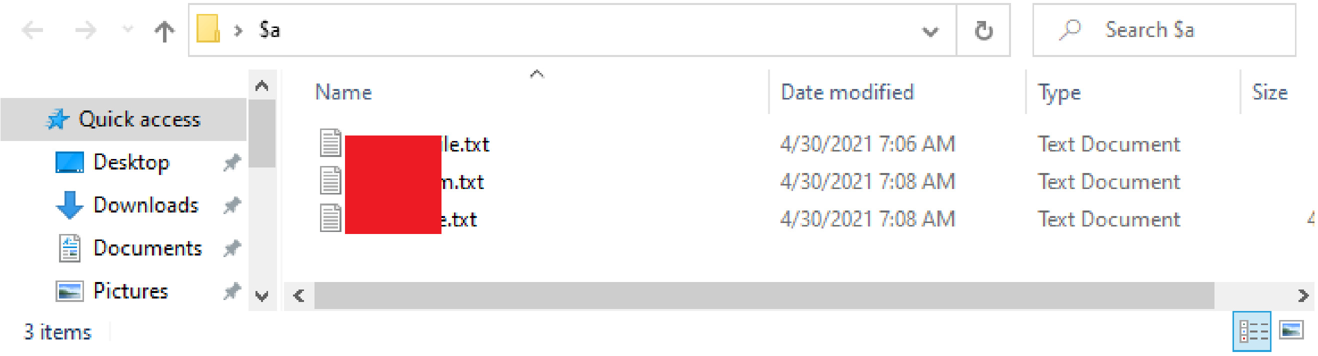
```
"cmd.exe", "taskkill /f /im mysql*", 0, 0);
"cmd.exe", "taskkill /f /im dsa*", 0, 0);
"cmd.exe", "taskkill /f /im veeam*", 0, 0);
"cmd.exe", "taskkill /f /im chrome*", 0, 0);
"cmd.exe", "taskkill /f /im iexplore*", 0, 0);
"cmd.exe", "taskkill /f /im firefox*", 0, 0);
"cmd.exe", "taskkill /f /im outlook*", 0, 0);
"cmd.exe", "taskkill /f /im excel*", 0, 0);
"cmd.exe", "taskkill /f /im outlook*", 0, 0);
"cmd.exe", "taskkill /f /im taskmgr*", 0, 0);
"cmd.exe", "taskkill /f /im tasklist*", 0, 0);
"cmd.exe", "taskkill /f /im Ntrtscan*", 0, 0);
"cmd.exe", "taskkill /f /im ds_monitor*", 0, 0);
"cmd.exe", "taskkill /f /im Notifier*", 0, 0);
"cmd.exe", "taskkill /f /im putty*", 0, 0);
"cmd.exe", "taskkill /f /im ssh*", 0, 0);
"cmd.exe", "taskkill /f /im TmListen*", 0, 0);
"cmd.exe", "taskkill /f /im iVPAgent*", 0, 0);
"cmd.exe", "taskkill /f /im CNTAoSMgr*", 0, 0);
"cmd.exe", "taskkill /f /im IBM*", 0, 0);
"cmd.exe", "taskkill /f /im bes10*", 0, 0);
"cmd.exe", "taskkill /f /im black*", 0, 0);
"cmd.exe", "taskkill /f /im robo*", 0, 0);
"cmd.exe", "taskkill /f /im copy*", 0, 0);
"cmd.exe", "taskkill /f /im sql", 0, 0);
"cmd.exe", "taskkill /f /im store.exe", 0, 0);
"cmd.exe", "taskkill /f /im sql*", 0, 0);
"cmd.exe", "taskkill /f /im vee*", 0, 0);
"cmd.exe", "taskkill /f /im wrsa*", 0, 0);
"cmd.exe", "taskkill /f /im wrsa.exe", 0, 0);
"cmd.exe", "taskkill /f /im postg*", 0, 0);
"cmd.exe", "taskkill /f /im sage*", 0, 0);
```

