FiveHands Ransomware

us-cert.cisa.gov/ncas/analysis-reports/ar21-126a

Summary

This Analysis Report uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, Version 9. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of a recent successful cyberattack against an organization using a new ransomware variant, which CISA refers to as FiveHands. Threat actors used publicly available penetration testing and exploitation tools, FiveHands ransomware, and SombRAT remote access trojan (RAT), to steal information, obfuscate files, and demand a ransom from the victim organization. Additionally, the threat actors used publicly available tools for network discovery and credential access.

This report provides the tactics, techniques, and procedures the threat actors used in this attack as well as indicators of compromise (IOCs). It also includes CISA's recommended mitigations to protect networks from ransomware attacks and to detect—and respond to—these attacks.

Refer to Malware Analysis Report AR21-126B for full technical details and associated IOCs.

For a PDF copy of this report, click here.

Note: the analysis of FiveHands ransomware is ongoing; CISA will update this report as new information becomes available.

Description

Initial Access

The initial access vector was a zero-day vulnerability in a virtual private network (VPN) product (*Exploit Public-Facing Application* [T1190]).

Publicly Available Tool: SoftPerfect Network Scanner

The cyber actor used *SoftPerfect Network Scanner for Discovery* [TA0007] of hostnames and network services (*Network Service Scanning* [T1046]).

Details on the SoftPerfect Network Scanner artifacts are below.

netscan.exe

The `netscan.exe` artifact is a stand-alone version of the SoftPerfect Network Scanner, version 7.2.9 for 64-bit operating systems. 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."

The utility can also be used with Nmap for vulnerability scanning. The utility will generate a report of its findings called `netscan.xml`.

netscan.xml

The `netscan.xml` artifact is an Extensible Markup Language (XML) document reporting scanning results for the SoftPerfect Network Scanner program. The XML document indicates that a random scan was conducted to identify hostnames on a network and to search for:

- web servers,
- file servers,
- database servers, and
- any open Remote Desktop Protocol (RDP) ports for several subnets of unrouteable Internet Protocol (IP) addresses.

netscan.lic

A license is required to unlock all of the features of the SoftPerfect Network Scanner. The `netscan.lic` artifact is the Network Scanner license that was included with this submission. The license name is `DeltaFoX`.

FiveHands Ransomware

The malicious cyber actor used PsExec to execute `ServeManager.exe`, which CISA refers to as FiveHands ransomware (*Execution* [TA0002], *System Services: Service Execution* [T1569.002], *Impact* [TA0040]). FiveHands is a novel ransomware variant that uses a public key encryption scheme called `NTRUEncrypt`. **Note:** the NTRUEncrypt public key cryptosystem encryption algorithm (NTRU), is a lattice-based alternative to Rivest-Shamir-Adleman, known as RSA, and Elliptic-curve cryptography, or ECC, and is based on the shortest vector problem in a lattice.

To prevent data recovery, FiveHands uses WMI to first enumerate then delete Volume Shadow copies (*Inhibit System Recovery* [T1490]; *Windows Management Instrumentation* [T1047]). The malware also encrypts files in the recovery folder (*Data Encrypted for Impact* [T1486]). After the files are encrypted, the program will write a ransom note to each folder and directory on the system.

Details on the ransomware artifacts are below.

PsExec.exe

The `PsExec.exe` artifact is the legitimate remote administration program. This tool is part of Microsoft's Sysinternals tool suite. This utility was used to execute the program `ServeManager.exe` with the following arguments:

```
psexec.exe -d @comps.txt -s -relatime -c ServeManager.exe -key
```

The arguments are defined as follows:

`-d` --> Run psexec.exe without any prompts.

`@` --> Remotely access this list of hostnames/IP addresses.

`-s` --> Run the program with system level privileges.

`-relatime` --> This is a typo. This should be -realtime, or run this process before any other process.

`-c` --> Copy the program to the remote system before executing.

