Telefónica

etisalat

TREND REPORT_

How Wiper Malware Affects Middle East and South America

2018.06.19

CYBER SECURED BY ElevenPaths

elevenpaths.com

Index

1. Introduction

Two of the current members of the **Telco Security Alliance**, Etisalat and Telefónica detect similar malware behaviours in its respective footprint and are willing to provide regular CyberSecurity Threat advisory for user awareness and to take corrective action to protect critical information from Cyber Threats.

Please be advised that the received intelligence from various sources about the expected cyber-attack called **Wiper Malware** which could wipe the hard drive of the infected systems.

The main intention of the attacks is to **destroy systems and/or data**, causing great financial and reputation damages. Shamoon, Black Energy, Destover, ExPetr/Not Petya and Olympic Destroyer: All of these wiper malwares, and others like them, have a singular purpose of destroying systems and or data, usually causing great financial and reputational damage to victim companies.

1.1.Wiper Malware Analysis

Wiper Malware codes has been active since 2012, when the malware Shamoon appeared. Wiper malwares attacks the master boot record and core file system operations and it makes difficult to recover from the malicious software. Once the malware gets into a system, it spreads and, in most of the cases, it could be very difficult to detect and shut it down in time to avoid a major disruption. A wiper's destructive capability can vary, ranging from the overwriting of specific files, to the destruction of the entire filesystem. The amount of data impacted will be a direct consequence of the technique used. Which, of course, will have direct impact on the business the harder the data/system recovery process becomes, the bigger the business impact.

Usually, a wiper malware has three attack vectors: **files** (data), **boot section** of the **operating system** and data. The backup destruction is commonly done by deleting the volume shadow copies and the backups.

It simply erases the first 10 sectors of the physical disk, or the malware can rewrite these first 10 sectors with a new boot loader that will perform additional damage. The wipers will also use operating system command-line utilities to destroy the recovery console. Most of the wipers do not overwrite the entire hard disk. The wiper can perform the destruction of the hard disk by:

- Creating a list of targeted files
- Listing files in specific folders
- Rewriting a certain amount of bytes at the beginning of each file
- Overwriting the file completely, if the files are smaller than one amount
- Write certain amount of butes every other amount

Shamoon: This type bypasses any protection to files enforced by the operating system, allowing the destruction of files while the system is still running.

The propagation of these malwares is different one from another; in recent cases, such as **Olympic Destroyer**, the malware was released in the form of wiper worms, performing self-replication and lateral movement inside the networks.

Moreover, replication modules are usually used together with credential-harvesting modules and some of the worms also carry the code to exploit vulnerabilities that allow remote code execution.

2. Timeline of Attacks

Over the last 10 years there have been multiple incidents related to wiper malwares, starting from **Shamoon1** in 2012, until the **Olympic** attack in February 2018.

The different wipers have used specific techniques to achieve their goals: release of MeDoc, data exfiltration and release into a public domain, attack over Microsoft Windows SMB protocols on the internet, compromise of the vendor M.E.Doc using the software to execute their own code on the target device. .

Image 1: Timeline of Wiper attacks since 2012

2.1.Wiper Attacks in the Middle East

The two main wipers that have affected assets from Middle East are **StoneDrill** and **Shamoon**. Shamoon, also called W32.Disttrack, was first discovered in August 2012, when it compromised thousands of computers in Gulf States. Shamoon was used against **national oil companies**.

