Second Wave of Shamoon 2 Attacks Identified

By Robert Falcone

Published: 2017-01-09 · Archived: 2026-04-05 16:21:39 UTC

In November 2016, we observed the reemergence of destructive attacks associated with the 2012 Shamoon attack campaign. We covered this attack in detail in our blog titled Shamoon 2: Return of the Disttrack Wiper, which targeted a single organization in Saudi Arabia and was set to wipe systems on November 17, 2016. Since our previous publication, we have found another, similar but different payload used to target a second organization in Saudi Arabia that was configured to wipe systems twelve days later on November 29, 2016. This latest attack potentially materially impacts one of the primary countermeasures employed against wiper attacks: Virtual Desktop Interface snapshots.

The payload used in this attack was very similar to the November 17, 2016 payload, but exhibited slightly different behaviors and contained hardcoded account credentials specific to the newly targeted organization. The hardcoded account credentials met Windows password complexity requirements, which suggests that the threat actors obtained the credentials through a previous, separate attack, similar to the November 17, 2016 attack.

The most notable thing about this latest sample is that it contains several usernames and passwords from official Huawei documentation related to their virtual desktop infrastructure (VDI) solutions, such as FusionCloud. VDI solutions can provide some protection against a destructive malware like Disttrack through the ability to load snapshots of wiped systems. The fact that the Shamoon attackers had these usernames and passwords may suggest that they intended on gaining access to these technologies at the targeted organization to increase the impact of their destructive attack. If true, this is a major development and organizations should consider adding additional safeguards in protecting the credentials related to their VDI deployment.

At this time, we have no details of the attack we believe preceded this Shamoon attack to obtain credentials. We also have no details on the delivery method used to deliver the new, similar, but different Disttrack payload in this attack.

The Second Shamoon 2 Attack

This second known attack associated with Shamoon 2 also used the Disttrack payload, albeit a new, similar but different one from the original Shamoon 2 attack. Specifically, it used a 64-bit variant that was configured to begin its destructive activities on November 29, 2016. Like the Disttrack sample used in the first reported Shamoon 2 attack, it including a wiper and communications module stored in resources within the executable.

Table 1 below shows that the method the Disttrack payload uses to extract and decrypt the modules from resources is the same; however, the resource names changed from “X509”, “PKCS7” and “PKCS12” to “LANG”, “MENU” and “ICO”.

Component	Resource Name	Offset	Size	Base64 key

Wiper	LANG	94399-14 = 94385	563712	OWRKbTxrleYfLm…
Communications	MENU	218709-14 = 218695	187904	QsCfQA6ze9CoOz…
Unknown	ICO	Unknown	Unknown	ijX7buB1FIjSn/0D…

Our efforts to decrypt the "ICO" resource have thus far been unsuccessful as the Disttrack payload has an associated key but does not contain code that decrypts and extracts this resource.

Propagation Inside Compromised Networks

Similar to the previous attack, the Disttrack payload in this attack spreads to other systems on the local network (/24 network specifically) by logging in using legitimate domain account credentials, copying itself to the system and creating a scheduled task that executes the copied payload. While this method is the same as discussed in our previous blog, the account credentials used in this attack were specific to the targeted organization and the file names used when copying the payload to remote systems were different.

Legitimate User Accounts

There were 16 account credentials found hardcoded within the Disttrack payload, appearing to be a mixture of individual user accounts and broader administrator accounts. All but one of the passwords met Windows complexity requirements, specifically, containing uppercase and lowercase characters, and either a number, symbol, or both. One of the general administrator accounts seen in this payload was also in the Disttrack payload in the first Shamoon 2 attack from November 17, 2016, which may not be specific to the targeted organization and instead used as an attempt to guess the login credentials. Based upon the existence of these credentials, it is highly likely the threat actors had carried out a previous attack to obtain these account credentials, as it is unlikely that these passwords were guessed or brute forced.

As noted earlier, a new development with this latest Disttrack payload is that several of the usernames and passwords are found within official documentation as administrator accounts for Huawei's virtualized desktop infrastructure (VDI) products, such as FusionCloud. This may suggest that the targeted organization used these credentials when deploying Huawei VDI systems. Shamoon actors may have obtained these credentials from a prior attack; however, it is also possible that the actors included these default usernames and passwords as an attempt to guess the login credentials to the VDI infrastructure.