ServeManager.exe

The `ServeManager.exe` artifact is a 32-bit executable file that is executed using the Microsoft Sysinternals remote administration tool, `PsExec.exe`. When the program is executed it will attempt to load into memory a large embedded module that is decoded with a supplied key. The module is decoded in memory and checked to verify that it has a portable executable (PE) header. If the header is verified, the payload is executed.

The payload is a 32-bit executable file that is used to encrypt files on the victim's system to extort a ransom. When the ransomware is executed, it will enumerate files and folders on the system and encrypt files with the extensions, `.txt`, `.chm`, `.dat`, `.ocx`, `.js`, `.tlb`, `.vbs`, `.sys`, `.lnk`, `.xml`, `.jpg`, `.log`, `.zip`, `.htm`, `.ini`, `.gif`, `.html`, `.css`, and others (*File and Directory Discovery* [T1083]). Key system files are not encrypted.

To thwart the recovery of the data, the ransomware uses Windows Management Instrumentation (WMI) to enumerate Volume Shadow copies using the command `select * from Win32_ShadowCopy` and then deletes copies by ID (`Win32_ShadowCopy.ID`). The malware will also encrypt files in the recovery folder at `C:\Recovery`. After the files are encrypted the program will write a ransom note to each folder and directory on the system called `read_me_unlock.txt`.

Figure 1 displays the ransom note (redacted for privacy).

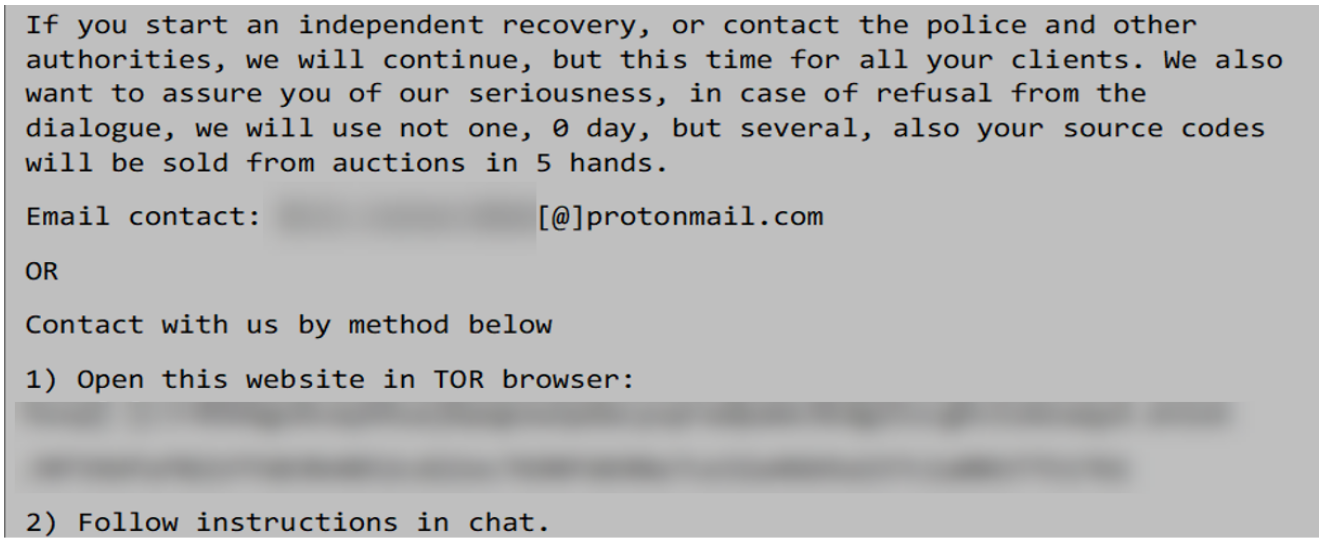

Figure 1: Ransom note

Remote Access Trojan: SombRAT

The threat actors used batch and text files to execute and invoke PowerShell scripts that decoded a SombRAT loader and enabled PowerShell to bypass the organization's anti-malware program (*Command and Scripting Interpreter: Windows Command Shell* [T1059.003], *Command and Scripting Interpreter: PowerShell* [T1059.001], *Defense Evasion* [TA0005]). SombRAT is a custom remote access Trojan (RAT) used to download and execute malicious payloads.[1]

