

From Shamoon to StoneDrill

APT REPORTS06 MAR 2017

⌚ 4 minute read

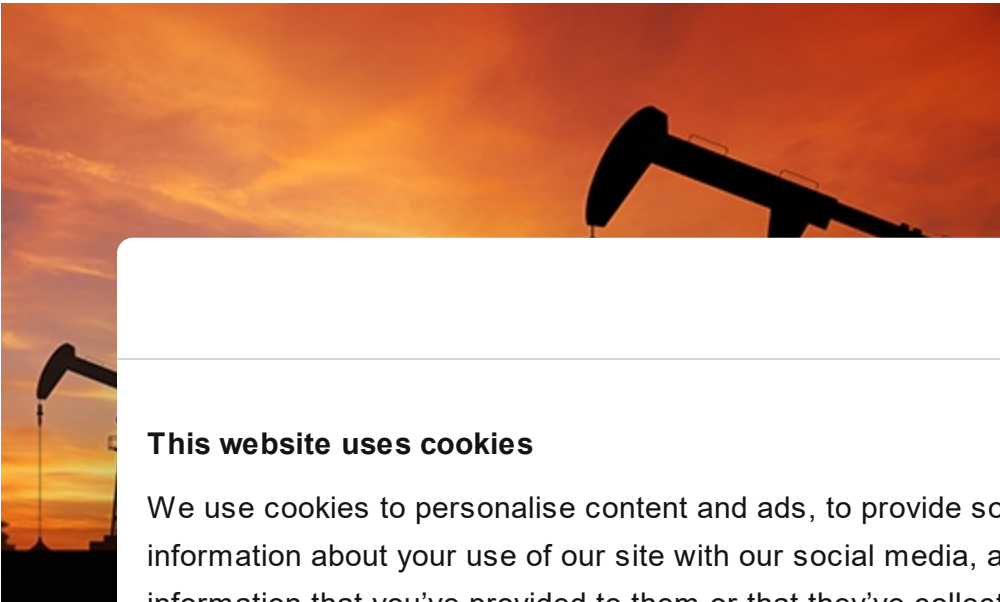
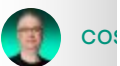


Table of Contents

Indicators of Compromise

Shamoon MD5s

// AU



Wipe



Beginnin multiple infamous [Shamoon](#) worm that targeted Saudi Aramco and reached 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.



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. Dandelion Edition**



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
			

Show details >

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

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.

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

Applied YARA training Q&A

PuzzleMaker attacks with Chrome zero-day exploit chain



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

Of course, we cannot rule out the possibility of Shamoon 2.0 being a StoneDrill variant. However, based on the timeframe and the nature of the attacks, we believe the most likely theory is the second.

- StoneDrill is a new group of malware.
- StoneDrill is a variant of Shamoon 2.0.
- StoneDrill is a new group of malware, but it is related to Shamoon 2.0 and other wiper attacks.

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.

Subscribe to our weekly e-mails

The hottest research right in your inbox

af053352fe1a02ba8010ec7524670ed9
b4ddab362a20578dc6ca0bc8cc8ab986
baa9862b027abd61b3e19941e40b1b2d
c843046e54b755ec63ccb09d0a689674
d30cfa003ebfcd4d7c659a73a8dce11e
da3d900f8b090c705e8256e1193a18ec
dc79867623b7929fd055d94456be8ba0
ec010868e3e4c47239bf720738e058e3
efab909e4d089b8f5a73e0b363f471c1

StoneDrill MD5s

ac3c25534c076623192b9381f926ba0d
0ccc9ec82f1d44c243329014b82d3125
8e67f4c98754a2373a49eaf53425d79a
fb21f3cea1aa051ba2a45e75d46b98b8

StoneDrill C2s

www.eservic[.]com
www.sec
www.act
www.chr

News

www.chr
service1
service.c
webmas



APT

TROJAN

APT trends report Q2 2024

CloudSorcerer – A new APT targeting Russian government entities



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

From Shamoon to StoneDrill

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

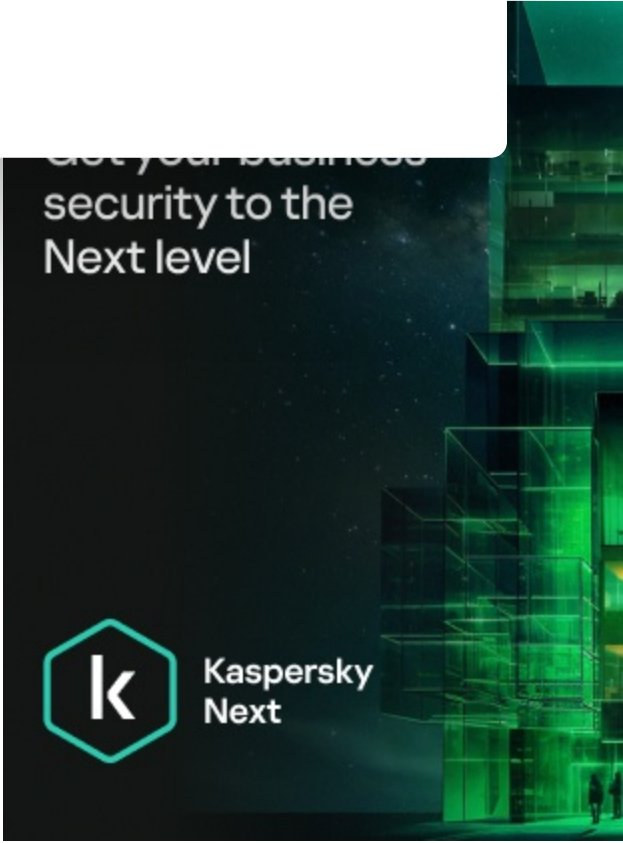
Type your comment here

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

A LIS
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
- MALWARE DESCRIPTIONS


Grandoreiro, the global trojan with grandiose goals
- CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!
- CRIMEWARE REPORTS

Analysis of the Crypt Ghoul group: continuing the


BORIS LARIN

// LA

-  THREATS

04 SEP 2024

Inside the world of the human cybercriminal

ANNA PAVLOVA
-  THREATS

60 MIN

Backlogs

// 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.



// SUBSCRIPTIONS MAILS

The hottest

Cookiebot
by Usercentrics

Subscribe

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

- Security technologies
- Research
- Publications
- All categories

- Encyclopedia
- Threats descriptions
- KSB 2023