Lists of stopped services and processes

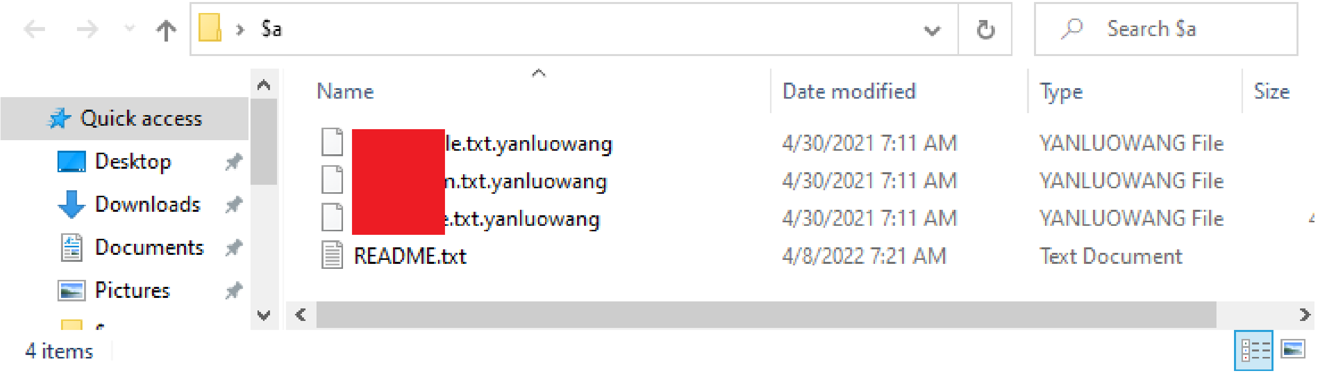
According to public information about the ransomware, it is only used in targeted attacks rather than in other RaaS families. Yanluowang itself needs parameters to be executed in the system, meaning it will be executed either manually or through a combination of scripts in the compromised system. The available syntax in the ransomware is:

```
encrypt.exe [(-p,-path,--path)<path>]
```

The Sosemanuk stream cipher is used to encrypt files, its key then encrypted using the RSA-1024 asymmetric algorithm. The RSA public key itself is embedded in the program but additionally encrypted with the RC4 stream cipher whose key is a string and also embedded in ransomware. Files before and after encryption:



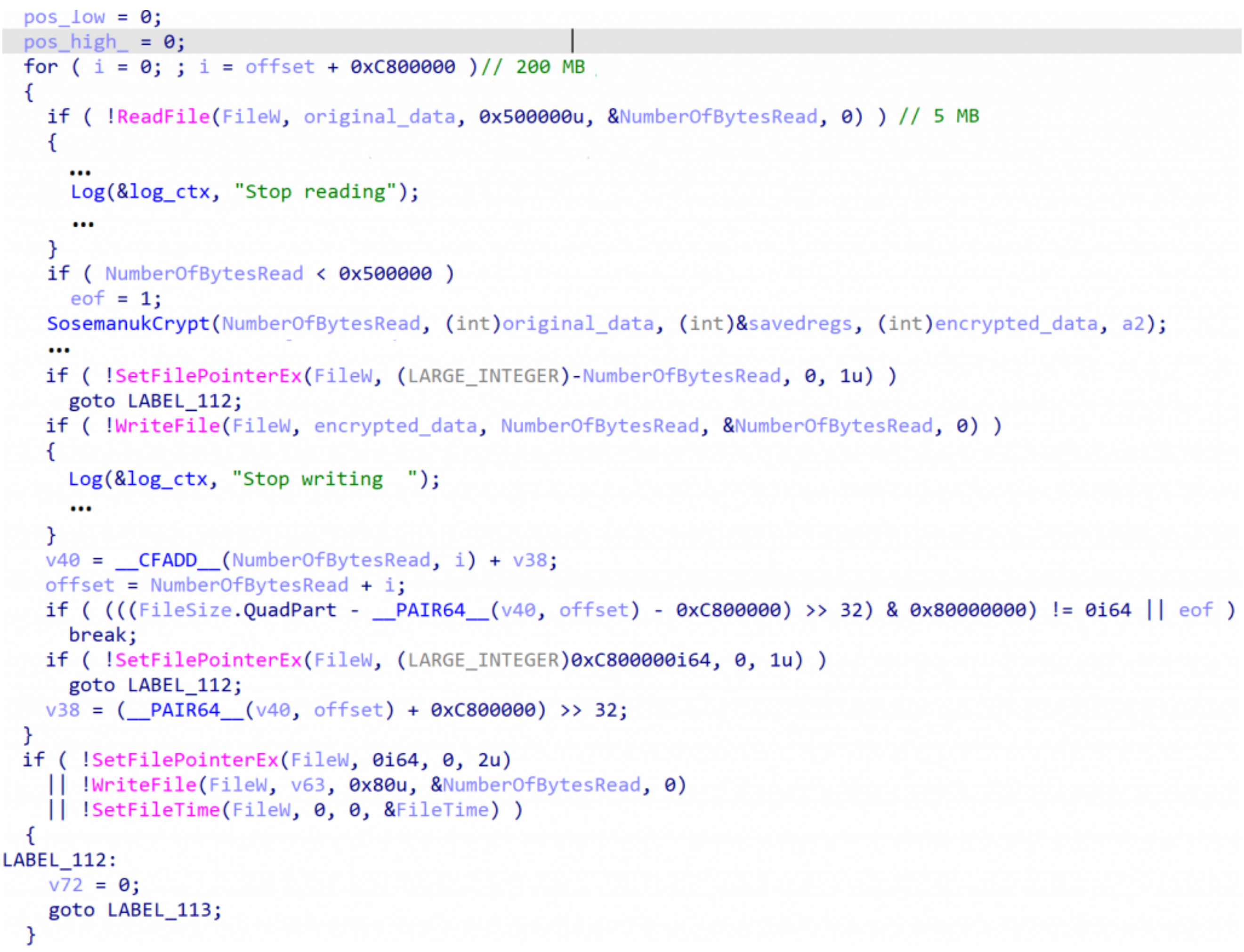
Name	Date modified	Type	Size
[redacted]le.txt	4/30/2021 7:06 AM	Text Document	
[redacted]n.txt	4/30/2021 7:08 AM	Text Document	
[redacted].txt	4/30/2021 7:08 AM	Text Document	4