The SombRAT loader recovered in this incident was a 64-bit variant that allowed the malicious actor to remotely download and load executable dynamic-link libraries (DLL) plugins on the affected system (*Ingress Tool Transfer* [T1105]). The loader used hardcoded public RSA keys for command and control (C2) sessions (*Command and Control* [TA0011]). The C2 communications were encrypted using Advanced Encryption Standard (AES), resulting in a Secure Sockets Layer tunnel with the threat actors (*Encrypted Channel: Asymmetric Cryptography* [T1573.002]).

Details on the SombRAT artifacts are below.

WwanSvc.bat

The `WwanSvc.bat` artifact is a batch file. When executed, it will invoke PowerShell, which decodes and executes a base64-encoded PowerShell script called `WwanSvc.txt` in the path `C:\ProgramData\Microsoft\WwanSvc\` (*Deobfuscate/Decode Files or Information* [T1140], *Obfuscated Files or Information* [T1027]).

WwanSvc.txt

The `WwanSvc.txt` artifact is a base64-encoded PowerShell script that is decoded and executed by `WwanSvc.bat`. The script allows PowerShell to run without system restrictions while bypassing the Microsoft anti-malware program. Next, the script decodes the file `WwanSvc.c` using a bitwise Exclusive OR (XOR) with a 256-byte key that is found in `WwanSvc.a`. Both `WwanSvc.a` and `WwanSvc.c` are located in `C:\ProgramData\Microsoft\`. The newly decoded script is then executed using the `InvokeExpression` command.

WwanSvc.a

The `WwanSvc.a` artifact contains a 256-byte key that is used by the base64-encoded script in `WwanSvc.txt` to decode a new PowerShell script in `WwanSvc.c`. The key is also used to decode the reflectively loaded payload in `WwanSvc.b`.

WwanSvc.c

The `WwanSvc.c` artifact is an XOR-encoded PowerSploit reflective loader program.[2] The program is decoded using the 256-byte key found in `WwanSvc.a`. The script will decode the content of `WwanSvc.b` and then check to confirm that it has a valid PE header. The script will also check the system environment for a 64-bit architecture (*System Information Discovery* [T1082]). The executable is not written to disk but loaded directly into memory.

WwanSvc.b

The `WwanSvc.b` artifact, when decoded, is a 64-bit variant of the SombRAT loader. The primary purpose of the loader is to allow a remote operator to securely download and load executable plugins on a target system. Given this plugin structure, the author can easily mold the RAT to provide additional functionalities and capabilities. The application contains the following two hardcoded public RSA keys, which it will utilize to secure its C2 sessions with the remote operator. Static analysis indicates that the C2 communications will also be encrypted using AES resulting in a secure Secure Sockets Layer (SSL) tunnel with the remote operator.

The configuration file `59fb3174bb34e803`, located in `C:\ProgramData`, contains the data the malware requires at runtime, including the operator-controlled remote C2 address. The malware decrypts this configuration file with the hardcoded AES key `ujnchdyfngtreaycnbjgi837157fncae`. See figure 2.

