

Home Products

Small Business 1-50 employees

Medium Business 51-999 employees

Enterprise 1000+ employees

**SECURELIST** by Kaspersky

CompanyAccount

Get In Touch

Dark mode

English

Solutions

Industries

Products

Services

Resource Center

About Us

GDPR

Content menu

Search...



Subscribe



# From Shamoon to StoneDrill

APT REPORTS

06 MAR 2017

4 minute read



Table of Contents



## Indicators of Compromise

Shamoon MD5s

StoneDrill MD5s

StoneDrill C2s

NewsBeef C2s

## // AUTHORS



COSTIN RAIU



MOHAMAD AMIN HASBINI

Expert

SERGEY BELOV



SERGEY MINEEV

## Wipers attacking Saudi organizations and beyond



[Download full report](#)

Beginning in November 2016, Kaspersky Lab observed a new wave of wiper attacks directed at multiple targets in the Middle East. The malware used in the new attacks was a variant of the infamous [Shamoon](#) worm that targeted Saudi Aramco and Rasgas back in 2012.

Dormant for four years, one of the most mysterious wipers in history has returned.

So far, we have observed three waves of attacks of the Shamoon 2.0 malware, activated on 17 November 2016, 29 November 2016 and 23 January 2017.


Also known as Disttrack, Shamoon is a highly destructive malware family that effectively wipes the victim machine. A group known as the *Cutting Sword of Justice* took credit for the Saudi Aramco attack by posting a Pastebin [message](#) on the day of the attack (back in 2012), and justified the attack as a measure against the Saudi monarchy.


The Shamoon 2.0 attacks seen in November 2016 targeted organizations in various critical and economic sectors in Saudi Arabia. Just like the previous variant, the Shamoon 2.0 wiper aims for the mass destruction of systems inside compromised organizations.


The new attacks share many similarities with the 2012 wave and now feature new tools and techniques. During the first stage, the attackers obtain administrator credentials for the victim's network. Next, they build a custom wiper (Shamoon 2.0) which leverages these credentials to spread widely inside the organization. Finally, on a predefined date, the wiper activates, rendering the infected machines completely inoperable. It should be noted that the final stages of the attacks are completely automated, without the need for communication with the command and control center.


While investigating the Shamoon 2.0 attacks, Kaspersky Lab also discovered a previously unknown wiper malware which appears to be targeting organizations in Saudi Arabia. We're calling this new wiper **StoneDrill**. StoneDrill has several "style" similarities to Shamoon, with multiple interesting factors and techniques to allow for the better evasion of detection. In addition to suspected Saudi targets, one victim of StoneDrill was observed on the Kaspersky Security Network (KSN) in Europe. This makes us believe the threat actor behind StoneDrill is expanding its wiping operations from the Middle East to Europe.


GREAT WEBINARS

13 MAY 2021, 1:00PM  
 **GReAT Ideas. Balalaika Edition**  
BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM  
 **GReAT Ideas. Green Tea Edition**  
JOHN HULTQUIST, BRIAN BARTHOLOMEW,  
SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK,  
YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM  
 **GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots**  
MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU,  
KURT BAUMGARTNER, DAN DEMETER,  
YAROSLAV SHMELEV

26 AUG 2020, 2:00PM  
 **GReAT Ideas. Powered by SAS: threat actors advance on new fronts**  
IVAN KWIATKOWSKI, MAHER YAMOUT,  
NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME,  
GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM  
 **GReAT Ideas. Powered by SAS: threat hunting and new techniques**  
DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,  
BRIAN BARTHOLOMEW, BORIS LARIN,  
ARIEL JUNGHEIT, FABIO ASSOLINI

To summarize some of the characteristics of the new wiper attacks, for both Shamoon and StoneDrill:

- Shamoon 2.0 includes a fully functional ransomware module, in addition to its common wiping functionality.
- Shamoon 2.0 has both 32-bit and 64-bit components.
- The Shamoon samples we analyzed in January 2017 do not implement any command and control (C&C) communication; previous ones included a basic C&C functionality that referenced local servers in the victim's network.
- StoneDrill makes heavy use of evasion techniques to avoid sandbox execution.
- While Shamoon embeds Arabic-Yemen resource language sections, StoneDrill embeds mostly Persian resource language sections. Of course, we do not exclude the possibility of false flags.
- StoneDrill does not use drivers during deployment (unlike Shamoon) but relies on memory injection of the wiping module into the victim's preferred browser.
- Several similarities exist between Shamoon and StoneDrill.
- Multiple similarities were found between StoneDrill and previously analysed NewsBeef [attacks](#).