Name	Date modified	Type	Size
[redacted]le.txt.yanluowang	4/30/2021 7:11 AM	YANLUOWANG File	
[redacted]n.txt.yanluowang	4/30/2021 7:11 AM	YANLUOWANG File	
[redacted].txt.yanluowang	4/30/2021 7:11 AM	YANLUOWANG File	4
README.txt	4/8/2022 7:21 AM	Text Document	

When the encryption process is completed, the file extensions will be changed to .yanluowang

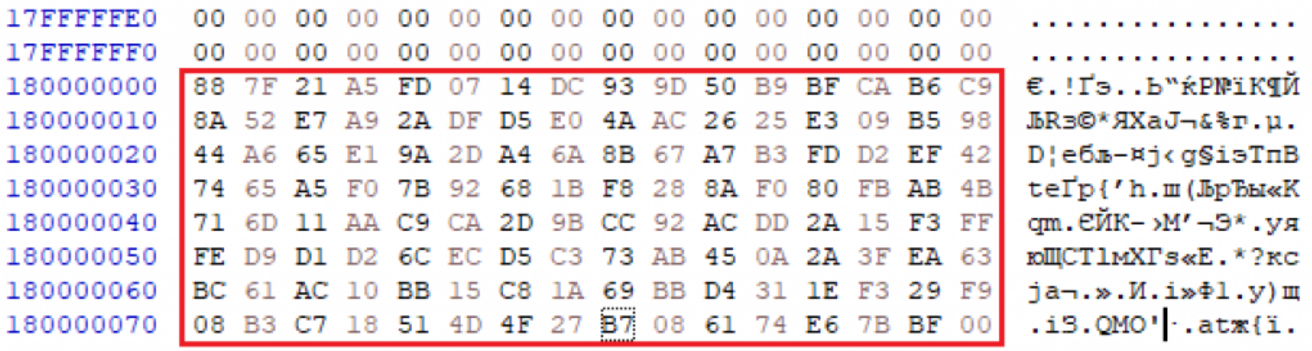
Yanluowang divides files into big and small along a 3 GB threshold. Small files are encrypted completely from beginning to end, big files are encrypted in stripes: 5 megabytes after every 200 megabytes.



```
  pos_low = 0;
  pos_high_ = 0;
  for ( i = 0; ; i = offset + 0xC800000 )// 200 MB
  {
    if ( !ReadFile(FileW, original_data, 0x500000u, &NumberOfBytesRead, 0) ) // 5 MB
    {
      ...
      Log(&log_ctx, "Stop reading");
      ...
    }
    if ( NumberOfBytesRead < 0x500000 )
      eof = 1;
    SosemanukCrypt(NumberOfBytesRead, (int)original_data, (int)&savedregs, (int)encrypted_data, a2);
    ...
    if ( !SetFilePointerEx(FileW, (LARGE_INTEGER)-NumberOfBytesRead, 0, 1u) )
      goto LABEL_112;
    if ( !WriteFile(FileW, encrypted_data, NumberOfBytesRead, &NumberOfBytesRead, 0) )
    {
      Log(&log_ctx, "Stop writing  ");
      ...
    }
    v40 = __CFADD__(NumberOfBytesRead, i) + v38;
    offset = NumberOfBytesRead + i;
    if ( (((FileSize.QuadPart - __PAIR64__(v40, offset) - 0xC800000) >> 32) & 0x80000000) != 0i64 || eof )
      break;
    if ( !SetFilePointerEx(FileW, (LARGE_INTEGER)0xC800000i64, 0, 1u) )
      goto LABEL_112;
    v38 = (__PAIR64__(v40, offset) + 0xC800000) >> 32;
  }
  if ( !SetFilePointerEx(FileW, 0i64, 0, 2u)
    || !WriteFile(FileW, v63, 0x80u, &NumberOfBytesRead, 0)
    || !SetFileTime(FileW, 0, 0, &FileTime) )
  {
LABEL_112:
    v72 = 0;
    goto LABEL_113;
  }
```

