Crysis Threat Actor Installing Venus Ransomware Through RDP

asec.ahnlab.com/en/54937/

By Sanseo

July 3, 2023

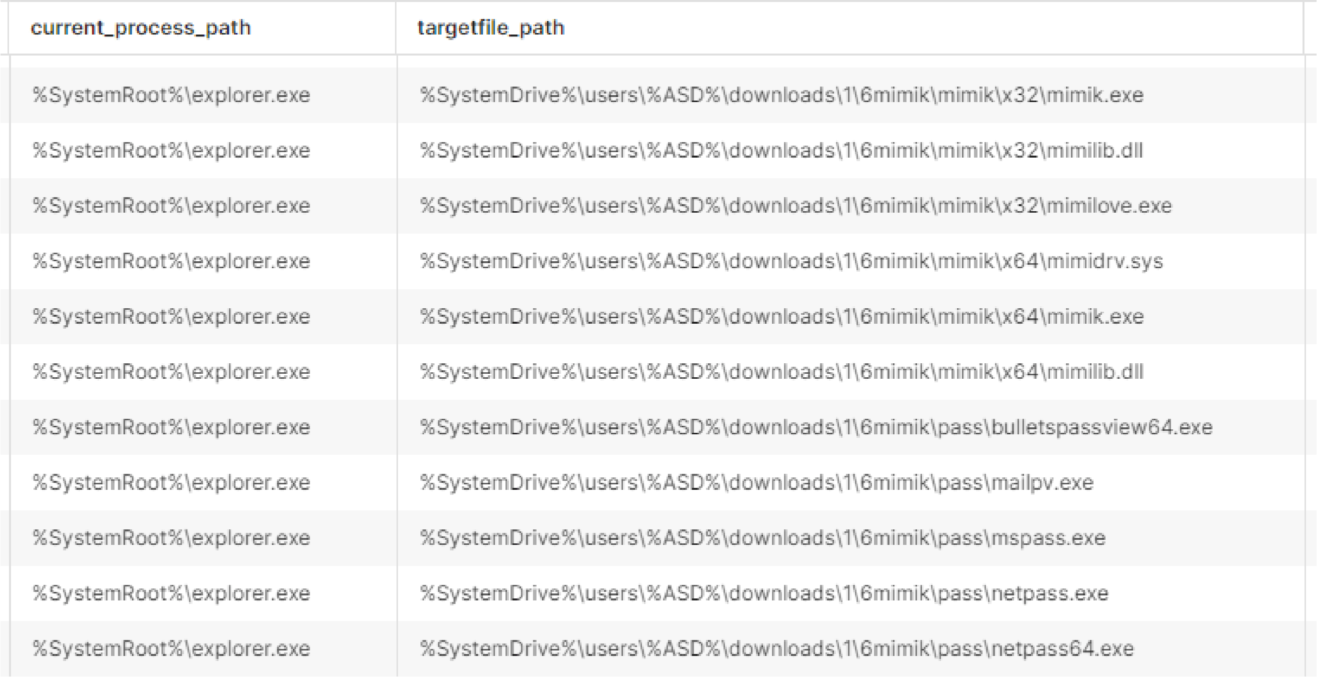
AhnLab Security Emergency response Center (ASEC) has recently discovered that the Crysis ransomware's threat actor is also using the Venus ransomware in the attacks. Crysis and Venus are both major ransomware types known to target externally exposed remote desktop services. **[1]** Actual logs from the AhnLab Smart Defense (ASD) infrastructure also show attacks being launched through RDP.

Aside from Crysis and Venus, the threat actor also installed a variety of other tools such as Port Scanner and Mimikatz. If the infected systems are turned out to be a company's internal network, the network can also become a target by such tools, and there are actual cases.

1. Installing Ransomware Using RDP

Threat actors who use RDP (Remote Desktop Protocol) as an attack vector generally scan for systems where RDP is active and allows external access. Systems found during this scanning process are subject to brute force or dictionary attacks. If a user has inappropriate account credentials, then threat actors can easily take those very credentials.

