Not a dream job: Hunting for malicious job offers from an APT

Tldr: A recent Mandiant's blog described a series of targeted attacks over Whatsapp by an APT cluster named UNC4034. We found several additional cases in VirusTotal which we believe with high confidence are related to the same activity set.

According to the original publication, this activity is most likely related to North Korean actor and could be an extension of Operation "Dream Job", leveraging targeted distribution of malicious ISO files. Based on Mandiant's research, in the first stage the attacker sends a job offer at Amazon to the victim by email, followed by a WhatsApp web message where the attacker shares a malicious ISO file, pretending to be part of the selection process.

The original publication provides 2 hashes of ISO files named amazon_test.iso and amazon_assessment.iso respectively. Unfortunately, only the first one was found in VirusTotal:

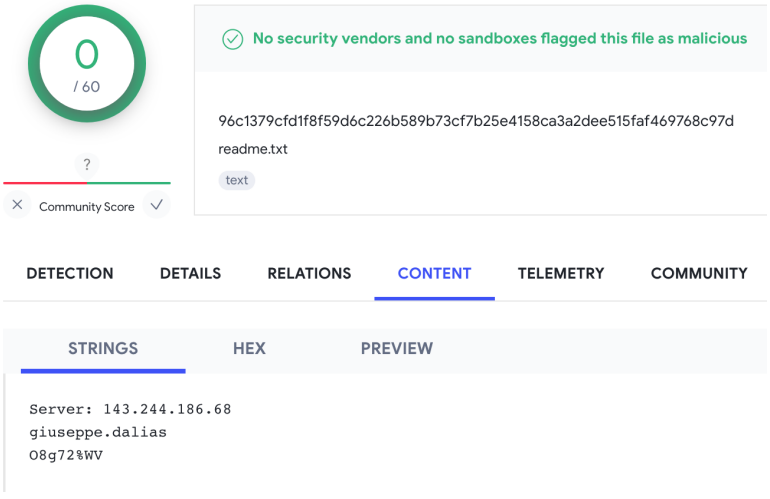
8cc60b628bded497b11dbc04facc7b5d7160294cbe521764df1a9ccb219bba6b
e03da0530a961a784fbba93154e9258776160e1394555d0752ac787f0182d3c0

Hunting for more samples

We started by trying to find the ISO we were missing in VirusTotal by searching for files with the same name:

name:"amazon_assessment.iso"

The search results provided us with one sample (dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031). In Mandiant's publication both samples share the same configuration which can be found in an embedded Readme.txt file. The new sample seems to be the new variant with a different configuration, also in a Readme.txt file, as shown below:



New sample's Readme.txt content

Both ISO files contain two files inside them - a Windows executable (apparently a poisoned version of Putty) and Readme.txt. We decided to search for all the ISO samples bundling only two specific files - Readme.txt and an *.exe file. Additionally, we filtered out all samples over 10Mb or submitted to VirusTotal before 2020. We obtained the following 6 samples, including the ones already discussed:

ISO sha256	Filename	ISO volume name
8cc60b628bded497b11dbc04facc7b5d7160294cbe521764df1a9ccb219bba6b	amazon_test.iso	AMAZON_TEST
dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031	Amazon_Assessment.iso	AMAZON_ASSESSMEI

ISO sha256	Filename	ISO volume name
3818527bc78efcece9d9bc87d77efa9450c2ba5c94f8441ea557ba29d865e7d3	SA_Assessment.iso	AMAZON_ASSESSMEI
cd8e12cddfe71b89597b6621d538b63673c8a8a3bf47a0fa572961ca1280e5b5	IT_Assessment.iso	AMAZON_ASSESSMEI
ccdb436a5941ba47a8b7e110021ad98ba6dc4e0296dc973429fc0c73de5e5397	Dell_SE_Assessment.iso	DELL_SE_ASSESSME
455a7ebf67aec7b4d6cc18ed930bde491c0327ba5e24968514dd9b3449a7c374	IBM_SSA_Assessment.iso	IBM_SSA_ASSESSME

Volume name (included in the ISO file metadata) can also be used as a pivoting point, as an alternative to the previous query, to find more samples in VirusTotal by clicking on them:

ExifTool File Metadata

MIMEType	application/x-iso9660-image
RootDirectoryCreateDate	1970:01:01 09:00:00+09:00
VolumeModifyDate	2022:06:17 18:14:36.00+09:00
VolumeBlockSize	2048
VolumeCreateDate	2022:06:17 18:14:36.00+09:00
VolumeName	AMAZON_TEST
VolumeBlockCount	1970
System	WIN32
VolumeSize	4.0 MB
FileTypeExtension	iso
FileType	ISO
Software	ULTRAISO V9.6 CD & DVD CREATOR, (C) EZB SYSTEMS, INC.