VDI solutions can provide some protection against a destructive malware like Disttrack through the ability to load snapshots of wiped systems. Also, since FusionCloud systems run a Linux operating system, which would not be susceptible to wiping by the Windows-only Disttrack malware, this could be seen as a reasonable countermeasure against attacks like Shamoon. However, if the attacker was able to log into the VDI management interfaces using the account credentials they could manually carry out destructive activities against the VDI deployment, as well as any snapshots. The targeting of VDI solutions with legitimate, stolen or default credential represents an escalation in tactics that administrators should be aware of and take immediate steps to evaluate and address.

New Disttrack Names

The filenames that the payload copies itself to within the System32 folder of the remote system differs from the previously reported attack, specifically using “ntertmgr32.exe” for 32-bit or “ntertmgr64.exe” for 64-bit systems. The scheduled task executes these files on the remote system, which results in the creation of a Disttrack service named “NtertSrv” compared to the service name “ntssrv” created by the Disttrack payload used in the November 17, 2016 attacks. This can be seen in Figure 1.

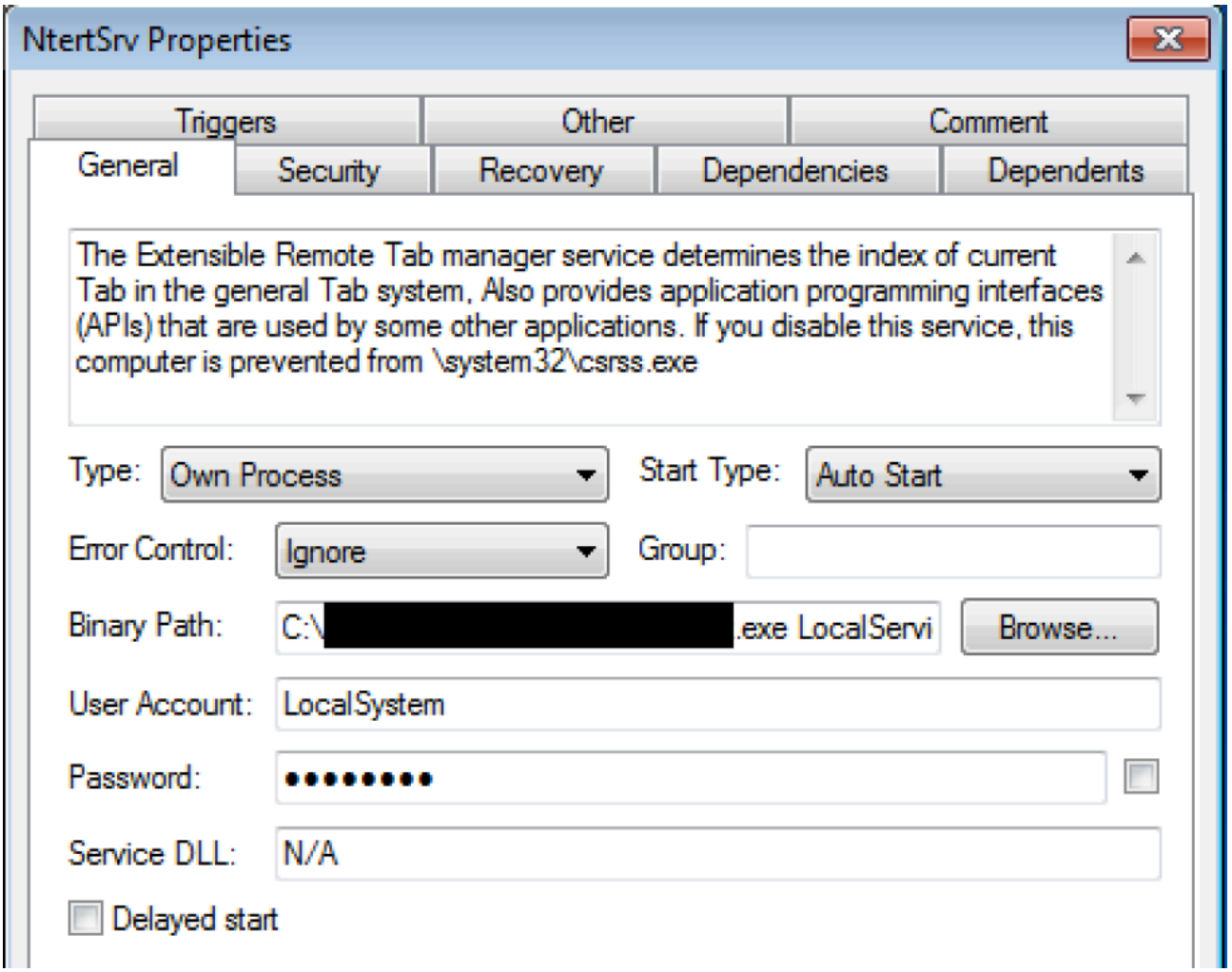

Figure 1 Disttrack service created on systems during propagation

Command and Control

The communications module used in this attack is rather hobbled, as it was configured without an operational command and control (C2) server to communicate with. The lack of an operational C2 is much like the November 17, 2016 attack that had the IP address “1.1.1.1” within its configuration to use as a C2 server. Unlike the non-operational C2 of “1.1.1.1” used in the first Shamoon 2 attack, this communications module completely lacked any IP address or domain name for a C2 server within its configuration.

Also, in this sample, Disttrack did not save its communications module to the system using the filename “netinit.exe” like in the original attack, rather it chose a random name from the following list:

• caiaw00e.exe
• sbuvideo.exe
• caiaw00i.exe
• olvume.exe
• usinwb2.exe
• briaw005.exe
• fpwwlwf.exe
• epiaw003.exe
• briaw002.exe
• olvsnap.exe
• dmwaudio.exe
• briaw006.exe