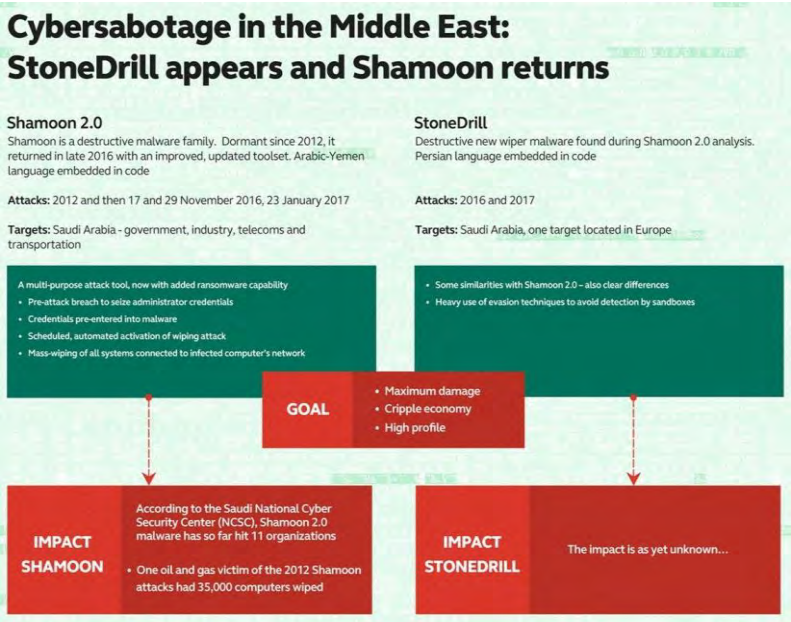


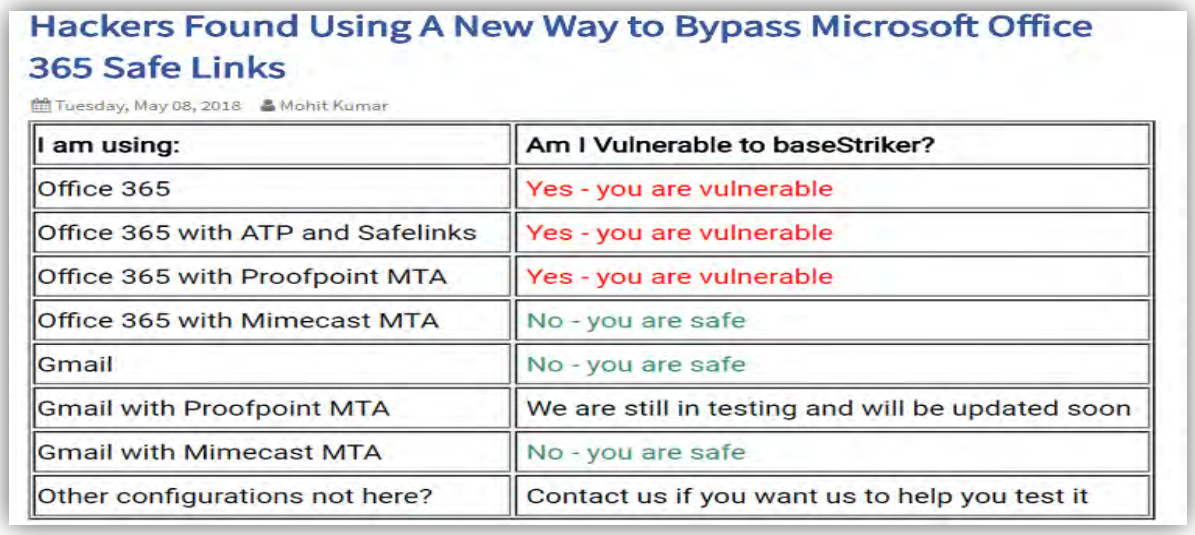
Image 2: Stonedrill and Shamoon – Kaspersky details

In 2017, researchers observed a resurgence of targeted attacks designed to destroy data or to cause data theft. They also discovered a previously unknown wiper malware which appears to be targeting organizations in Middle East. They called this new wiper StoneDrill; StoneDrill has several "style" similarities to Shamoon, with multiple interesting factors and techniques to allow a better evasion of detection.

Image 3: Timeline of Stonedrill Samples

2.2.Currents Threat in the Middle East

These types of threats have usually been linked to vulnerabilities in Microsoft systems. That is why several tweets that relate the latest Microsoft vulnerability as a possible attack vector for State Armies are extremely interested.



Hackers Found Using A New Way to Bypass Microsoft Office 365 Safe Links

Tuesday, May 08, 2018 Mohit Kumar

I am using:	Am I Vulnerable to baseStriker?
Office 365	Yes - you are vulnerable
Office 365 with ATP and Safelinks	Yes - you are vulnerable
Office 365 with Proofpoint MTA	Yes - you are vulnerable
Office 365 with Mimecast MTA	No - you are safe
Gmail	No - you are safe
Gmail with Proofpoint MTA	We are still in testing and will be updated soon
Gmail with Mimecast MTA	No - you are safe
Other configurations not here?	Contact us if you want us to help you test it

Image 4: Bypass Office safe links

This twit said that, "Serious bugs in Microsoft products are now deployed and the armies can used them. Update your systems and remove any unnecessary hardware connection to the Internet."