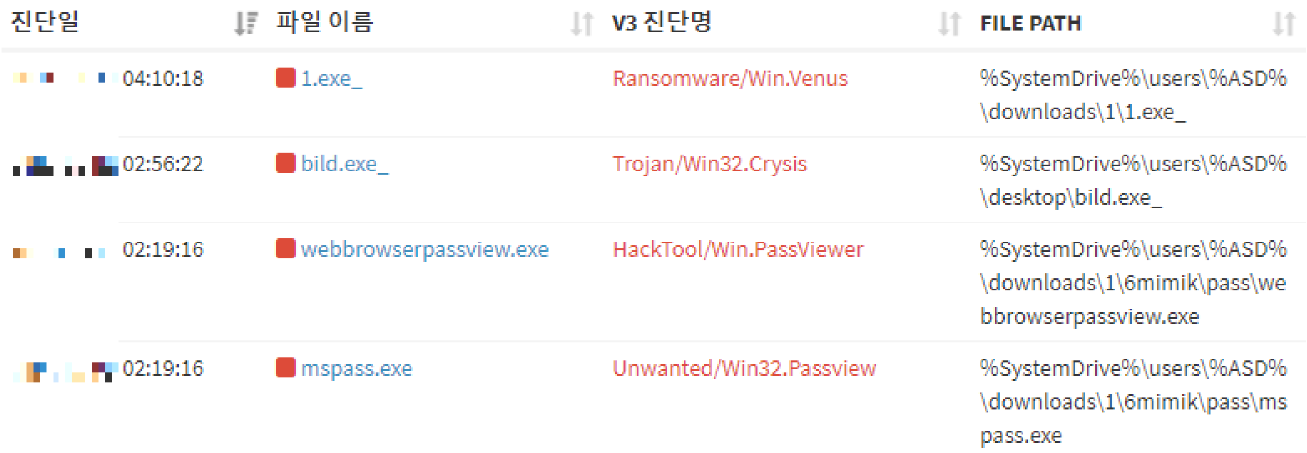
Threat actors can use the obtained account credentials to log in to the system through RDP, allowing them to gain control over the system in question and perform a variety of malicious actions. The threat actor who installed the Venus ransomware likely used RDP as the attack vector. This assumption is proved by the multiple malware types being generated by the Windows Explorer process (explorer.exe) as shown below.



current_process_path	targetfile_path
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\mimik\x32\mimik.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\mimik\x32\mimilib.dll
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\mimik\x32\mimilove.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\mimik\x64\mimidrv.sys
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\mimik\x64\mimik.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\mimik\x64\mimilib.dll
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\bulletspassview64.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\mailpv.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\mspass.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\netpass.exe
%SystemRoot%\explorer.exe	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\netpass64.exe

Figure 1. Installation log for various malware strains

In attacks identified in the past, the threat actor first attempted to encrypt the infected system using the Crysis ransomware, and after failing to do so, attempted encryption again using the Venus ransomware.



진단일	파일 이름	V3 진단명	FILE PATH
[redacted] 04:10:18	🟥 1.exe_	Ransomware/Win.Venus	%SystemDrive%\users\%ASD%\downloads\1\1.exe_
[redacted] 02:56:22	🟥 bild.exe_	Trojan/Win32.Crysis	%SystemDrive%\users\%ASD%\desktop\bild.exe_
[redacted] 02:19:16	🟥 webbrowserpassview.exe	HackTool/Win.PassViewer	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\webbrowserpassview.exe
[redacted] 02:19:16	🟥 mspass.exe	Unwanted/Win32.Passview	%SystemDrive%\users\%ASD%\downloads\1\6mimik\pass\mspass.exe

Figure 2. Crysis installed before Venus

Additionally, the threat actor used the same Crysis ransomware to continuously launch attacks against other systems. One of the identified attacks employed the same tactic of targeting an externally exposed RDP service. After the attack had succeeded, the attacker accessed other systems through RDP and infected them with Crysis.