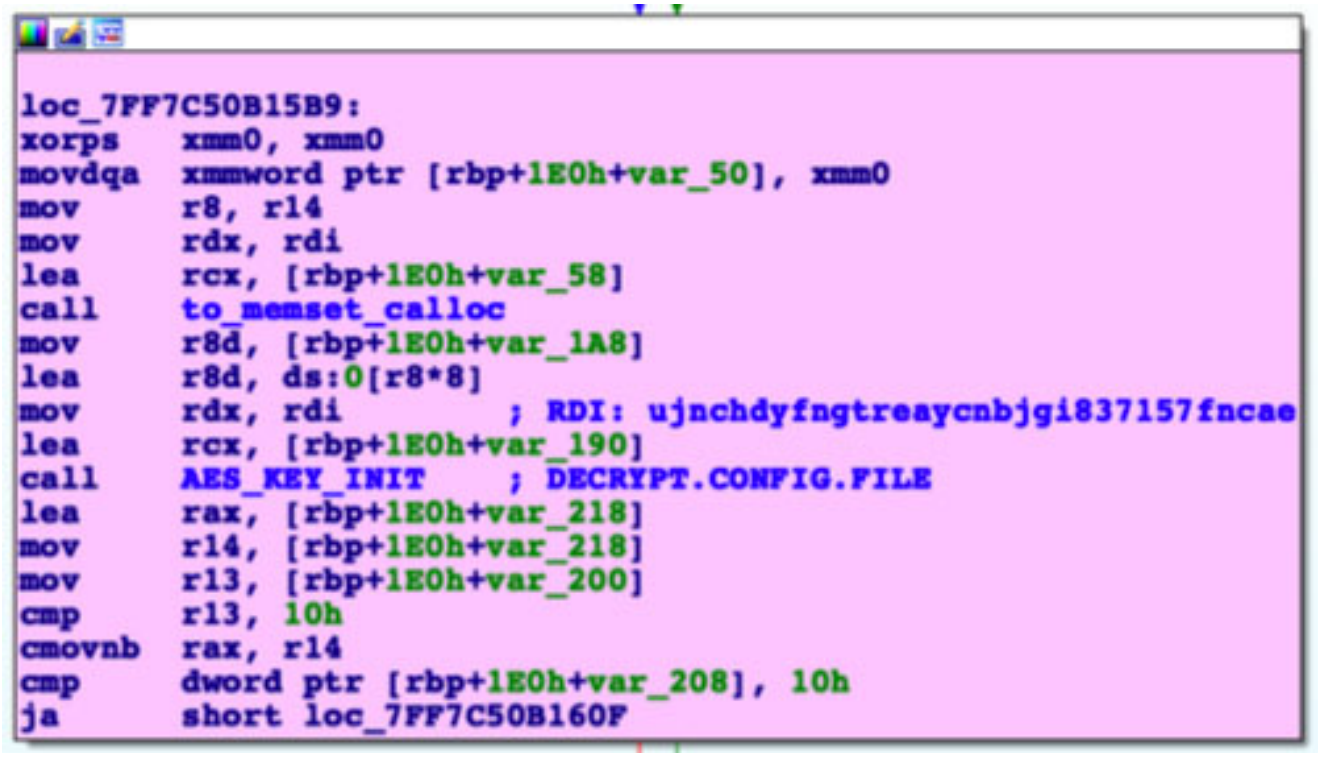

Figure 2: Hardcoded AES key

The malware contains numerous encoded strings, including the AES key used to decrypt the malware configuration file. The malware decrypts these strings by first XORing them with the first byte. The malware then decrypts the rest of the string by XORing it with the single byte XOR key `0xDE`.

This string can be decrypted by XORing the entire string with the value `0x78` and then XORing the result with `0xDE`.

The RAT provides most of its C2 capabilities to the remote operator by allowing the remote operator to securely transfer executable DLL plugins to the target system—via a protected SSL session—and load these plugins at will via the embedded plugin framework. The native malware itself does not provide much actual functionality to the operator without the code provided by the plugins. Some of the native functionality that the malware provides without the use of a plugin includes collecting system data—such as computer name, username, current process, operating system (OS) version, local system time, and the current process that the malware is masquerading as (*System Owner/User Discovery* [T1033], *Process Discovery* [T1057], *System Time Discovery* [T1124], *Masquerading* [T1036]). The program also contains native C2 capabilities allowing it to communicate with the remote operator using an embedded SOCKS proxy or via domain name system (DNS) tunneling (*Proxy* [T1090]).