We are releasing a full technical [report](#) that provides new insights into the Shamoon 2.0 and StoneDrill attacks, including:

- 1 The discovery techniques and strategies we used for Shamoon and StoneDrill.
- 2 Details on the ransomware functionality found in Shamoon 2.0. This functionality is currently inactive but could be used in future attacks.
- 3 Details on the newly found StoneDrill functions, including its destructive capabilities (even with limited user privileges).

#### FROM THE SAME AUTHORS

**Finding a needle in a haystack: Machine learning at the forefront of threat hunting research**

**StripedFly: Perennially flying under the radar**

**TOP 10 unattributed APT mysteries**

- 4 Details on the similarities between malware styles and malware components' source code found in Shamoon, StoneDrill and NewsBeef.

**Applied YARA training  
Q&A**

Our discovery of StoneDrill provides another dimension to the existing wave of wiper attacks against Saudi organizations that started with Shamoon 2.0 in November 2016. Compared to the new Shamoon 2.0 variants, the most significant difference is the lack of a disk driver used for direct access during the destructive step. Nevertheless, one does not necessarily need raw disk access to perform destructive functions at file level, which the malware implements quite successfully.

**PuzzleMaker attacks  
with Chrome zero-day  
exploit chain**

Of course, one of the most important questions here is the connection between Shamoon and StoneDrill. Both wipers appear to have been used against Saudi organizations during a similar timeframe of October–November 2016. Several theories are possible here:

- StoneDrill is a less-used wiper tool, deployed in certain situations by the same Shamoon group.
- StoneDrill and Shamoon are used by different groups which are aligned in their interests.
- StoneDrill and Shamoon are used by two different groups which have no connection to each other and just happen to target

Saudi organizations at the same time.

Taking all factors into account, our opinion is that the most likely theory is the second.

Additionally, StoneDrill appears to be connected with previously reported [NewsBeef activity](#), which continues to target Saudi organizations. From this point of view, NewsBeef and StoneDrill appear to be continuously focused on targeting Saudi interests, while Shamoon is a flashy, come-and-go high impact tool.

In terms of attribution, while Shamoon embeds Arabic-Yemen resource language sections, StoneDrill embeds mostly Persian resource language sections. Geopolitical analysts would be quick to point out that Iran and Yemen are both players in [the Iran-Saudi Arabia proxy conflict](#). Of course, we do not exclude the possibility of false flags.

---

Finally, many unanswered questions remain in regards to StoneDrill and NewsBeef. The discovery of the StoneDrill wiper in Europe is a significant sign that the group is expanding its destructive attacks outside the Middle East. The target for the attack appears to be a large corporation with a wide area of activity in the petro-chemical sector, with no apparent connection or interest in Saudi Arabia.

As usual, we will continue to monitor the Shamoon, StoneDrill and NewsBeef attacks.

## Subscribe to our weekly e-mails

The hottest research right in your inbox

☐ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

 **Subscribe**

A presentation about StoneDrill will be given at [the Kaspersky Security Analyst Summit](#) Conference in April 2-6, 2017.

Kaspersky Lab products detect the Shamoon and StoneDrill samples as:

- Trojan.Win32.EraseMBR.a
- Trojan.Win32.Shamoon.a
- Trojan.Win64.Shamoon.a
- Trojan.Win64.Shamoon.b
- Backdoor.Win32.RemoteConnection.d
- Trojan.Win32.Inject.wmyv
- Trojan.Win32.Inject.wmyt
- HEUR:Trojan.Win32.Generic

# Indicators of Compromise

## Shamoon MD5s

- 00c417425a73db5a315d23fac8cb353f
- 271554cff73c3843b9282951f2ea7509
- 2cd0a5f1e9bcce6807e57ec8477d222a
- 33a63f09e0962313285c0f0fb654ae11
- 38f3bed2635857dc385c5d569bbc88ac
- 41f8cd9ac3fb6b1771177e5770537518
- 5446f46d89124462ae7aca4fce420423
- 548f6b23799f9265c01feefc6d86a5d3
- 63443027d7b30ef0582778f1c11f36f3
- 6a7bff614a1c2fd2901a5bd1d878be59
- 6bebb161bc45080200a204f0a1d6fc08
- 7772ce23c23f28596145656855fd02fc
- 7946788b175e299415ad9059da03b1b2
- 7edd88dd4511a7d5bcb91f2ff177d29d
- 7f399a3362c4a33b5a58e94b8631a3d5
- 8405aa3d86a22301ae62057d818b6b68
- 8712cea8b5e3ce0073330fd425d34416
- 8fbe990c2d493f58a2afa2b746e49c86