• miWApRpl.exe
• caiaw00b.exe
• lxiaw003.exe

Lastly, the communications module also uses different file names than the original Shamoon 2 attack. Instead of setting a custom "kill time" in a file named "usbvideo324.pnf" within the "%WINDOWS%\inf" folder, it uses a file name of "dcT21x400i.pnf". It also would send the C2 server the contents of a file named "vsfnp7_6.pnf" from the folder "%WINDOWS%\inf" instead of "netimm173.pnf".

Destruction

Much like the initial attacks, the lack of an operational C2 server suggests that the threat actor's sole intention for carrying out this Shamoon 2 attack was to destroy data and systems. Without an operational C2, the actor would be unable to issue a command to set a custom "kill time" when the Disttrack payload would begin wiping systems, which would force the payload to rely on its hardcoded "kill time". The hardcoded date suggests that this attack was set to begin wiping systems on November 29, 2016 at 1:30 AM local Saudi Arabia time.

Unlike the previous Shamoon attacks that occurred on a holiday and over a weekend, this kill time occurred during the work week, as November 29, 2016 was a Tuesday. However, it appears this attack attempted to maximize its impact by occurring very early in the morning before the majority of the organization's staff were on site. This aligns with the Shamoon actors conducting their attacks off-hours to increase the efficacy of the attack by increasing the timeframe of detection and response.

When Disttrack observes the system clock exceeding the "kill time", it will save its wiper component to the system using one of the following randomly chosen filenames:

• pdwmtphw.exe
• caiaw00a.exe
• sdwprint.exe
• caiaw00d.exe
• kyiaw002.exe
• sdwscdrv.exe

- briaw00a.exe
- saiaw002.exe
- _mvscdsc.exe
- hdvmp32.exe
- _s3wcap32.exe
- hpiaw001.exe
- lxiaw004.exe
- cniaw001.exe
- lxiaw006.exe
- caiaw00f.exe
- newtvsc.exe

When executed, the wiper component will extract a kernel driver from its resource section and decrypt it with a 172-byte XOR key. The wiper saves the kernel driver (SHA256: 5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a) to the "Windows\System32\Drivers" folder in a file named "vdsk911.sys". The wiper then uses this file to create a kernel driver service named "vdsk911", as seen in Figure 2.