Example of ISO metadata

We could use the following query based on metadata that also filters out results based on the previous criteria:

metadata:ASSESSMENT tag:isoimage size:10mb-

Not only PuTTY

Although we didn't deeply analyze the found samples, we spotted two more remote client tools in addition to Putty inside the ISO files - a weaponized versions of TightVNC Viewer and KiTTY (PuTTY's fork).

ISO sha256	Filename
8cc60b628bded497b11dbc04facc7b5d7160294cbe521764df1a9ccb219bba6b	cf22964951352c62d553b228cf4d2d9efe1ccb51729
dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031	52ec2098ed37d4734a34baa66eb79ec21548b42b9
3818527bc78efcece9d9bc87d77efa9450c2ba5c94f8441ea557ba29d865e7d3	75771b5c57bc7f0d233839a610fa7a527e40dc51b2
cd8e12cddfe71b89597b6621d538b63673c8a8a3bf47a0fa572961ca1280e5b5	6af9af8aa0d8d4416c75e0e3f7a20dfe8af345fb5c5a
ccdb436a5941ba47a8b7e110021ad98ba6dc4e0296dc973429fc0c73de5e5397	14f736b7df6a35c29eaed82a47fc0a248684960aa8f
455a7ebf67aec7b4d6cc18ed930bde491c0327ba5e24968514dd9b3449a7c374	37e30dc2faaabaf93f0539ffbde032461ab63a2c242f

Interestingly, a couple of samples reveal forgotten pdb paths that could point to the attacker's environment:

Portable Executable Info

Debug Artifacts

Path	Z:\Work\Putty_Downloader\putty-src\windows\VS2012\x64\Release\putty.pdb
GUID	8d97ea00-e3c0-4920-8981-a019afecf797

PDB path reveals "Work" folder

A TightVNC sample also included the following pdb path:

N:\2.MyDevelopment\3.Tools_Development\4.TightVNCCustomize\Munna_Customize\tightvnc\x64\Release\tvnviewer.pdb

Also, in some cases attackers reused the same ISO details for different campaigns. For instance, they didn't change the volume name (Amazon related) with the ISO name they distributed (SA_Assessment or IT_Assessment).

Names

SA_Assessment.iso

ISO Image Info

file_structure_version	1
application_id	ULTRAISO V9.6 CD & DVD CREATOR, (C) EZB SYSTEMS, INC.
effective	0000-00-00 00:00:00
created	2022-09-01 18:46:27
total_size	3280963
expires	0000-00-00 00:00:00
modified	2022-09-01 18:46:27
min_date	2022-08-17 02:29:36
num_files	2
system_id	WIN32
max_date	2022-09-01 18:46:27
volume_id	AMAZON_ASSESSMENT
type_code	CD001

Infrastructure

We extracted all the IP addresses from the Readme.txt files, as well as the contacted hosts during sandbox execution.

ISO sha256	IP from Readme.txt	IP from Sandbox
8cc60b628bded497b11dbc04facc7b5d7160294cbe521764df1a9ccb219bba6b	137.184.15[.]189	-
dc20873b80f5cd3cf221ad5738f411323198fb83a608a8232504fd2567b14031	143.244.186[.]68	44.238.74[.]84
3818527bc78efcece9d9bc87d77efa9450c2ba5c94f8441ea557ba29d865e7d3	147.182.237[.]105	3.137.98[.]129
cd8e12cddfe71b89597b6621d538b63673c8a8a3bf47a0fa572961ca1280e5b5	137.184.15[.]189	172.93.201[.]253
ccdb436a5941ba47a8b7e110021ad98ba6dc4e0296dc973429fc0c73de5e5397	-	44.238.74[.]84
455a7ebf67aec7b4d6cc18ed930bde491c0327ba5e24968514dd9b3449a7c374	-	44.238.74[.]84

Please note these IPs are subject to double checking before adding them to any blocking list. By checking the VirusTotal IP report for any of them, you can find in the “Relations” tab the “Files Referring” section to obtain which files hardcode the IP address, and “Communicating Files” to get which files contacted the IP during sandbox execution:

Files Referring (3)

Scanned	Detections	Type	Name
2022-10-24	38 / 71	Win32 EXE	PuTTY
2022-09-22	13 / 60	ISO image	Amazon_Assessment.iso
2022-09-23	0 / 60	Text	readme.txt

Files with hardcoded 143.244.186[.]68

Conclusions

As a result of this quick research we identified additional samples that seem to be part of the same campaign described by Mandiant, in this case expanding the scheme behind its distribution to, apparently, Dell and IBM in addition to Amazon. Submissions of the identified samples are observed between June and September 2022.

In this post we described some ideas we used to identify these samples, but we encourage security researchers to both monitor additional activity and to dig into the newly found samples found to reveal further stage payloads. We

created a VirusTotal Collection including the indicators associated with this malicious activity. As always, we are happy to hear any additional ideas to hunt for malicious campaigns.

Happy hunting!