The encryption code for big files

After a file is encrypted, an RSA-encrypted Sosemanuk key is written to the end of it. The encrypted endfile block has a size of 1024 bytes.



```
17FFFFFE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
17FFFFFF0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
180000000  88 7F 21 A5 FD 07 14 DC 93 9D 50 B9 BF CA B6 C9  €.!Ґэ..Ь“ќР№їКЙ
180000010  8A 52 E7 A9 2A DF D5 E0 4A AC 26 25 E3 09 B5 98  ЉRз©*ЯХаJ¬&%г.µ.
180000020  44 A6 65 E1 9A 2D A4 6A 8B 67 A7 B3 FD D2 EF 42  D¦eбљ-¤j‹g§іэТпB
180000030  74 65 A5 F0 7B 92 68 1B F8 28 8A F0 80 FB AB 4B  teҐр{’h.ш(ЉрЂы«K
180000040  71 6D 11 AA C9 CA 2D 9B CC 92 AC DD 2A 15 F3 FF  qm.ЄЙК-›М’¬Э*.уя
180000050  FE D9 D1 D2 6C EC D5 C3 73 AB 45 0A 2A 3F EA 63  юЩСТlмХГs«E.*?кc
180000060  BC 61 AC 10 BB 15 C8 1A 69 BB D4 31 1E F3 29 F9  јa¬.».И.i»Ф1.у)щ
180000070  08 B3 C7 18 51 4D 4F 27 B7 08 61 74 E6 7B BF 00  .іЗ.QMO'·.atж{ї.
```

An encrypted block with a Sosemanuk key

Files decryption

Kaspersky experts have analyzed the ransomware and found a vulnerability that allows decrypting files of affected users via a known-plaintext attack. All that was required for this to work was added to the Rannoh decryption tool.

To decrypt a file, you should have at least one original file. As mentioned earlier, the Yanluowang ransomware divides files into big and small files along a 3 gigabyte threshold. This creates a number of conditions that must be met in order to decrypt certain files:

- To decrypt small files (less than or equal to 3 GB), you need a pair of files with a size of 1024 bytes or more. This is enough to decrypt all other small files.
- To decrypt big files (more than 3 GB), you need a pair of files (encrypted and original) no less than 3 GB in size each. This will be enough to decrypt both big and small files.

By virtue of the above points, if the original file is larger than 3 GB, it is possible to decrypt all files on the infected system, both big and small. But if there is an original file smaller than 3 GB, then only small files can be decrypted.

Indicators of Compromise

Kaspersky solutions detect and protect against this ransomware, detecting it as **Trojan-Ransom.Win32.Yanluowang** with File Threat Protection and proactively as **PDM:Trojan.Win32.Generic** with Behavior Detection.

MD5
afaf2d4ebb6dc47e79a955df5ad1fc8a
ba95a2f1f1f39a24687ebe3a7a7f7295

Piece of advice

Still, it is important for a company to have a security solution that would enable instant response to such ransomware threats in order to avoid large financial losses. Yanluowang was deployed in targeted human-operated attacks. As usual in such cases, we would like to remind you that a comprehensive cybersecurity strategy is required to protect against this type of threats.

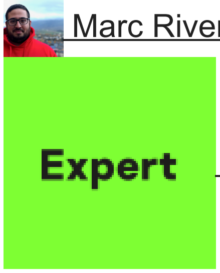
Here are Kaspersky’s recommendations for staying safe from ransomware attacks:

- Do not expose remote desktop services (such as RDP) to public networks unless absolutely necessary, and always use strong passwords.
- Promptly install available patches for commercial VPN solutions that provide access for remote employees and act as gateways to your network.
- Always keep software up to date on all your devices to prevent ransomware from exploiting vulnerabilities.

- Focus your defense strategy on detecting lateral movement and data exfiltration to the Internet. Pay special attention to outgoing traffic to detect cybercriminals' connections.
- Back up data regularly. Make sure you can quickly access your backups in an emergency.
- To protect the corporate environment, educate your employees. Dedicated training courses can help, such as the ones provided on Kaspersky Automated Security Awareness Platform.
- Use the latest Threat Intelligence information to stay on top of actual TTPs used by threat actors.
- Use solutions like Kaspersky Endpoint Detection and Response and Kaspersky Managed Detection and Response service which help to identify and stop an attack in the early stages, before attackers can achieve their objectives.
- Use a reliable endpoint security solution, such as Kaspersky Endpoint Security for Business, that is powered by exploit prevention, behavior detection and a remediation engine capable of rolling back malicious actions. KESB also has self-defense mechanisms that can prevent its removal by cybercriminals.

- Cybercrime
- Malware Technologies
- Ransomware
- Trojan

Authors

- Marc Rivero
- 

 Yanis Zinchenko

How to recover files encrypted by Yanluowang

Your email address will not be published. Required fields are marked *