Connecting the Bots

The **Hancitor** downloader has been around for quite some time already. It is known since at least 2016 for dropping Pony and Vawtrak. As a loader, it has been used to download other malware families, such as Ficker stealer and NetSupport RAT, to compromised hosts. Its operators also showed interest in post exploitation activities, deploying Cobalt Strike Beacon on the hosts located in Active Directory environments. After a few unremarkable and quiet years, Hancitor resurfaced again — it decided to join the Big Game Hunting.

Hancitor became another commodity malware which partnered with ransomware gangs to help them gain initial access to target networks – the increasing trend outlined by Group-IB researchers in the recent Ransomware Uncovered 2020/2021 report.

Group-IB Threat Intelligence team found that Hancitor is being actively used by the threat actors to deploy Cuba ransomware. **Cuba ransomware** has been active since at least January 2020. Its operators have a DLS site, where they post exfiltrated data from their victims who refused to pay the ransom. As of April 28, the site mentioned nine companies primarily from aviation, financial, education and manufacturing industries. Hancitor's deep interest in Big Game Hunting is further supported by Jason Reaves's earlier findings about Hancitor's association with the Zeppelin ransomware.

The blog post examines a typical Hancitor and Cuba kill chain, the threat actors' TTPs, detailed recommendations, and mitigation techniques.

Usually, Hancitor is distributed via spam campaigns. Such emails are disguised to look like DocuSign notifications:

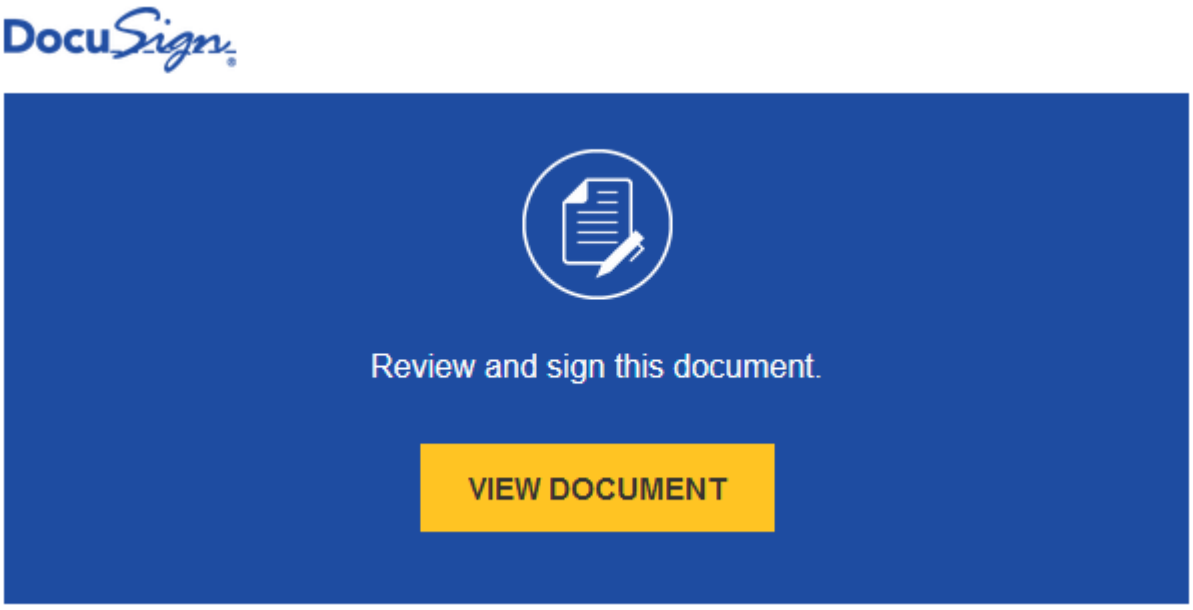

Figure 1. An example of spam email content

Clicking the malicious link obviously leads to downloading a weaponized document. As always, the document contains instructions on how to remove “protection”:

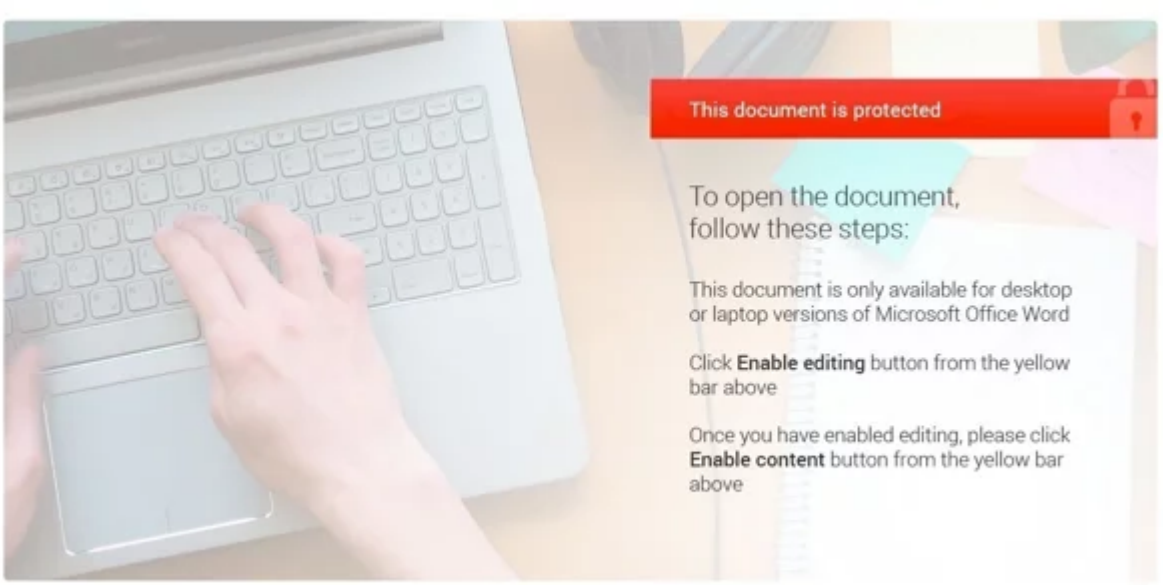

Figure 2. The contents of weaponized document

In recent campaigns, if the content is enabled, the macros extracts and drops Hancitor DLL to *C:\Users\%username%\AppData\Roaming\Microsoft\Word*, and runs it via *rundll32.exe*.

Such behavior is easy detectable by host-based defenses as winword.exe should not normally start *rundll32.exe*:

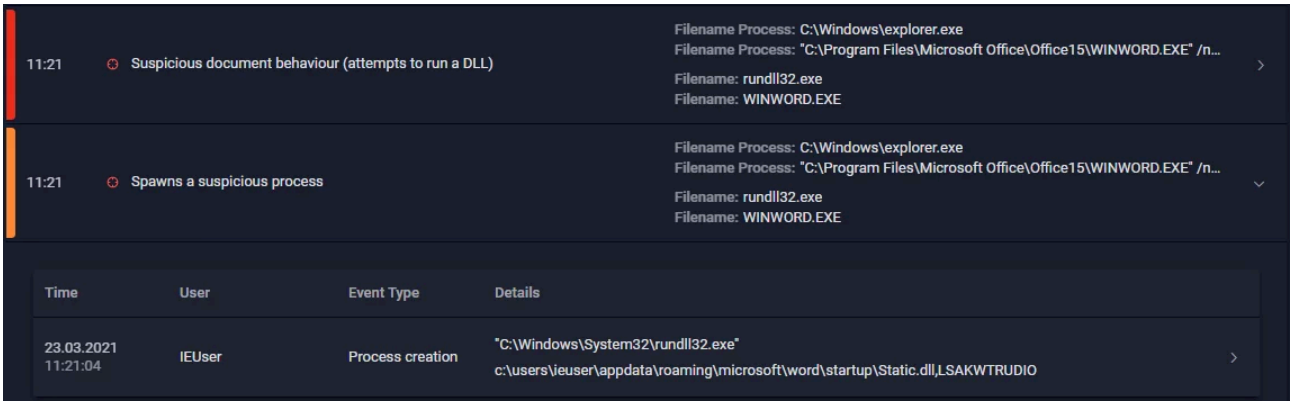

Figure 3. Group-IB Managed XDR Huntpoint detecting abnormal activity caused by Hancitor

Data received from C2 server is base64-encoded and XORed with 0x7A. After decoding and decrypting, the received command is checked. The command should be presented as one of the following symbols: «b», «e», «l», «n», «r». If it's supported, Hancitor does one of the following actions:

Command Code	**Description**
b	Downloads a PE from the server, which address was received from C2. Downloaded data is decrypted, decompressed and injected to newly started svchost.exe process.
e	Downloads a PE from the server, which address was received from C2. Downloaded data is decrypted, decompressed and executed in separate thread of the Hancitor process.
l	Downloads a PE from the server, which address was received from C2. Downloaded data is decrypted, decompressed and injected to newly started svchost.exe process via creation of the remote thread.
n	Looks like an equivalent of the ping command.
r	Download a PE from the server, which address was received from C2. Downloaded data is decrypted, decompressed and saved to a temporary file. If downloaded file is an EXE file, it is executed via CreateProcess, if downloaded file is a DLL file, it is executed via rundll32.exe.