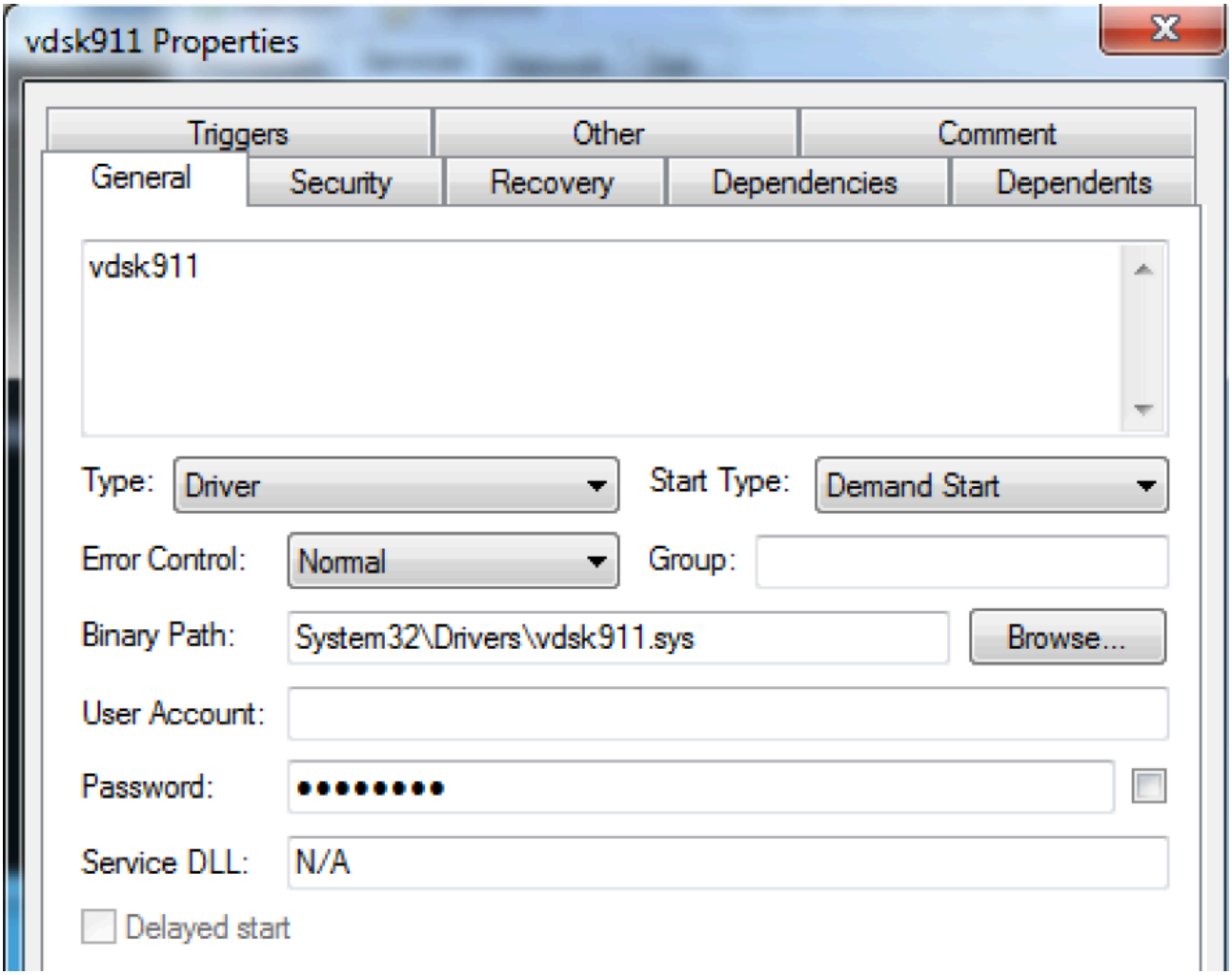

Figure 2 RawDisk kernel driver service created by Disttrack wiper

The kernel driver is the 64-bit version of the commercial RawDisk driver by EldoS Corporation, which is the exact same file as the "drdisk.sys" driver extracted from the Disttrack 64-bit payload in the 'X509' resource in the first reported Shamoon 2 attack. The Disttrack payload will use this kernel driver to access the master boot record (MBR), partition tables and files and folders on the system to overwrite them with the same image of the deceased Syrian boy as in the previous Shamoon 2 attack.

During our analysis, we again observed the wiper setting the system time to a random date between August 1 and August 20, 2012, as seen in Figure 3. As mentioned in our previous blog, the reason the wiper sets the system time to this random date in August 2012 is due to a temporary license key needed to use the RawDisk kernel driver. The temporary license key used in this attack is the exact same as the first attack.