2. Malware Used in the Attack Process

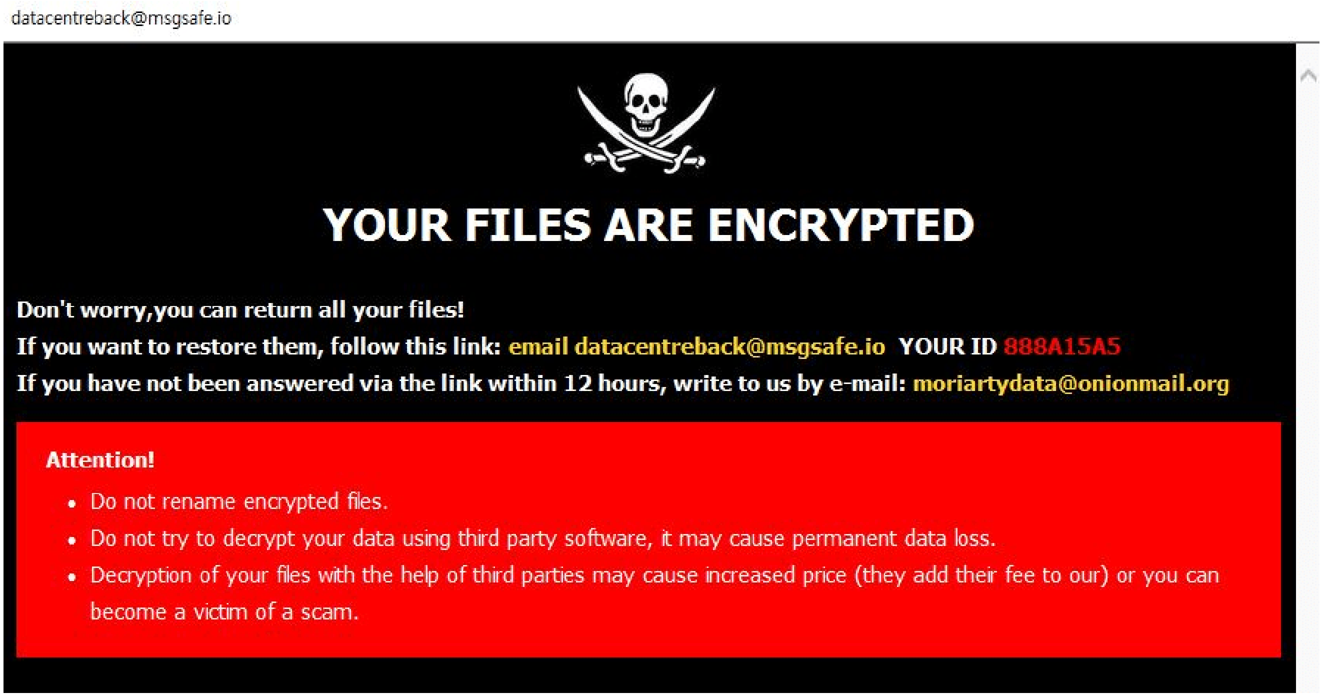
The threat actor installs various malware types in the infected system. Installed tools are scanners and account credential theft tools, most of them being created by NirSoft. It can be assumed through this that the network of the infected system can also be targeted.