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of the SideWinder APT group

BlindEagle flying high in Latin America

940cee0d5985960b4ed265a859a7c169  
9d40d04d64f26a30da893b7a30da04eb  
aae531a922d9cca9ddca3d98be09f9df  
ac8636b6ad8f946e1d756cd4b1ed866d  
af053352fe1a02ba8010ec7524670ed9  
b4ddab362a20578dc6ca0bc8cc8ab986  
baa9862b027abd61b3e19941e40b1b2d  
c843046e54b755ec63ccb09d0a689674  
d30cfa003ebfcd4d7c659a73a8dce11e  
da3d900f8b090c705e8256e1193a18ec  
dc79867623b7929fd055d94456be8ba0  
ec010868e3e4c47239bf720738e058e3  
efab909e4d089b8f5a73e0b363f471c1

**EastWind campaign:  
new CloudSorcerer  
attacks on government  
organizations in Russia**

**APT trends report Q2  
2024**

**CloudSorcerer – A  
new APT targeting  
Russian government  
entities**

**StoneDrill MD5s**

ac3c25534c076623192b9381f926ba0d  
0ccc9ec82f1d44c243329014b82d3125  
8e67f4c98754a2373a49eaf53425d79a  
fb21f3cea1aa051ba2a45e75d46b98b8

**StoneDrill C2s**

www.eservic[.]com  
www.securityupdated[.]com  
www.actdire[.]com  
www.chromup[.]com

**NewsBeef C2s**

www.chrome-up[.]date  
service1.chrome-up[.]date  
service.chrome-up[.]date  
webmaster.serveirc[.]com

 [Download full report](#)



APT

BACKDOOR

SHAMOON

STONEDRILL

TARGETED ATTACKS

TROJAN

WIPER

# From Shamoon to StoneDrill

Your email address will not be published. Required fields are marked \*

Type your comment here

Name \*

Email \*

Comment



**NEAL DENNIS**  
Posted on March 6, 2017. 11:57 pm

Can y'all share, even if offline, the one Euro connection?

[Reply](#)

**ALIS**  
Posted on March 10, 2017. 11:55 am

Great report, thanks for sharing.

[Reply](#)

## // LATEST POSTS

SAS

**The Crypto Game of Lazarus APT: Investors vs. Zero-days**

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

**Grandoreiro, the global trojan with grandiose goals**

GREAT

CRIMEWARE REPORTS

**Stealer here, stealer there, stealers everywhere!**

GREAT

CRIMEWARE REPORTS

**Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia**

KASPERSKY

## // LATEST WEBINARS



THREAT INTELLIGENCE  
AND IR

04 SEP 2024, 5:00PM 60 MIN

**Inside the Dark Web: exploring the human side of cybercriminals**

ANNA PAVLOVSKAYA



TECHNOLOGIES AND  
SERVICES

13 AUG 2024, 5:00PM 60 MIN

**The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise**

OLEG GOROBETS,  
ALEXANDER LISKIN



CYBERTHREAT TALKS

16 JUL 2024, 5:00PM 60 MIN

**Cybersecurity's human factor – more than an unpatched vulnerability**

OLEG GOROBETS



TRAININGS AND  
WORKSHOPS

09 JUL 2024, 4:00PM 60 MIN

**Building and prioritizing detection engineering backlogs with MITRE ATT&CK**

ANDREY TAMOYKIN

## // REPORTS

## Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

## EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

## BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

## APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.



## // SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

 **Subscribe**

☐

I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

<a href="#">APT (Targeted attacks)</a>	<a href="#">APT reports</a>	<a href="#">Archive</a>
<a href="#">Secure environment (IoT)</a>	<a href="#">Malware descriptions</a>	<a href="#">All tags</a>
<a href="#">Mobile threats</a>	<a href="#">Security Bulletin</a>	<a href="#">Webinars</a>
<a href="#">Financial threats</a>	<a href="#">Malware reports</a>	<a href="#">APT Logbook</a>
<a href="#">Spam and phishing</a>	<a href="#">Spam and phishing reports</a>	<a href="#">Statistics</a>
<a href="#">Industrial threats</a>	<a href="#">Security technologies</a>	<a href="#">Encyclopedia</a>
<a href="#">Web threats</a>	<a href="#">Research</a>	<a href="#">Threats descriptions</a>
<a href="#">Vulnerabilities and exploits</a>	<a href="#">Publications</a>	<a href="#">KSB 2023</a>
<a href="#">All threats</a>	<a href="#">All categories</a>	

© 2024 AO Kaspersky Lab. All Rights Reserved.  
Registered trademarks and service marks are the property of their respective owners.

[Privacy Policy](#) | [License Agreement](#)  
| [Cookies](#)