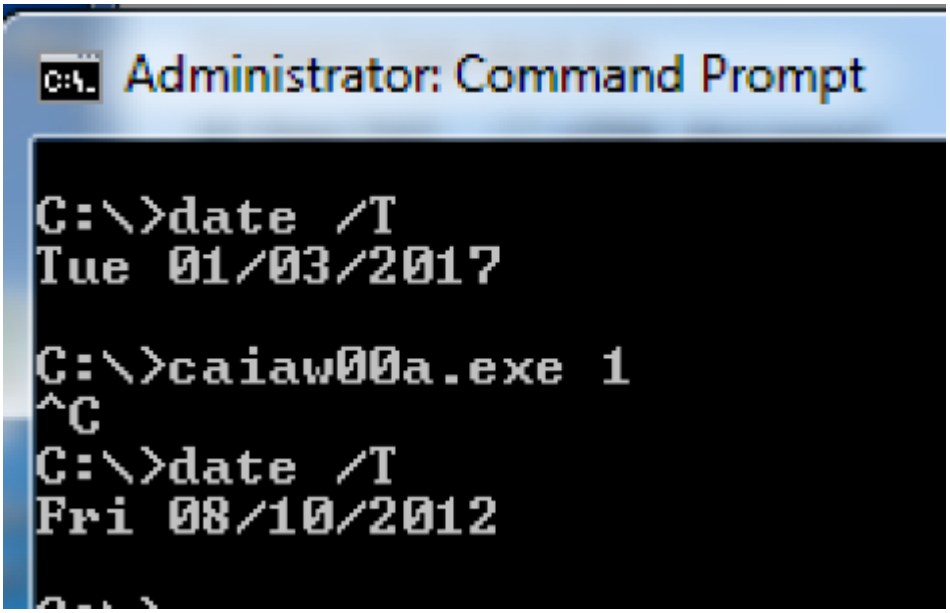

Figure 3 Wiper changing the system date to a random date in August 2012

Since our original blog, we've successfully decrypted the license key, which can be seen in Figure 4. The expiration date in the temporary license key is an 8-byte field (highlighted by the orange box) that corresponds to Microsoft's FILETIME structure, which represents the number of 100-nanosecond intervals since January 1, 1601 (UTC). In the temporary license key used in all of the Shamoon related attacks, the expiration date was set to August 30, 2012 at 8:34:29 UTC, which is the reason the wiper sets the system time to a random day between August 1 and August 20, 2012. Also, we found that the temporary license key was registered to "binnatova@bsunanotechnology.com". We are unsure how this email address is involved with Shamoon, as it was likely compromised back in 2012 and used by the actor to obtain the temporary license for RawDisk.

Figure 4 RawDisk temporary license decrypted showing August 2012 expiration date

After the MBR, partition tables and files are overwritten, the wiper issues the command of "shutdown -r -f -t 2" to reboot the system, which is the same command as used in the first Shamoon 2 attack. Figure 5 shows the dialog box that pops up as a result of this command, which will be followed by a system reboot.