One of the most common payloads delivered by Hancitor these days is Ficker stealer, which is actively advertised on various underground forums and is capable of extracting data from various web-browsers, mail clients, cryptocurrency wallets, etc. However, Cobalt Strike usage deserves more attention.

During the post-exploitation phase, the threat actors rely mostly on Cobalt Strike, leveraging its capabilities on various stages of attack lifecycle.

From execution perspective, just like many other ransomware operators, they used jump psexec and jump psexec_psh, and relied heavily on SMB Beacons, commonly using generic pipe names. In some cases, they also used less common techniques, such as WMI and WinRM to execute the Beacon stagers on remote hosts.

As Cobalt Strike has credential dumping capabilities, the threat actors leverage mimikatz's sekurlsa::logonpasswords. At the same time, in some cases they use a separate binary to run mimikatz on some hosts. This tool is also used for enabling lateral movement capability with obtained hashes and mimikatz's sekurlsa::pth.

The Beacon's capabilities were also used to scan the compromised network. In addition, the group leveraged some custom tools for network reconnaissance. The first tool is called Netping – it's a simple scanner capable of collecting information about alive hosts in the network and saving it into a text file, the other tool, Protoping, to collect information about available network shares. Built-in tools were also abused. For example, adversary used net view command to collect information about the hosts in the network and nltest utility to collect information about the compromised domain.

Besides Cobalt Strike's capabilities to run the Beacon stagers on remote hosts, the attackers used Remote Desktop Protocol to move laterally. They have a batch script called rdp.bat in their arsenal, which is used to enable RDP connections and add corresponding firewall rule on the target host. Similar scripts were observed to be used by ProLock and Egregor operators.

Ficker stealer wasn't the only publicly advertised tool in the threat actors' arsenal. Another tool, which is becoming more and more popular among various ransomware operators – SystemBC. Such additional backdoors allowed the attackers to download and execute additional payloads even if Cobalt Strike activity was detected and blocked.

The approach to ransomware deployment is quite trivial, but still effective. Like many others, the threat actors usually leveraged PsExec for deployment.

The exfiltrated data is published on a dedicated Cuba DLS (Data Leak Site).

As of April 28, the website offers to download data for free from 9 mainly US companies from the aviation, financial, education, manufacturing, and logistics companies which refused to pay the ransom. The actual number of victims is expected to be higher.

An interesting feature of the site is that it also includes the paid content section:

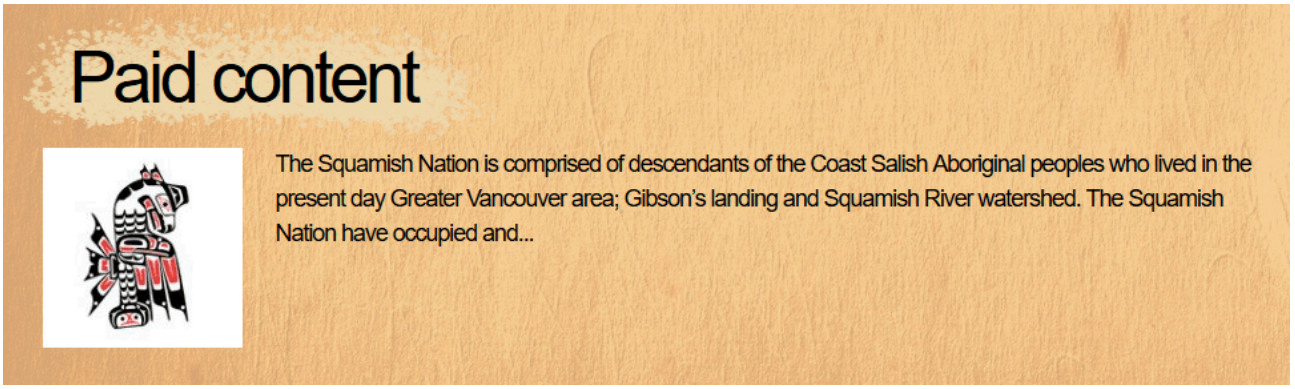

Figure 4. Paid content featured on Cuba's DLS

Cuba ransomware samples that Group-IB DFIR team observed wasn't very sophisticated, and even didn't have Windows Shadow Copies removing functionality, so the threat actors had to have additional scripting capabilities.