File Name (Path Name)	Types
1.exe_	Venus Ransomware
bild.exe_	Crysis Ransomware
\mimik\x32\mimik.exe \mimik\x32\mimilib.dll \mimik\x64\mimik.exe \mimik\x64\mimilib.dll	Mimikatz
webbrowserpassview.exe	Web Browser Password Viewer – NirSoft
mailpv.exe	Mail PassView – NirSoft
vncpassview.exe	VNCPassView – NirSoft
wirelesskeyview64.exe	Wireless Key View – NirSoft
bulletspassview64.exe	BulletsPassView – NirSoft
routerpassview.exe	RouterPassView – NirSoft
mspass.exe	MessenPass (IM Password Recovery) – NirSoft
rdpv.exe	Remote Desktop PassView – NirSoft
netpass64.exe	Network Password Recovery – NirSoft
ns64.exe	Network Share Scanner

Table 1. Tools used in attacks

After the threat actor takes over the system via RDP, the above tools are used to scan the network to check if the infected system is part of a specific network. If the system is part of a specific network, then the ransomware can perform internal reconnaissance and collect account credentials in order to also encrypt the other systems on the network. Mimikatz can be used in this process. Using the collected account information, lateral movement can occur to other systems within the network. In an actual attack case involving Crysis, the threat actor used RDP for lateral movement into other systems within the network.

The threat actor ultimately executed Crysis to encrypt the system, and after recognizing failure after a few hours, retried the attack using Venus. If the Crysis ransomware ran correctly, the user would have seen the following ransom note.



datacentreback@msgsafe.io

YOUR FILES ARE ENCRYPTED

Don't worry,you can return all your files!
If you want to restore them, follow this link: email datacentreback@msgsafe.io YOUR ID 888A15A5
If you have not been answered via the link within 12 hours, write to us by e-mail: moriartydata@onionmail.org

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 3. The ransom note of Crysis ransomware used in the attacks

Threat actor’s email address: datacentreback@msgsafe[.]io, moriartydata@onionmail[.]org

3. Venus Ransomware

Among the files copied to the Download folder by the threat actor, Venus ransomware has the name bild.exe_.

Overview	Description
Extension	.venus
Paths excluded from encryption	“Tor Browser”, “Windows”, “dropbox”, “iexplorer”
Paths excluded from encryption	“venus”, “README.txt”, “README.html”
Ransom note	README.html
Processes for Termination	Refer to the information further below
Others	Deletes volume shadow copies

Table 2. Venus Ransomware overview

Venus first terminates various programs such as Office, email clients, and databases to encrypt more files.

List of Target Processes for Termination

List of Target Processes for Termination
agntsvc.exe, agntsvc.exe, agntsvc.exe, agntsvc.exe, dbeng50.exe, dbsnmp.exe, encsvc.exe, excel.exe, firefoxconfig.exe, infopath.exe, isqlplussvc.exe, msaccess.exe, msftesql.exe, mspub.exe, mydesktopqos.exe, mydesktopservice.exe, mysqld.exe, mysqld-nt.exe, mysqld-opt.exe, ocautoupds.exe, ocomm.exe, ocssd.exe, onenote.exe, oracle.exe, outlook.exe, powerpnt.exe, sqbcoreservice.exe, sqlagent.exe, sqlbrowser.exe, sqlservr.exe, sqlservr.exe, sqlwriter.exe, synctime.exe, tbirdconfig.exe, thebat64.exe, thunderbird.exe, winword.exe, wordpad.exe, xfssvccon.exe

Table 3. List of target processes for termination

An icon for the .venus file extension is registered before the encryption process begins. Because the encrypted files' file extensions are changed to .venus, users see the files with the following icon.