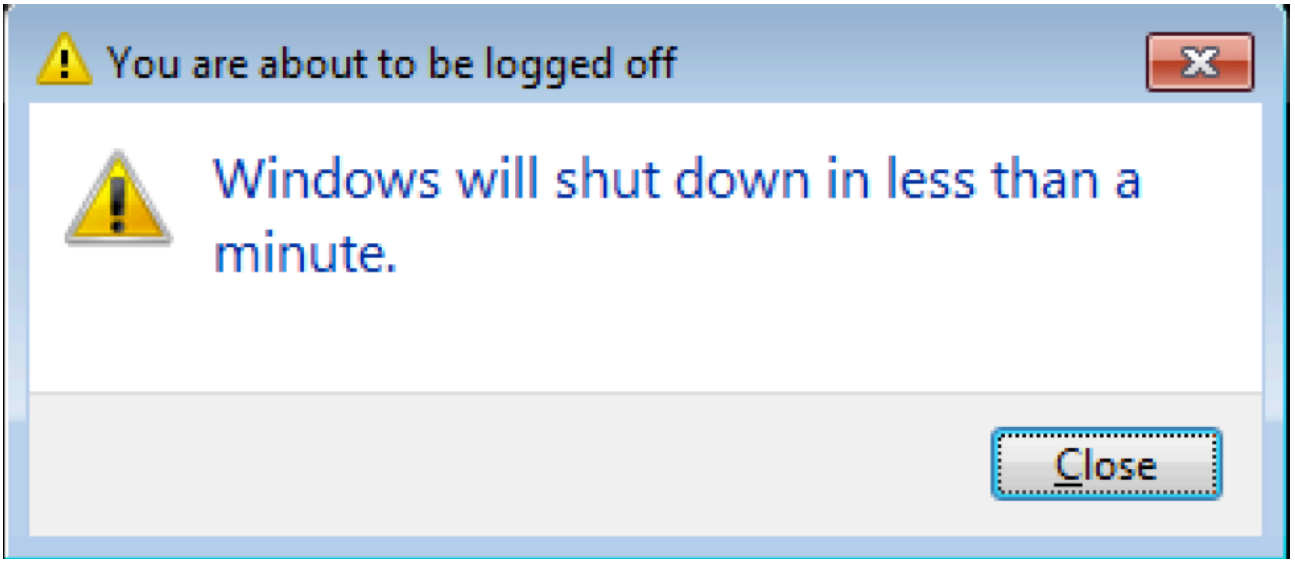

Figure 5 The shutdown dialog box opened just before reboot of a Windows 7 system wiped by Disttrack

The purpose of rebooting the system remains the same, as the portions of the hard disk and filesystem needed to successfully boot the system were overwritten with a JPEG image, the system is no longer able to start up. Figure 6 shows the result of this reboot in an analysis virtual machine, as the operating system could no longer be found.

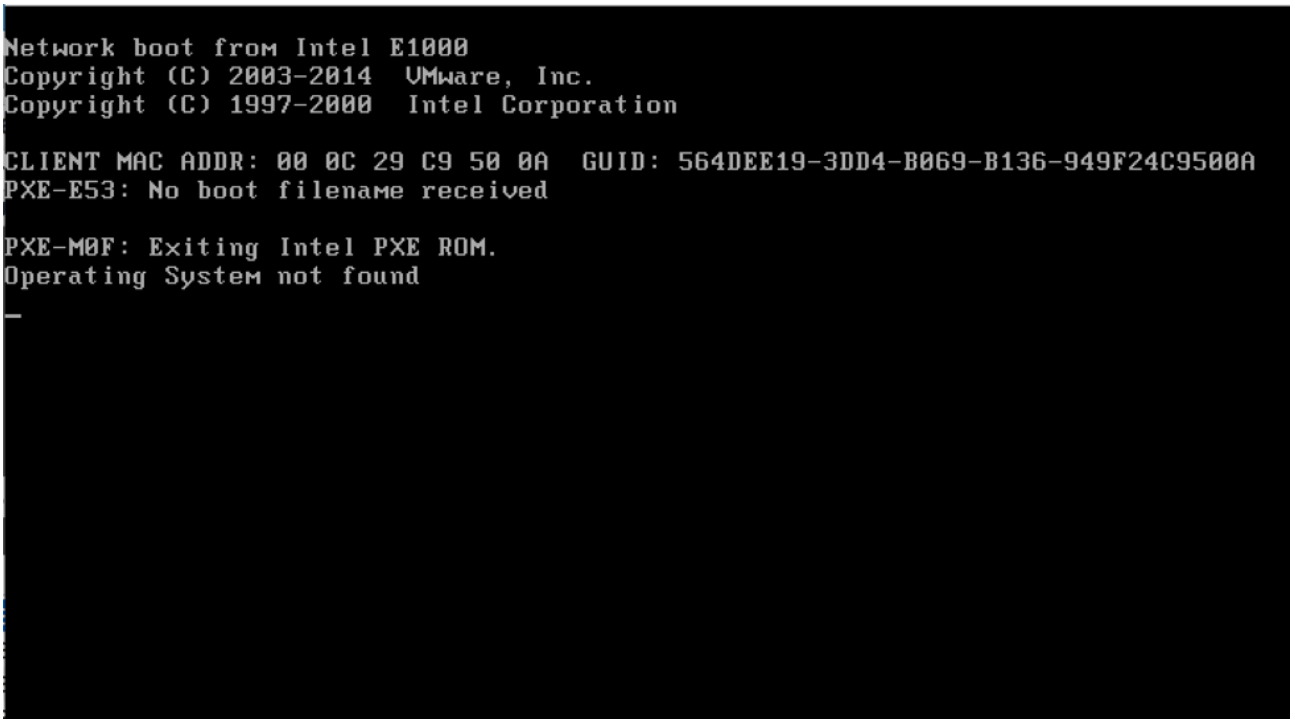

Figure 6 System unable to find its operating system

The operating system fails to load as the MBR is overwritten with a JPEG image. As seen in Figure 7, sector 0 of the physical hard disk, which normally stores the master boot record now contains the beginning of a JPEG file marked by the “JFIF” magic bytes in the two orange boxes.

