SECURELIST

What was that Wiper thing?

0.6

GReAT
Kaspersky Lab Expert
Posted August 29, 13:00 GMT
Tags: Duqu, Targeted Attacks, Wiper, Cyber weapon, Gauss, Flame

In April 2012, several stories were published about a mysterious malware attack shutting down computer systems at businesses throughout Iran.

Several articles mentioned that a virus named Wiper was responsible. Yet, no samples were available from these attacks, causing many to doubt the accuracy of these reports.

Following these incidents, the International Telecommunication Union (ITU) asked Kaspersky Lab to investigate the incidents and determine the potentially destructive impact of this new malware.

After several weeks of research, we failed to find any malware that shared any known properties with Wiper. However, we did discover the nation-state cyber-espionage campaign now known as Flame and later Gauss.

It is our firm opinion that Wiper was a separate strain of malware that was not Flame. Although Flame was a highly flexible attack platform, we did not see any evidence of very destructive behavior. Given the complexity of Flame, one would expect it to be used for long-term surveillance of targets instead of direct sabotage attacks on computer systems. Of course, it is possible that one of the last stages of the surveillance was the delivery of a Wiper-related payload, but so far we haven-t seen this anywhere.

So, months later, we are left wondering: Just what was Wiper?

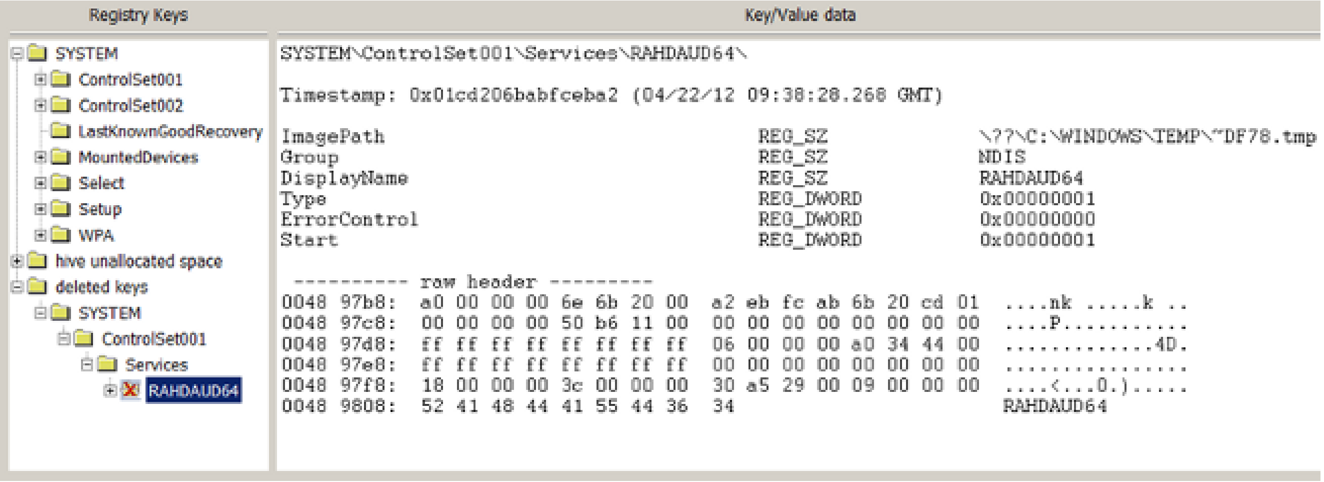
Enter Wiper

During the investigation of the mysterious malware attack in April, we were able to obtain and analyze several hard drive images that were attacked by Wiper. We can now say with certainty that the incidents took place and that the malware responsible for these attacks existed in April 2012. Also, we are aware of some very similar incidents that have taken place since December of 2011.

The attacks mostly took place in the last 10 days of the month (between the 21st and 30th) although we cannot confirm that this was due to a special function being activated on certain dates.

The creators of Wiper were extremely careful to destroy absolutely every single piece of data which could be used to trace the incidents. So, in every single case we-ve analyzed, almost nothing was left after the activation of Wiper. It-s important to stress ?almost nothing here because some traces did remain that allowed us to get a better understanding of the attacks.