The general recommendation would be to keep all Microsoft systems updated.

2.3.Wiper Attacks in LATAM

Back in 2015, a specific variant of a wiper popularly known as **KillDisk** was discovered while attacking several industrial sectors **all over the world**: energy, mining, banking... Since then, it has been used as a digital **extortion** weapon. But since January 2018, there have been detected serious incidents related with wiper malware and, specifically, Latin American Banks networks.

This was described as a powerful wiper artefact. This KillDisk variant was not only able to wipe several important files in the system, but the MBR of all the physical drives in the system, so there is no way of booting them. It was able to overwrite the first 0x20 sectors of every device with "0x00". After waiting for about 15 minutes, the malware forced the system to reboot, killing essential processes of the operative system. Once rebooted, the computer **is not able to start the operative system** again so the files were not only deleted, but the whole **system remained inaccessible**.

This program has evolved since then and not only as an extortion weapon itself, but, as a smokescreen to **distract** administrators in the network while the attackers performed other attacks related with banking activities and get some benefits. These KillDisk variants are usually distributed in some innovative ways.

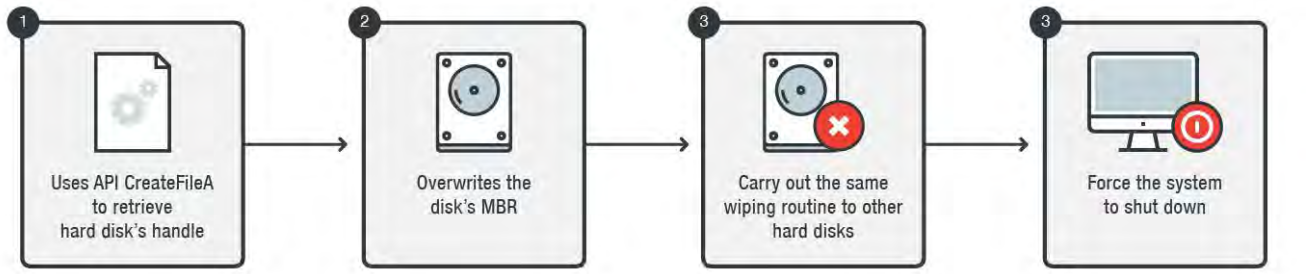


Image 6: KillDisk Wiper basic routine

2.4. Wiper Attacks in LATAM as a smokescreen

In January 2018, some incidents related with banking systems in **Bancomext** (Banco Nacional de Comercio Exterior) were detected, when some North Korean group tried to attack the **SWIFT** (Society for Worldwide Interbank Financial Telecommunication) internal network of the bank aiming to steal up to 110 million USD dollars. The attackers got to break in the network, take control of it and then launch this distracting attack while trying to get to the real target.

Later, in May 2018, several banks in Chile and other LATAM countries observed similar wiper malware attacks. This time, this **KillDisk variant** was clearly used as a **smokescreen** to get to where the real target was: the SWIFT local network in the bank. While administrators tried to understand what was happening to thousands of desktop computers rebooting and unable to boot back again, the attackers tried to abuse de SWIFT network.

From the technical and tactical point of view, this particular wiper samples used in these attacks had some interesting particularities. For example, it was created using **NSIS language**, normally used to easily create installation programs for Windows. Aside, it was strongly **obfuscated using VMprotect**, which is a very sophisticated program to avoid reverse engineering the sample, and making it very difficult to know how it eventually works. The malware was conceived to break systems, not to take control of them since it did not even use any command and control communication point (as usually done in any other malware). This specific sample wiped the first sector only (512 bytes) with 0x00.

This wiper used an interesting way to propagate in the internal network, using, ironically, the antivirus agents to spread itself from a server to the desktop computers. Since these antivirus programs are able to spread and install programs from server to clients, antivirus signature updates and other routines from a central server, this KillDisk variant used this as a way to reach and infect the computers in the internal network. This all happened while the attackers were trying to perform fraudulent operations in the SWIFT network.