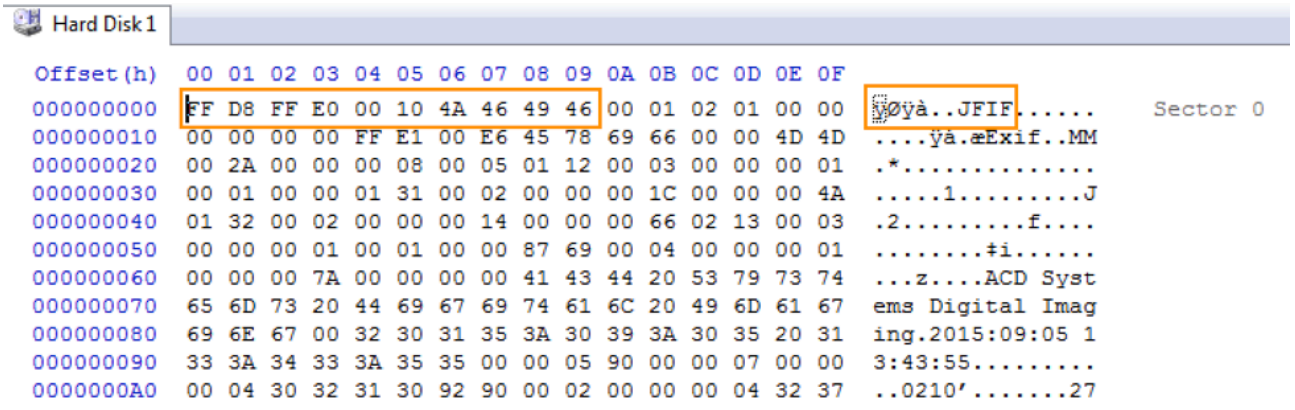

Figure 7 Hexdump of sector 0 of the physical showing the MBR overwritten with a JPEG file

Conclusion

We analyzed a second Disttrack payload associated with Shamoon 2, which suggests that the threat actors targeted a second Saudi Arabian organization in this attack campaign. The actors used the Disttrack payload to spread to other systems on the local network using legitimate credentials. The legitimate credentials were specific to the targeted organization and were complex enough to suggest that the threat actors carried out a previous attack to obtain the credentials. Also, the actors hardcoded credentials found in Huawei’s official documentation for its VDI solutions, suggesting that the threat actors may have had access to appliances hosting the infrastructure. The Disttrack wiper was set to begin overwriting systems on November 29, 2016 at 1:30 AM, which aligns with the

Shamoon actor's tactic to maximize its impact by attacking at a time when the targeted organization would have less staff and resources available onsite.

Palo Alto Networks customers are protected from the Disttrack payload used in this attack:

- WildFire properly classifies Disttrack samples as malicious
- Threat protection AV signature of Virus/Win32.WGeneric.ktoto detects the new payload.
- AutoFocus customers can monitor Disttrack activity using the Disttrack tag

Indicators of Compromise

Hashes

010d4517c81bcdc438cb36fdf612274498d08db19bba174462ecbede7d9ce6bb (64-bit Disttrack)
efd2f4c3fe4e9f2c9ac680a9c670cca378cef6b8776f2362ed278317bfb1fca8 (Communication)
113525c6bea55fa2a2c6cf406184092d743f9d099535923a12cdd9b9192009c4 (Wiper)
5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a (vdsk911.sys)

Filenames

ntertmgr32.exe
ntertmgr64.exe
vdsk911.sys
dcT21x400i.pnf
vsfnp7_6.pnf
caiaw00e.exe
sbuvideo.exe
caiaw00i.exe
olvume.exe
usinwb2.exe
briaw005.exe
fpwwlwf.exe
epiaw003.exe
briaw002.exe
olvsnap.exe
dmwaudio.exe
briaw006.exe
miWApRpl.exe
caiaw00b.exe
lxiaw003.exe
pdwmtphw.exe
caiaw00a.exe
sdwprint.exe
caiaw00d.exe
kyiaw002.exe

sdwscdrv.exe
briaw00a.exe
saiaw002.exe
_mvscdsc.exe
hdvmp32.exe
_s3wcap32.exe
hpiaw001.exe
lxiaw004.exe
cniaw001.exe
lxiaw006.exe
caiaw00f.exe
newtvsc.exe

Service Names

NtertSrv
vdsk911
