

Shamoon 3 Targets Oil and Gas Organization

By Robert Falcone

Published: 2018-12-13 · Archived: 2026-04-05 17:45:17 UTC

Summary

On December 10, a new variant of the Distrack malware was submitted to VirusTotal (SHA256:c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f) that shares a considerable amount of code with the Distrack malware used in the Shamoon 2 attacks in 2016 and 2017 that we previously published [here](#), [here](#), and [here](#). While we could not identify the impacted organization from the malware, today Saipem [disclosed](#) they were attacked. In previous attacks, we were able to determine the impacted organization based on the domain names and credentials used by the Distrack tool to spread to other systems on the network. However, that functionality was missing from this sample. Unlike past Shamoon attacks, this particular Distrack wiper would not overwrite files with an image. Instead it would overwrite the MBR, partitions, and files on the system with randomly generated data.

According to a [press release](#), Saipem confirmed that they experienced a cyberattack that involved a variant of the Shamoon malware. The attack caused infrastructure and data availability issues, forcing the organization to carry out restoration activities. Saipem told [Reuters](#) that 300 systems on their network were crippled by the malware related to the 2012 Shamoon attacks. While we cannot definitively confirm that Saipem was the impacted organization, the timing of this incident with the emergence of the Distrack sample discussed in this blog is quite coincidental.

Dropper

The sample submitted to VirusTotal is a Distrack dropper, which is responsible for installing a communications and wiper module to the system. The dropper is also responsible for spreading to other systems on the same local network, which it accomplishes by attempting to log into other systems on the network remotely using previously stolen usernames and passwords. Unfortunately, this particular sample does not contain any domains, usernames, or passwords to perform this spreading functionality, so this sample would only run on the system in which it was specifically executed.

The dropper has a hardcoded kill time of '12/7/17 23:51'; if the system date is after this date the dropper installs the wiper module and starts wiping files on the system. The dropper reads the '%WINDOWS%\inf\mdmnis5tQ1.pnf' file to obtain a custom kill date that it will use instead of the hardcoded time. The communications module installed by the dropper writes to this file, which will be discussed in a later section. The dropper also decrypts a string '\inf\averbh_noav.pnf' that is the other file that the communications module uses to write system information to and if the wiper was able to successfully wipe the system, but the dropper does not appear to use this file.

The dropper has three resources, two of which contain embedded modules, specifically a communications module and a wiper module. The third resource contains an x64 variant of the dropper, which it will use if the architecture of the system is determined to be x64. The resources have a language set to 'SUBLANG_ARABIC_YEMEN' that was also found in the previous Distrack samples used in Shamoon 2 attacks. The resource names are PIC, LNG, and MNU, which are slightly altered versions of the ICO, LANG, and MENU names found in previous samples.

The dropper extracts modules from these resources by seeking a specific offset and reading a specific number of bytes as the length of the ciphertext. The dropper then decrypts the ciphertext by using an XOR cipher and a specific base64 encode string that is decoded and used as the key. Before accessing the ciphertext, the dropper subtracts 14 from the specified offset, which is the same as previous Distrack samples delivered in Shamoon 2 attacks. Tables 1, 2, and 3 include the resources, the information used to extract them, and the resulting module.

Resource name	PIC
Description	x64 variant of Dropper
Base64 Key	2q9BQGHGVktPVIMZ6Nx17Njp4B5mHgj51hbybNlnRWsNIWniq6hOYvf5CksMXvPOyl/3dYKDn7ymSGIK0+I5KA8YC8dzkkAwn
Offset	8786-14
Length	983552
SHA256 of Cleartext	0975eb436fb4adb9077c8e99ea6d34746807bc83a228b17d321d14dfbbe80b03

Table 1 Resource containing the x64 variant of the Distrack dropper

Resource name	MNU
Description	Communications module
Base64 Key	U3JGgjnUDzWJEpOxzuwHjOijgav56cZatHh98dLbazGiBe7UMOCvdyCvU5/8mH1n7jUcMSIPFmqr7M671h5jradiKMn9M1sBdAmI
Offset	8601-14
Length	266752
SHA256 of Cleartext	0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe

Table 2 Resource containing the communications module in the Distrack dropper

Resource name	LNG
Description	Wiper module
Base64 Key	cb5F91PLTu1hN8oPgG2a6AQiJkphsXAmWFarsUoYEFo/BNgxF8Rj/hdzHxW/k/fLCZboSJRLnr9OH578lJyiSSdvz3uUaNA/vycy7ZJ
Offset	7892-14
Length	402432
SHA256 of Cleartext	391e7b90bf3f0bfeb2c2602cc65aa6be4dd1c01374b89c4a48425f2d22fe231c

Table 3 Resource containing the wiper module within the Distrack dropper

The dropper will install itself to the system (and remote systems if spreading was possible) by creating a service with the attributes listed in Table 4 below.

Service name	MaintenaceSrv
Service display name	Maintenace Host Service
Service description	The Maintenace Host service is hosted in the LSA process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process compl\x1d
Binary path	MaintenaceSrv32.exe or MaintenaceSrv64.exe

Table 4 Service created by the Distrack dropper

The dropper chooses a random name when installing the communication and wiper modules to the system. The communications module will have one of the following filenames with the 'exe' file extension:

- netnbrve
- prnod802
- netrdiscent
- netr142l
- mdmadccnt
- prnca00
- bth2bht_ibv32
- cxfalcon_ibL32
- mdmsupr30
- digitalmediadevicectl
- mdmetech2dmv
- netb57vxx
- winwsdprint
- prnkwy005
- composite005
- mdmar1_ibv32
- prnle444

- kscaptur_ibv32
- mdmzyxlga
- usbvideob
- input_ibv48
- prnok002_ibv
- averfx2swtvZ
- wpdmtp_ibv32
- mdmti_ibv32
- printupg_ibv32
- wiabr788

The wiper module will have one of the following filenames with the 'exe' file extension:

- _wialx002
- __wiaca00a
- tsprint_ibv
- acpipmi2z
- prnlx00ctl
- prngt6_4
- arcx6u0
- _tdibth
- prncaz90x
- mdmgcs_8
- mdmusrk1g5
- netbxndxlg2
- prnsv0_56
- af0038bdax
- averfix2h826d_noaverir
- megasasop
- hidirkbdmvs2
- vsmxraid
- mdamx_5560
- wiactn7001

Wiper

The wiper module (SHA256: 391e7b90bf3f0bfeb2c2602cc65aa6be4dd1c01374b89c4a48425f2d22fe231c) that the dropper writes to the system is responsible for overwriting the data within the MBR, partitions, and files on the system. The wiper carries out this wiping using a legitimate hard disk driver called RawDisk by EIDos. The wiper contains the EIDos RawDisk driver in a resource named 'e' that it extracts by skipping to offset 1984 and reading 27792 bytes from that offset. It then decrypts the data using aa 247-byte key and saves it to '%WINDOWS%\system32\hdv_725x.sys'. The wiper then creates a service named 'hdv_725x' for this driver using the following command line command and runs it with "sc start hdv_725x":

```
sc create hdv_725x type= kernel start= demand binpath= %WINDOWS%\system32\hdv_725x.sys
```

This wiper was configured using the 'R' flag, which generates a buffer of random bytes that it will use to overwrite the MBR, partitions and files. The sample supports two additional configuration flags as well, specifically 'F' and 'E' flags that will either overwrite files using a file or encrypt its contents.

The wiper could be configured to use a file to overwrite the files on the disk using the 'F' configuration flag, as we saw images used to overwrite files in previous Shamoon attacks. This file would be stored in a resource named 'GRANT', but this particular wiper is not configured to use a file for overwriting so the GRANT resource does not exist. If it were configured to use a file, this sample would extract the file using the information listed in Table 5.

Resource name	GRANT
Description	File to overwrite within Wiper module
Base64 Key	heocXOK4rDmQg4LRfiURi9wSOuSMwe0e69NfEpZLmyNixiUGYdEtpx/ZG3rMRN7GZlJ1/crQTz5Bf6W0xgkyYCwzD247FolCGA
Offset	71-14
Length	<unknown>
SHA256 of Cleartext	<unknown>

Table 5 Resource in wiper module that would contain file to use for overwriting data

This sample is also capable of being configured to import an RSA key to encrypt the MBR, partitions, and files via configuration flag 'E'. This sample was not configured to encrypt files, and the RSA key is empty in the wiper.

