Handy guide to a new Fivehands ransomware variant

research.nccgroup.com/2021/06/15/handy-guide-to-a-new-fivehands-ransomware-variant/

June 15, 2021

by **Michael Matthews** and **William Backhouse**

tl;dr

NCC Group's Incident Response team observed a new variant of the FiveHands ransomware, deployed by an affiliate leveraging publicly available tools to progress their attack. This blog post aims to describe the developments in the ransomware variant and the techniques used by the affiliate.

The affiliate appears to have been active for a long period of time. Open-source intelligence suggests a link to UNC2447, matching several characteristics shown through the campaign. Including aggressive tactics when urging the victim to pay the ransom. In this instance,

attempts were made to directly call individuals within the organisation using spoofed caller IDs.

Initial Access

An externally facing SonicWall VPN appliance was the initial access vector exploited by the actor, allowing them to generate a VPN profile and join the target network using the hostname “Commando”, which matches the default hostname of the complete Mandiant offensive VM. In addition, the source port of 4444 was used which is the default listener port for Metasploit.

```
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: command0
Account Domain: COMMANDO

Network Information:
Workstation Name: COMMANDO
Source Network Address: 10.X.X.X
Source Port: 4444

Network Information:
Workstation Name: COMMANDO
Source Network Address: 10.X.X.X
Source Port: 2360
```

Attackers Toolbox

Several publicly available tools were leveraged by the attacker, a brief description has been provided below detailing their functionality.

Netscan.exe

The SoftPerfect website states that the “SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices, via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), and PowerShell. It also scans for remote services, registry, files and performance counters; offers flexible filtering and display options and exports NetScan results to a variety of formats from XML to JSON.”

Advanced_port_Scanner.exe

The advanced port scanner website states that the “Advanced Port Scanner is a free network scanner allowing you to quickly find open ports on network computers and retrieve versions of programs running on the detected ports.”

Hostclean.exe

Preferring a GUI environment, the remote desktop software “Remote Utilities” was used to enact some level of persistent C2 with hosts connecting back to the master console which was an IP address based in Russia.

Reviewing the log files revealed the user account used to register the product: pau7887pau@yandex[.]ru. Open source research provides a link to Hybrid Analysis pointing towards a sample that was uploaded in July 2020, which turns out to be the remote desktop tool by Remote Utilities.

pCloud.exe

The pCloud website states that “pCloud is Europe’s most secure encrypted cloud storage, where you can store your personal files or backup your PC or share your business documents with your team”

pCloud was leveraged as the main data exfiltration method.

AllInOnePasswordRecoveryPro.exe

AllInOnePasswordRecoveryPro website states that “All-In-One Password Recovery Pro is the enterprise software to instantly recover ALL your lost or forgotten passwords from 100+ popular Windows Apps with a click of button. Long & short, it is the One software to recover your all type of passwords including website login, e-mail, messenger, FTP, download manager, remote desktop, database, router, credential manager, Wi-Fi passwords.”

PsExec.exe

PsExec.exe is the legitimate remote administration program by Sysinternals. This utility was used to remotely execute the encryptor.exe payload and create accounts.

Encryptor.exe

Encryptor.exe was the loader for the FiveHands ransomware. The loader was written in Go and took a 16-byte key over the command line using the “-key” switch to decrypt the payload, before loading the ransomware directly into memory. It is believed that the key is derived during the build process to generate a unique binary as part of RaaS.

As in most cases, where command line logging is not enabled, it was fortunate the actor used RDP extensively as the -key parameters were obtained through the bitmap cache. In short, the bitmap cache is a collection of small bitmap files that make up snippets of an RDP session. A large proportion of the key could be seen in the bitmap images available, the remaining characters obtained through brute forcing the key. The key is 16 characters long and is made up of upper- and lower-case characters with numbers. No symbols were present.

Passwords

A unique attribute of the affiliate was the use of the password “Remark123!”. Open source research throws up a link to the online sandbox “AnyRun” containing the following command executed “net localgroup Administrators gook /add” as part of “Update.exe”. Followed by adding the user to the Remote Desktop Users group, the favoured lateral movement technique for the actor.

The upload timestamp of 12/08/2020 paired with prior information suggests the actor has been active for quite some time, predating FiveHands involvement.

pCloud Data Exfiltration

Yet another internet cloud storage provider being used maliciously for data exfiltration, pCloud joins the list. Although a paid product, a free account will allow users to store up to 10GB of files. The operation of pCloud is similar to that of other cloud storage products such as Google Drive, managed both through an installed application or a web browser. The installed version provides a virtual disk which is used to sync files with the cloud.

Whilst pCloud syncs/uploads files from the host, the contents are cached locally on disk in the following location:

```
C:\Users\<Username>\AppData\local\pCloud\Cache\Cached
```

Using your favourite file carving tool, it is possible to recover the contents of files synced with the cloud. In turn revealing data exfil! A valuable outcome for most forensic investigators.

FiveHands Ransomware

The sample analysed has many similarities with what is already in the public domain however, the developers have added and changed parts of the code. For example, the target’s ID for the TOR ransomware page is not generated at runtime but it is hardcoded. We assess that this ransomware family operates under a Ransomware as a Service (RaaS) model.

Technical Analysis

The loader observed was written in Go, with the ransomware written in C++.

The entry point and the core functionality of the ransomware is stored in the export function ‘Run’. Despite the loader not passing any command line parameters, the ransomware supports the following:

Parameter	Description

-limit	Specify the maximum size of a file to encrypt
-skip	Specify the minimum size of files to encrypt
-blocks	Encrypt only the first block (163840 bytes at most) of a file
-full	Encrypt the entire file
-path	Encrypt only a specified path

The ransomware can encrypt the following resources:

- Network Shares
- Mounted Drives
- Specified File Paths (-path parameter)

Encryption Process

The ransomware sample uses a combination of RSA and AES algorithms in order to encrypt a file on the system. The implementations of the encryption algorithms are taken directly from the open-source library ‘Mbed TLS’.