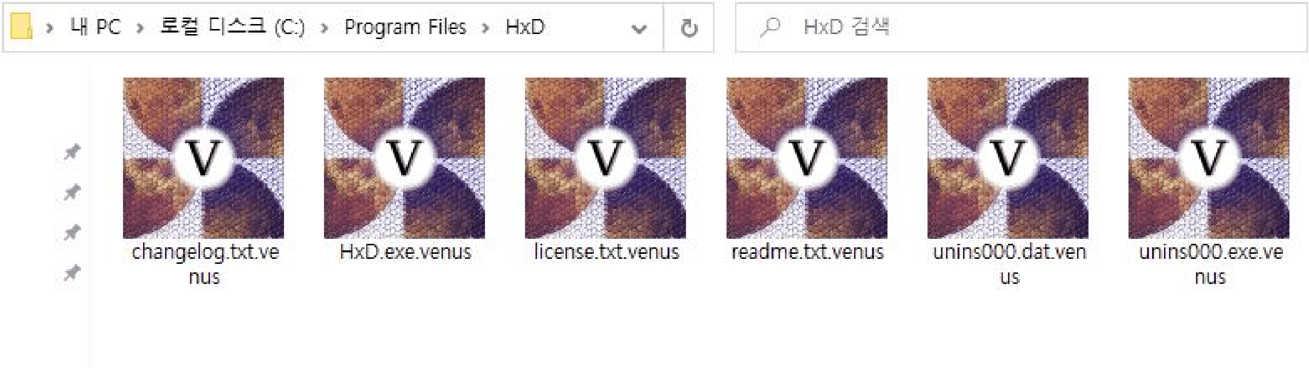


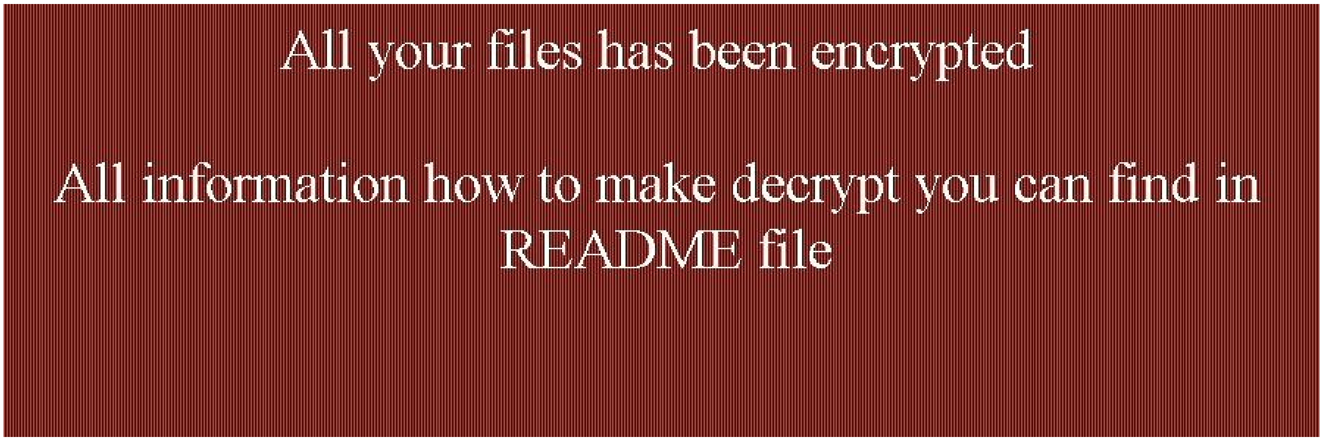
Figure 4. Encrypted files

The command used by Venus to delete volume shadow copies are as follows.

> cmd.exe /C wbadmin delete catalog -quiet && vssadmin.exe delete shadows /all /quiet && bcdedit.exe /set {current} nx AlwaysOff && wmic SHADOWCOPY DELETE

At this stage, the ransomware changes the desktop and displays the README file. The file contains a message saying that the threat actors had stolen information from the system and encrypted the files, urging the user to make contact within 48 hours.