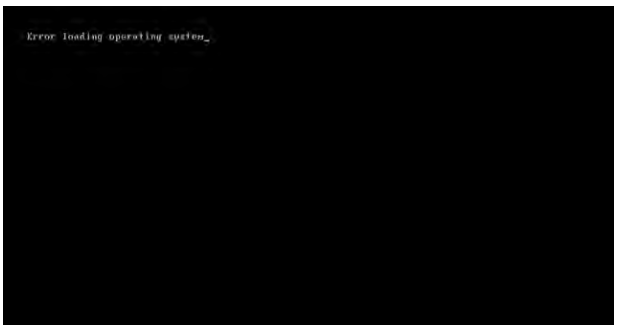


Image 7: Systems become inoperative after restart

3. Mitigation

Wiper attacks are extremely destructive, deploying defensive tactics including Intrusion Prevention signatures and Antivirus solutions are simply not effective enough on their own to mitigate this type of attack. Due to the different features and origin of these kind of attacks, it is recommended that organizations establish different actions to pre-vent any damage from attackers. Most of the security organizations and specialized websites, advice that organizations should focus their defense strategy against these attacks by performing following actions:

- **Security Assessment** - Conduct a security assessment of the control network, in order to identify and remove any security loophole.
- The development of a **security plan** that cover any update on the products used by the company will help to close any security hole and the spread of this kind of attacks.
- **Threat Intelligence** - Request of external advice against this kind of attacks and the utilization of the contracted early alert services.
- **Training** - Develop a training plan for the employees of the companies, in order to inform them how they should work to prevent these kind of attacks.
- **Perform** scheduled programs to evaluate and update the main vendor products and own developed services. The system must be up to date, since this kind of malwares use to spread by taking advance of the most common vulnerabilities from OS systems, such as Windows (Shamoon).
- **Isolate** important intellectual property to hardened networks. Access only over privileged connections.
- Utilize off site **data backups** for critical information.
- **Do not enable macros** from Microsoft office attachments and Beware, of phishing, do not follow unsolicited Web links.
- Restrict users' ability (**permissions**) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services.
- **Restrict execution of PowerShell /WSCRIPT/ PSEXEC / WMIC** in enterprise environment. Ensure installation and use of the **latest version of PowerShell**, with enhanced logging enabled.

4. Indicators of Compromise

4.1.Shamoon MD5s

00c417425a73db5a315d23fac8cb353f

271554cff73c3843b9282951f2ea7509

2cd0a5f1e9bcce6807e57ec8477d222a

33a63f09e0962313285c0f0fb654ae11

38f3bed2635857dc385c5d569bbc88ac

41f8cd9ac3fb6b1771177e5770537518

5446f46d89124462ae7aca4fce420423

548f6b23799f9265c01feefc6d86a5d3

63443027d7b30ef0582778f1c11f36f3

6a7bff 614a1c2fd2901a5bd1d878be59

6bebb161bc45080200a204f0a1d6fc08

7772ce23c23f28596145656855fd02fc

7946788b175e299415ad9059da03b1b2

7edd88dd4511a7d5bcb91f2ff177d29d

7f399a3362c4a33b5a58e94b8631a3d5

8405aa3d86a22301ae62057d818b6b68

8712cea8b5e3ce0073330fd425d34416

8fbe990c2d493f58a2afa2b746e49c86

940cee0d5985960b4ed265a859a7c169

9d40d04d64f26a30da893b7a30da04eb

aae531a922d9cca9ddca3d98be09f9df

ac8636b6ad8f946e1d756cd4b1ed866daf

053352fe1a02ba8010ec7524670ed9

b4ddab362a20578dc6ca0bc8cc8ab986

baa9862b027abd61b3e19941e40b1b2d

c843046e54b755ec63ccb09d0a689674

d30cfa003ebfcd4d7c659a73a8dce11e

da3d900f8b090c705e8256e1193a18ec

dc79867623b7929fd055d94456be8ba0

ec010868e3e4c47239bf720738e058e3ef

ab909e4d089b8f5a73e0b363f471c1

4.2.StoneDrill MD5s

ac3c25534c076623192b9381f 926ba0d 0ccc9ec82f 1d44c243329014b82d3125 8e67f 4c98754a2373a49eaf 53425d79afb21f3cea1aa051ba2a45e75d46b98b8

4.3.StoneDrill C2s

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

4.4.NewsBeef C2s

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

4.5.Disttrack Droppers

47bb36cd2832a18b5ae951cf5a7d44fba6d8f5dca0a372392d40f51d1fe1ac34 (x64)