Generally, the following steps are taken:

1. Generate a new AES-128 key (CBC mode) and encrypt a block (163840 bytes at most) of the target file

2. Store the AES key/IV and other metadata of the target file in a memory block and encrypt it using an embedded public RSA key (See Appendix section for a detailed description of the memory block)

3. If there is more data to encrypt in the target file then keep encrypting each block but with a new AES IV each time

4. Add the extension ‘.crypt’ to the encrypted file. The developers have also included the extension ‘).crypt’. This extension is only used if the use of ‘.crypt’ fails.

The above process is repeated for each target file. In case of a locked file, the ransomware attempts to unlock it via the ‘Windows Restart Manager’.

The ransomware excludes the following folders and extensions from the encryption process:

- programdata
- $recycle.bin
- program files
- windows
- all users

- winnt
- appdata
- application data
- local settings
- boot
- read_me_unlock.txt
- ntldr
- pagefile.sys
- ntdetect.com
- autoexec.bat
- desktop.ini
- autorun.inf
- ntuser.dat
- iconcache.db
- bootsect.bak
- boot.ini
- bootfont.bin
- config.sys
- io.sys
- msdos.sys
- ntuser.dat.log
- thumbs.db
- swapfile.sys
- .exe
- .dll
- .scr
- .sys
- .msi

Appendix

Public RSA Key

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlCzts7lbjf+KBhuz2GpB
is7X2oFE+gIUjQzwHzJvU06VSWT2YNtnqed3KlX7nKbrf4Ajso7CeyjzpK9maKYV
TsLrVm+zRWVWwyojOFKAhtMXR8d6G33bWaKOa0cNrh0OpIn/lWMoLVIAA1BztGk2
OZe7tlxT7FFLH5PaUdLUlXkcFHBDvnmk8beZXSEPufuDrsJAOSjfxVCXZuPBqMU2
2SlXtc1LIHY0O13JxWBmyjdqtYNl+AoBhyCM0jW8nlBVqfZlLx0+FBtp3lyWiCrh
dHnTCMn7c7B/ypISph3I6tIQs+Vt/glz+6q4rcZW3qKNjvDnff7dCi0MW9BRZSxX
GwIDAQAB
-----END PUBLIC KEY-----
```

Structures used in the encrypted block(s) of a target file

```
struct Encrypted_File_Block
{
 BYTE AES_Encrypted_File[N]; // Where N is the size of the encrypted block
 BYTE Encrypted_RSA_Block[0x60];
 DWORD Marker; // (0xABCCDCDB)
};

struct Encrypted_RSA_Block
{
  DWORD Marker; //0xBAADC0DE
  QWORD Size_of_encrypted_data;
  LPFILETIME lpCreationTime;
  LPFILETIME lpLastAccessTime;
  LPFILETIME lpLastWriteTime;
  DWORD Types_Of_Parameters; //Indicates what parameters that are passed.
  DWORD Maximum_Bytes_To_Encrypt_Per_Block; //Hardcoded to 0x00028000 (163840)
  DWORD Random_number; // Random generated number when the '-blocks' parameter is
passed. Otherwise, set to 0. Appears to have no use.
  DWORD Unknown; // Hardcoded to 3 when '-blocks' parameter is passed. Otherwise, set
to 0.
  QWORD Parsed_limits_parameter; // Parsed value of '-limits' parameter. 0x6400000 by
default
  DWORD Plaintext_Data_CRC32; // Checksum of the plaintext data
  BYTE AES_KEY[0x10]; //Generated AES KEY
  BYTE AES_IV[0x10]; // Generated AES IV
};
```

Indicators

Advanced Port Scanner

- 3477A173E2C1005A81D042802AB0F22CC12A4D55 (SHA1)
- 763499B37AACD317E7D2F512872F9ED719AACAE1 (SHA1)

FiveHands Encrypted Dropper

9A0FC9B53117ECDF78A899649C59F50C (MD5)

pCloud

- 8087F3C1F7F65E2CFC202550D3645000 (MD5)
- A6C8787815BC72DF7B0CFA6831157143 (MD5)
- 95425ACE5598941165025136AD52893D (MD5)
- pcloud[.]com

Remote Utilities

- 9E63911B5B7E63023708125418D6D4D5 (MD5)
- 1A426D873C1C6EA9D25747932F392E14 (MD5)
- B521ECCF21D13DCB062DDF39EF4BF351 (MD5)
- 185.175.47[.]32

- pau7887pau[at]yandex[.]ru
- Moderator.hldns[.]ru

SoftPerfect Network Scanner

132071DC69B875D239F133984655A26A (MD5)

MITRE ATT&CK

Tactic	Description
Initial Access	T1133 – External Remote Services
Execution	T1059.003 – Windows Command Shell
Persistence	T1136.002 – Create Account
Defence Evasion	T1562 – Impair DefencesT1070 – Indicator Removal on Host
Credential Access	T1003.001 – LSASS Memory
Discovery	T1046 – Network Service ScanningT1069.002 – Permission Groups Discovery
Lateral Movement	T1021.001 – Remote Desktop Protocol
Collection	T1039 – Data From Network Shared Drive
Command and Control	T1219 – Remote Access Software
Exfiltration	T1567.002 Exfiltration to Cloud Storage
Impact	T1486 – Data Encrypted for Impact