The malware does contain hardcoded commands that it uses to evaluate against operator-provided data. These commands are encoded within the binary, and they are not encoded before being compared against operator-provided data—indicating the malware expects the

remote operator to encode the commands before passing them to the RAT.

The malware contains an encoded note, presumably designed for malware analysts who analyze the code. See figure 3.

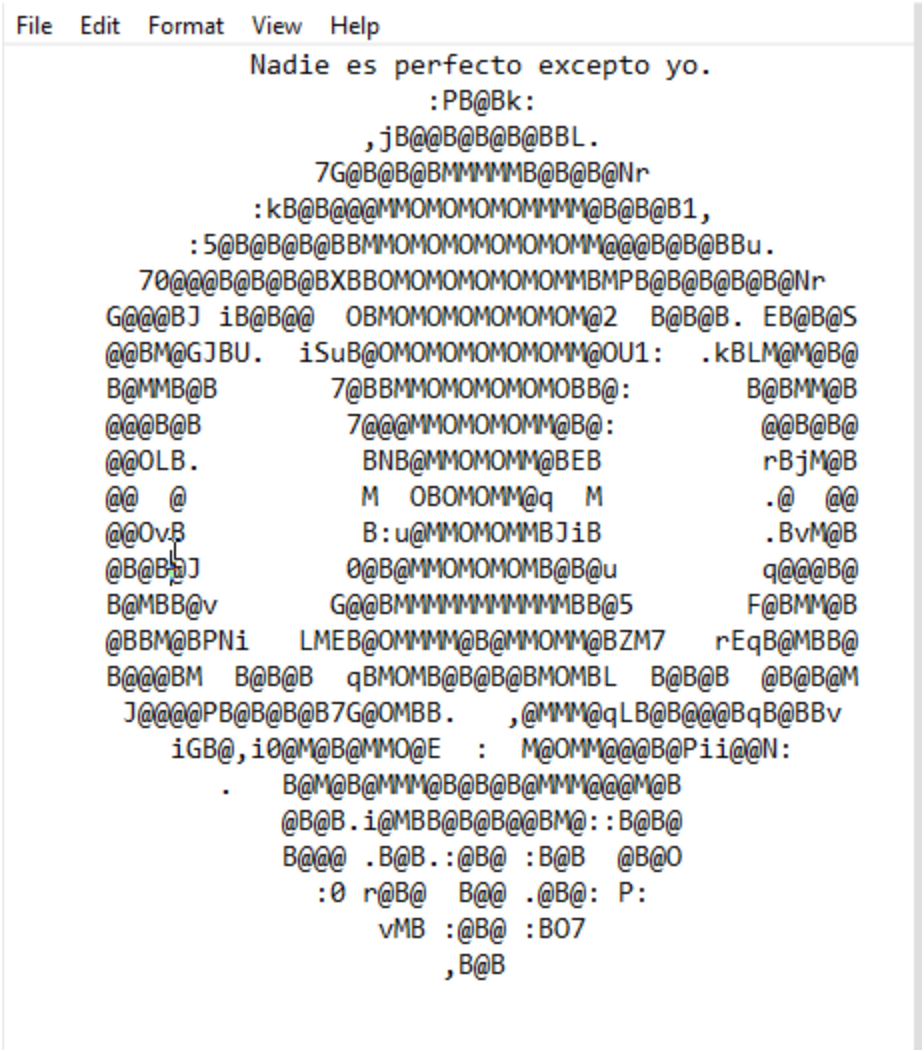

Figure 3: Encoded note

59fb3174bb34e803

The `59fb3174bb34e803` artifact is an encrypted configuration file that is read by the WwanSvc program. The configuration file contains the hardcoded domain, `feticost[.]com`. The program attempts DNS queries for this domain prepending a third level domain that consists of seven to nine random hexadecimal characters (e.g., `bb95058f1[.]feticost.com`).