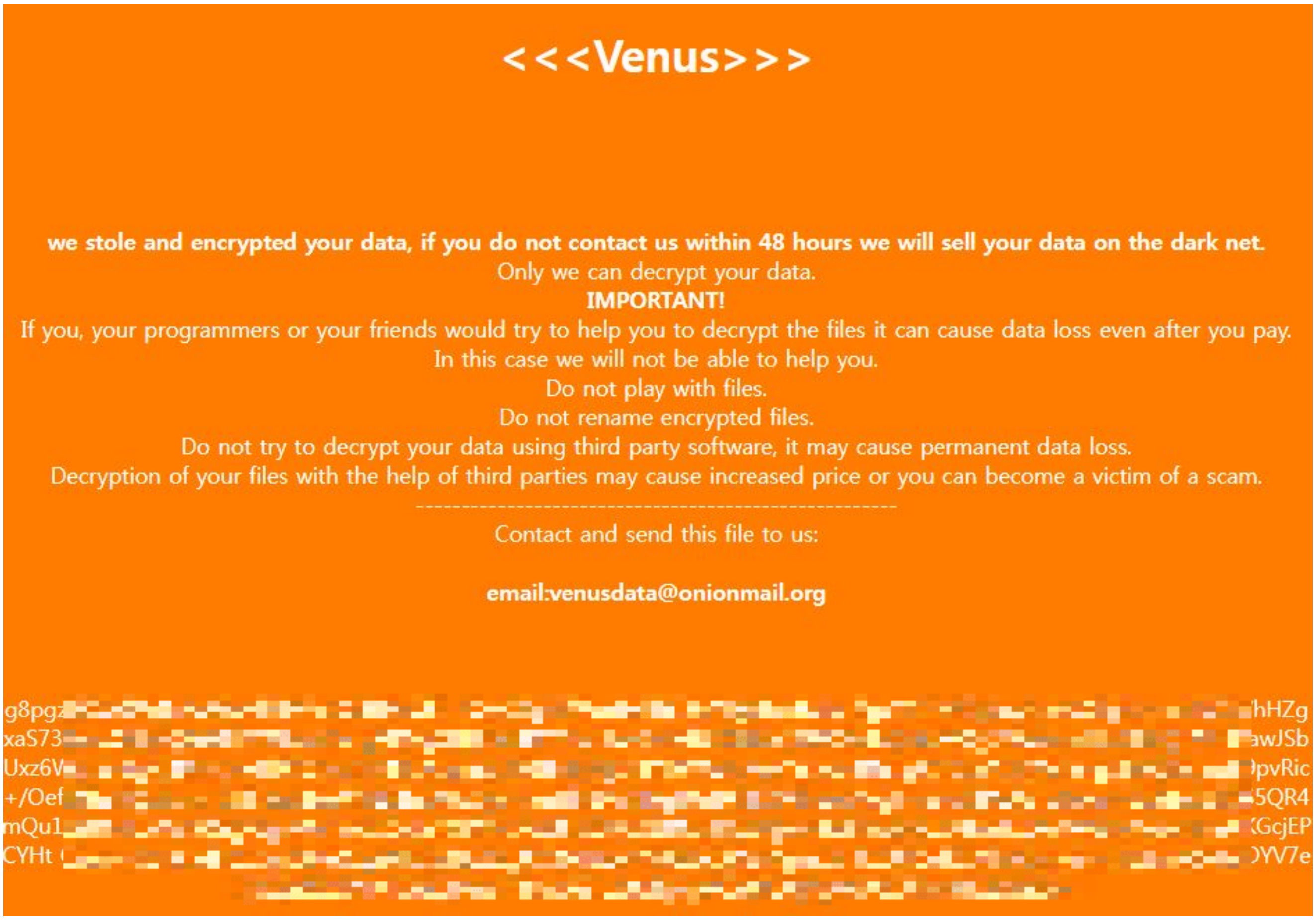
Threat actor's email address: venusdata@onionmail.org



All your files has been encrypted

All information how to make decrypt you can find in README file

Figure 5. Changed desktop



<<<Venus>>>

we stole and encrypted your data, if you do not contact us within 48 hours we will sell your data on the dark net.
Only we can decrypt your data.
IMPORTANT!
If you, your programmers or your friends would try to help you to decrypt the files it can cause data loss even after you pay.
In this case we will not be able to help you.
Do not play with files.
Do not rename encrypted files.
Do not try to decrypt your data using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price or you can become a victim of a scam.