394a7ebad5dfc13d6c75945a61063470dc3b68f7a207613b79ef000e1990909b (x86)

4.6.Communication Components

772ceedbc2cacf7b16ae967de310350e42aa47e5cef19f4423220d41501d86a5 (x64)

61c1c8fc8b268127751ac565ed4abd6bdab8d2d0f2ff6074291b2d54b0228842 (x86)

4.7.Wiper Components

c7fc1f9c2bed748b50a599ee2fa609eb7c9ddaeb9cd16633ba0d10cf66891d8a (x64)

128fa5815c6fee68463b18051c1a1ccdf28c599ce321691686b1efa4838a2acd (x86)

4.8.EldoS RawDisk Samples

5a826b4fa10891cf63aae832fc645ce680a483b915c608ca26cedbb173b1b80a (x64)

4744df6ac02ff0a3f9ad0bf47b15854bbebb73c936dd02f7c79293a2828406f6 (x86)

4.9.OlympicDestroyer

0311CEC923C57A435E735E106517797F

104ECBC2746702FA6ECD4562A867E7FB

12668F8D072E89CF04B9CBCD5A3492E1

19C539FF2C50A0EFD52BB5B93D03665A

221C6DB5B60049E3F1CDBB6212BE7F41

3514205D697005884B3564197A6E4A34

3C0D740347B0362331C882C2DEE96DBF

47E67D1C9382D62370A0D71FECC5368B

4C8FA3731EFD2C5097E903D50079A44D

4F43F03783F9789F804DCF9B9474FA6D

51545ABCF4F196095ED102B0D08DEA7E

52775F24E230C96EA5697BCA79C72C8E

567D379B87A54750914D2F0F6C3B6571

5778D8FF5156DE1F63361BD530E0404D

583F05B4F1724ED2EBFD06DD29064214

58DD6099F8DF7E5509CEE3CB279D74D5

59C3F3F99F44029DE81293B1E7C37ED2

64AA21201BFD88D521FE90D44C7B5DBA

65C024D60AF18FFAB051F97CCDDFAB7F

68970B2CD5430C812BEF5B87C1ADD6EA

6E0EBEEEA1CB00192B074B288A4F9CFE

7C3BF9AB05DD803AC218FC7084C75E96

83D8D40F435521C097D3F6F4D2358C67

86D1A184850859A6A4D1C35982F3C40E

4.10.CVE-2018-8174 | Windows VBScript Engine Remote Code Execution Vulnerability

b48ddad351dd16e4b24f3909c53c8901 – RTF documento

15eafc24416cbf4cfe323e9c271e71e7 – Internet Explorer exploit (CVE-2018-8174)

1ce4a38b6ea440a6734f7c049f5c47e2 – Payload autosoundcheckers[.]com

4.11.TROJ_KILLDISK.IUB

8a81a1d0fae933862b51f63064069aa5af3854763f5edc29c997964de5e284e5

1a09b182c63207aa6988b064ec0ee811c173724c33cf6dfe36437427a5c23446

a3f2c60aa5af9d903a31ec3c1d02eeeb895c02fcf3094a049a3bdf3aa3d714c8

5. References

- Global SOCS of Etisalat and Telefónica
- Threat Post: "*Secrets of the Wiper: Inside the World's Most Destructive Malware*". https://threatpost.com/secrets-of-the-wiper-inside-the-worlds-most-destructive-malware/131836/
- Kaspersky: https://www.kaspersky.com/
- Blog Talos Intelligence: "Wipers - Destruction as a means to an end". https://blog.talosintelligence.com/2018/05/wipers-destruction-as-means-to-end.html
- Blog Trend Micro: "New KillDisk Variant Hits Financial Organizations in Latin America". https://blog.trendmicro.com/trendlabs-security-intelligence/new-killdisk-variant-hits-financial-organizations-in-latin-america/

About ElevenPaths

At ElevenPaths, Telefónica Cyber Security Unit, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We're always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

www.elevenpaths.com
@ElevenPaths
blog.elevenpaths.com

About Etisalat

Headquartered in Abu Dhabi, Etisalat was established four decades ago in the UAE as the country's first telecommunications service provider. An international blue-chip organization, Etisalat Group provides innovative solutions and services to 163 million subscribers in 17 countries across the Middle East, Asia and Africa.

www.etisalat.ae
@etisalat