The file `feticost[.]com` resolved to the IP address `51.89.50[.]152` at the time of analysis.

Publicly Available Tool: RouterScan.exe

The `RouterScan.exe` artifact is Router Scan v2.60 by Stas'M. This utility is used to identify network routers and proxy servers on a network (*Discovery* [TA0007]). The latest release of this program (v2.60) contains a list of common admin names and passwords that can be used for a dictionary attack to gain access to a network router (*Credential Access* [TA0006], *Brute Force: Password Guessing* [T1110.001]). The program also contains code to identify common vulnerabilities and leverage exploits against many popular routers (*Active Scanning: Vulnerability Scanning* [T1595.002]). The program can be customized to scan any subnet and any particular port, or protocol (*Network Service Scanning* [T1046]). The latest version also contains software to scan for wireless network access points (*System Network Connections Discovery* [T1049]).

To execute this program, two libraries are required: `librouter.dll` and `libeay32.dll`. Upon execution, the program will generate several telemetry files that are dropped in the current directory. These files are named `RouterScan.log`, `Config.ini`, `filter.txt`, `exclusions.txt`, `ports.txt`, and `ranges.txt`.

Open-Source Tool: grabff.exe

The `grabff.exe` artifact is a 32-bit .NET executable called grabff and is used for *Credential Access* [TA0006]. The program uses a command line interface to extract Firefox stored passwords and authentication information from the user's profile located at `C:\Users\<user>\AppData\Roaming\Mozilla\Firefox\Profiles` (*Command and Scripting Interpreter: Windows Command Shell* [T1059.003], Credentials from Password Stores: Credentials from Web Browsers [T1555.003]). The program will extract the password databases found in `key3.db`, `key4.db`, and `logins.json` as well as the SQLite-based certificate database, `cert9.db`. The data can be copied to any designated directory.

Open-Source Tool: rclone.exe

The `rclone.exe` artifact is an open-source cloud content management program called Rclone. The program uses a command line interface to manage files in cloud storage. The program is capable of uploading and downloading files, verifying file integrity, and providing file encryption. The program can use any of the following protocols: SSH File Transfer Protocol (SFTP), Web Distributed Authoring and Versioning (WebDAV), File Transfer Protocol (FTP), and Digital Living Network Alliance (DLNA).

s3browser-9-5-3.exe

The `s3browser-9-5-3.exe` artifact is the free version of the S3 Browser program used to upload and download data from a cloud account. The program can fully configure a cloud account, modify HTTP headers and object tags, enable multiple simultaneous uploads and downloads, and provide server-side encryption (*Create Account: Cloud Account* [T1136.003]). By default, the installed components of the program are stored in the path

`C:\Program Files\S3 Browser`. Activity logs are created on a daily basis and are stored in the path `C:\Users\<user>\AppData\Roaming\S3Browser\logs` in the format `s3browser-win32-YYYY-MM-DD-log.txt`.

Solution

Should your organization be a victim of ransomware, CISA strongly recommends responding by using the Ransomware Response Checklist located in the Joint Ransomware Guide, co-authored by CISA and the Multi-State Information Sharing and Analysis Center. The guide contains steps for detection and analysis as well as containment and eradication.

CISA recommends organizations implement the following practices to strengthen the security posture of their systems.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up to date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Implement multi-factor authentication (MFA), particularly on all VPN connections, external-facing services, and privileged accounts. Where MFA is not implemented, enforce a strong password policy and implement regular password changes.
- Decommission unused VPN servers, which may act as a point of entry for attackers.
- Monitor network traffic for unexpected and unapproved protocols, especially outbound to the internet (e.g., SSH, SMB, RDP).
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for—and remove—suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate access control lists (ACLs).

References

[1] BlackBerry ThreatVector Blog, The CostaRicto Campaign: Cyber-Espionage Outs…
[2] MITRE ATT&CK – PowerSploit

Revisions

May 6, 2021: Initial Version

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.