Contact and send this file to us:

email:venusdata@onionmail.org

[redacted]

Figure 6. Venus ransom note

4. Conclusion

Attackers have continuously been using RDP from the past in the initial compromise and lateral movement processes. These attacks usually occur through brute force and dictionary attacks against systems with inappropriate account credentials. In particular, many ransomware operators use RDP as their main initial attack vector besides the Crysis threat actors in this Venus ransomware incident.

Users can deactivate RDP when not in use to decrease the number of attack attempts. If RDP is being used, it is advised to use a complex account password and to change it periodically to prevent brute force and dictionary attacks. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection
– Trojan/Win32.Crysis.R213980 (2018.11.23.00)
– HackTool/Win.PassViewer.C5353353 (2023.01.08.03)
– Ransomware/Win.Venus.C5220541 (2023.02.20.03)
– Trojan/Win64.Mimikatz.R348743 (2020.08.20.07)
– Trojan/Win32.RL_Mimikatz.R281240 (2019.07.14.00)
– Trojan/Win32.RL_Mimikatz.R364133 (2021.01.25.01)
– Trojan/Win.Mimikatz.R428853 (2021.07.02.01)
– HackTool/Win.Mailpassview.C5353346 (2023.01.08.03)
– HackTool/Win.PassViewer.C5353355 (2023.01.08.03)
– HackTool/Win64.WirelessKeyView.C3697346 (2020.05.21.06)
– HackTool/Win.PassViewer.C5353358 (2023.01.08.03)
– Unwanted/Win32.Agent.R266440 (2019.04.23.00)
– HackTool/Win.PSWTool.R345815 (2022.09.02.00)
– HackTool/Win.PassViewer.C5353351 (2023.01.08.03)
– Unwanted/Win32.HackTool.C613821 (2014.11.01.00)
– Unwanted/Win32.Passview.C568442 (2014.09.23.00)

Behavior Detection
– Ransom/MDP.Decoy.M1171
– Ransom/MDP.Command.M2255
– Ransom/MDP.Event.M1785

IOC
MD5
– 67b1a741e020284593a05bc4b1a3d218: Venus Ransomware (1.exe_)
– 786ce74458720ec55b824586d2e5666d: Crysis Ransomware (bild.exe_)
– 51373c09f0cb65ab149b0423d85f057e: Mimikatz (\mimik\x32\mimik.exe)
– 4984b907639851dfa8409e60c838e885: Mimikatz (\mimik\x32\mimilib.dll)
– 8d0a0f482090df08b986c7389c1401c2: Mimikatz (\mimik\x64\mimik.exe)
– 3a302cd820b1535ccc6545542bf987d1: Mimikatz (\mimik\x64\mimilib.dll)
– 57445041f7a1e57da92e858fc3efeabe : Web Browser Password Viewer (webbrowserpassview.exe)
– cc2d70a961bc6dce79168ae99ab30673 : Mail PassView (mailpv.exe)
– d28f0cfae377553fcb85918c29f4889b : VNCPassView (vncpassview.exe)
– 2a541cb2c47e26791bca8f7ef337fe38 : Wireless Key View (wirelesskeyview64.exe)
– 7f31636f9b74ab93a268f5a473066053 : BulletsPassView (bulletspassview64.exe)
– 3684fe7a1cfe5285f3f71d4ba84ffab2 : RouterPassView (routerpassview.exe)

– df218168bf83d26386dfd4ece7aef2d0 : MessenPass (mspass.exe)
– 44bd492dfb54107ebfe063fcbfbddff5 : Remote Desktop PassView (rdpv.exe)
– f627c30429d967082cdcf634aa735410 : Network Password Recovery (netpass64.exe)
– 597de376b1f80c06d501415dd973dcec : Network Share Scanner (ns64.exe)

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:Crysis,Ransomware,RDP,Venus