Files are encrypted using ChaCha20 with 12-bytes length IV. The keys are encrypted with RSA-4096 algorithm. The RSA implementation is likely copied from the following repository.

According to Group-IB TI&A, the group behind ransomware deployments is Balbesi. Despite the fact the group is leveraging quite common techniques in their operations, their attacks are still quite effective and affects organizations from various sectors, including financial, pharmaceutical, educational, industrial, professional services and software development, focusing mainly on Europe and USA.

Below you can find both MITRE ATT&CK mapping and corresponding mitigations list.

Hancitor fuels Cuba ransomware operations MITRE ATT&CK and MITRE Shield

GROUP-IB

Tactic	Technique	Mitigations	Group-IB Solutions
Initial Access	Phishing: Spearphishing Link (T1566.002)	Restrict Web-Based Content (M1021), User Training (M1017)	Threat Hunting Framework, Group-IB Education
Execution	Command and Scripting Interpreter: PowerShell (T1059.001)	Antivirus/Antimalware (M1049), Code Signing (M1045), Disable or Remove Feature or Program (M1042), Privileged Account Management (M1026)	Threat Hunting Framework
	Command and Scripting Interpreter: Windows Command Shell (T1059.003)	Execution Prevention (M1038)	
	User Execution: Malicious File (T1204.002)	Execution Prevention (M1038), User Training (M1017)	Threat Hunting Framework, Group-IB Education
	Windows Management Instrumentation (T1047)	Privileged Account Management (M1026), User Account Management (M1018)	Threat Hunting Framework
Defense Evasion	Process Injection (T1055)	Behavior Prevention on Endpoint (M1040), Privileged Account Management (M1026)	Threat Hunting Framework
	Access Token Manipulation (T1134)	Privileged Account Management (M1026), User Account Management (M1018)	
	Deobfuscate/Decode Files or Information (T1140)	-	
	Obfuscated Files or Information (T1027)	Antivirus/Antimalware (M1049)	
	Signed Binary Proxy Execution: Rundll32 (T1218.011)	Exploit Protection (M1050)	
	Valid Accounts (T1078)	Password Policies (M1072), Privileged Account Management (M1026)	
Credential Access	OS Credential Dumping (T1003)	Active Directory Configuration (M1015), Credential Access Protection (M1043), Operating System Configuration (M1028), Privileged Account Management (M1026), Privileged Process Integrity (M1025), User Training (M1017)	Threat Hunting Framework, Group-IB Education
Discovery	Account Discovery (T1087)	Operating System Configuration (M1028)	Threat Hunting Framework
	Domain Trust Discovery (T1482)	Audit (M1047), Network Segmentation (M1030)	
	Permission Groups Discovery (T1069)	-	
	Process Discovery (T1057)	-	
	Remote System Discovery (T1018)	-	
Lateral Movement	Lateral Tool Transfer (T1570)	Filter Network Traffic (M1037), Network Intrusion Prevention (M1031)	Threat Hunting Framework
	Remote Services: Remote Desktop Protocol (T1021.001)	Audit (M1047), Disable or Remove Feature or Program (M1042), Limit Access to Resource Over Network (M1035), Multi-factor Authentication (M1032), Network Segmentation (M1030), Operating System Configuration (M1028), Privileged Account Management (M1026), User Account Management (M1018)	
	Remote Services: SMB/Windows Admin Shares (T1021.002)	Filter Network Traffic (M1037), Limit Access to Resource Over Network (M1035), Password Policies (M1027), Privileged Account Management (M1026)	
	Remote Services: Windows Remote Management (T1021.006)	Disable or Remove Feature or Program (M1042), Network Segmentation (M1030), Privileged Account Management (M1026)	
	Use Alternate Authentication Material: Pass the Hash (T1550.002)	Privileged Account Management (M1026), Update Software (M1051), User Account Control (M1052), User Account Management (M1018)	
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	Network Intrusion Prevention (M1031)	Threat Hunting Framework
	Data Encoding (T1132)	Network Intrusion Prevention (M1031)	
	Encrypted Channel (T1573)	Network Intrusion Prevention (M1031), SSL/TLS Inspection (M1020)	
	Proxy (T1090)	Filter Network Traffic (M1037), Network Intrusion Prevention (M1031), SSL/TLS Inspection (M1020)	
Exfiltration Impact	Exfiltration Over C2 Channel (T1041)	Network Intrusion Prevention (M1031)	Threat Hunting Framework
	Data Encrypted for Impact (T1486)	Data Backup (M1053)	

Group-IB, 2021

Source: https://blog.group-ib.com/hancitor-cuba-ransomware