After completing this wiping functionality, the sample will reboot the system using the following command line, which will render it unusable when the system reboots as the important system locations and files have been overwritten with random data:

```
shutdown -r -f -t 2
```

Communications

The communications module (SHA256: 0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe) dropped by the Distrack dropper will use the following two supporting files:

%WINDOWS%\inf\mdmnis5tQ1.pnf - Used to set a wipe date for associated wiper module

%WINDOWS%\inf\averbh_noav.pnf - Used to mark successful wiping

The communications module is responsible for reaching out to hardcoded URLs to communicate with the C2 server, but like previous Distrack samples, this communication module does not contain functional C2 domains to use in the URLs. If it did, it would create a URL with a parameter named 'selection' followed by system information and the contents of the 'averbh_noav.pnf' file, as seen here:

```
[C2 URL, empty]?selection=[system info and contents of averbh_noav.pnf]
```

When communicating with the C2 URL, the communications module would use a User Agent of 'Mozilla/13.0 (MSIE 7.0; Windows NT 6.0)', which is the same as past Distrack communication module samples. Table 6 below show the two commands the C2 could respond with that the communications module could handle.

Command	Description
E	Reads base64 encoded file from the C2 server, runs 'del /f /a %TEMP%\Temp\reilopycb*.exe' to delete previously downloaded executables, runs 'mkdir %TEMP%\Temp\reilopycb] > nul 2>&1' to create a folder and saves the executale to a file named '[tick count].exe'. The Trojan then runs the downloaded executable %TEMP%\Temp\reilopycb[tick count].exe'
T	Opens the '\inf\mdmnis5tQ1.pnf' file and writes a supplied date to the file. The '\inf\mdmnis5tQ1.pnf' file is used by another associated module to this communications module that is responsible for wiping the system.

Table 6 Commands available within the communication module's command handler

Conclusion

The Distrack sample uploaded to VirusTotal is a variant of the samples used in the Shamoon 2 attacks in 2016 and 2017. The tool does not have the capability to spread to other systems on the local network. Instead it would have to be loaded onto and executed on the system that the actors intend to wipe. The wipe date of '12/7/2017' does not seem timely. However, this older date is still effective as the Distrack dropper will install and run the wiper module as long as the system date is after the wipe date. Unlike past Shamoon attacks, this particular Distrack wiper would not overwrite files with an image. Instead, it would overwrite the MBR, partitions and files on the system with random data. While we can't confirm this sample was used in the Saipem attack, it is likely at least related to it.

Palo Alto Networks customers are protected from this threat:

- WildFire detects all samples associated with this attack with malicious verdicts
- AutoFocus customers can track this attack and previous Shamoon attacks using the [Distrack](#)

Indicators of Compromise

- c3ab58b3154e5f5101ba74fccfd27a9ab445e41262cdf47e8cc3be7416a5904f - Distrack Dropper x86
- 0975eb436fb4adb9077c8e99ea6d34746807bc83a228b17d321d14dfbbe80b03 - Distrack Dropper x64
- 0694bdf9f08e4f4a09d13b7b5a68c0148ceb3fcc79442f4db2aa19dd23681afe - Distrack Comms module x86
- 391e7b90bf3f0bfeb2c2602cc65aa6be4dd1c01374b89c4a48425f2d22fe231c - Distrack Wiper module x86
- 6985ef5809d0789efff623cd2436534b818fd2843f09fa2de2b4a6e2c0e1a879 - EIDos RawDisk Driver x86
- ccb1209122085bed5b5ded3f923835a65d3cc1071f7e4ad52bc5cf42057dd2150 - Distrack Comms module x64

dab3308ab60d0d8acb3611bf364e81b63cfb6b4c1783864ebc515297e2297589 - Distrack Wiper module x64

bc4513e1ea20e11d00cfc6ce899836e4f18e4b5f5beee52e0ea9942adb78fc70 - EIDos RawDisk Driver x64

Source: <https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/>