From some of the destroyed systems we were lucky enough to recover a copy of the registry hive. The registry hive did not contain any malicious drivers or startup entries. However, we came up with the idea to look into the hive slack space for deleted entries. This is what we found:



```
SYSTEM\ControlSet001\Services\RAHDAUD64\

Timestamp: 0x01cd206babfceba2 (04/22/12 09:38:28.268 GMT)

ImagePath                                        REG_SZ        \??\C:\WINDOWS\TEMP\~DF78.tmp
Group                                            REG_SZ        NDIS
DisplayName                                      REG_SZ        RAHDAUD64
Type                                             REG_DWORD     0x00000001
ErrorControl                                     REG_DWORD     0x00000000
Start                                            REG_DWORD     0x00000001

 ---------- raw header ---------
0048 97b8:  a0 00 00 00 6e 6b 20 00  a2 eb fc ab 6b 20 cd 01  ....nk .....k ..
0048 97c8:  00 00 00 00 50 b6 11 00  00 00 00 00 00 00 00 00  ....P...........
0048 97d8:  ff ff ff ff ff ff ff ff  06 00 00 00 a0 34 44 00  .............4D.
0048 97e8:  ff ff ff ff ff ff ff ff  00 00 00 00 00 00 00 00  ................
0048 97f8:  18 00 00 00 3c 00 00 00  30 a5 29 00 09 00 00 00  ....<...0.).....
0048 9808:  52 41 48 44 41 55 44 36  34                       RAHDAUD64
```

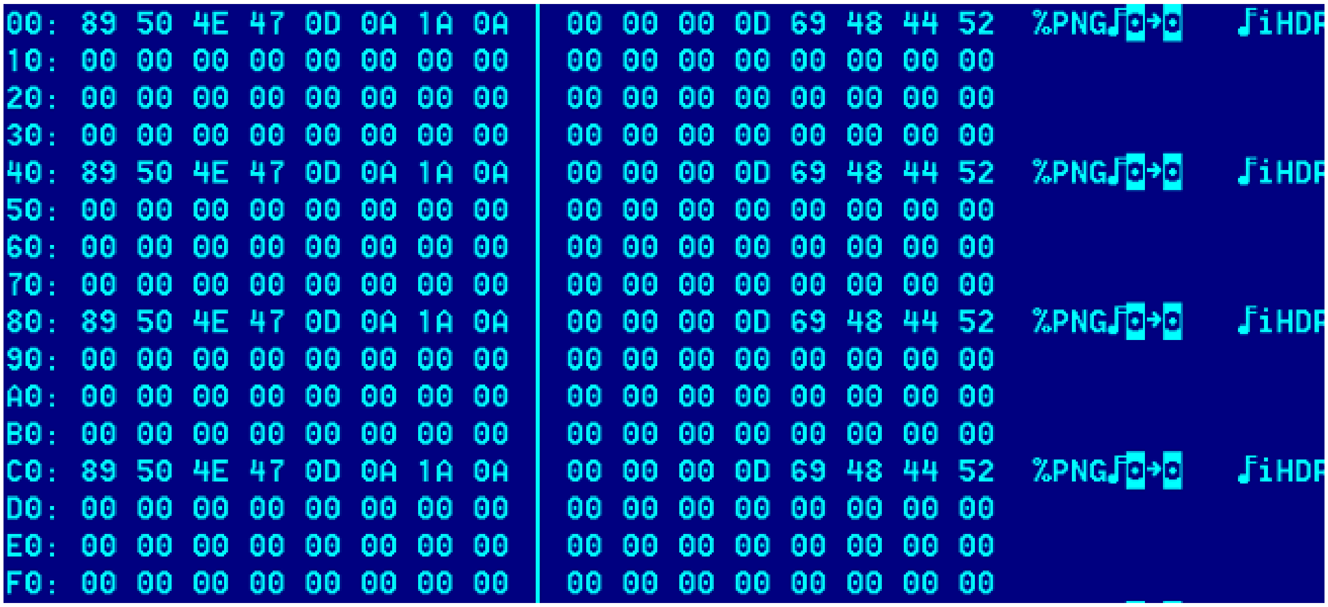
Interestingly, on 22 April, just before this system went down, a specific registry key was created and then deleted. The key was a service named ?RAHDAUD64. It pointed to a file on disk named ?~DF78.tmp, in the ?C:\WINDOWS\TEMP folder.

The moment we saw this, we immediately recalled Duqu, which used filenames of this format. In fact, the name Duqu was coined by the Hungarian researcher Boldizsár Bencsáth from the CrySyS lab because it created files named ?~dqXX.tmp. (see)

We tried to recover the file ?~DF78.tmp from the disk, but found that the physical space where it resided was filled with garbage data.

We found the same ?wiping pattern in several of the other systems we analyzed - a service named ?RAHDAUD64 which was deleted just before it is wiped - and its file filled with garbage data. In these other systems, the RAHDAUD64 service pointed to different filenames, such as ?~DF11.tmp and ?~DF3C.tmp. So it-s possible the names were random.

Another peculiarity of the wiping process was a specific pattern which was used to trash the files on disk:



```
00: 89 50 4E 47 0D 0A 1A 0A │ 00 00 00 0D 69 48 44 52  %PNG♪◙→◙   ♪iHDR
10: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
20: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
30: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
40: 89 50 4E 47 0D 0A 1A 0A │ 00 00 00 0D 69 48 44 52  %PNG♪◙→◙   ♪iHDR
50: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
60: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
70: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
80: 89 50 4E 47 0D 0A 1A 0A │ 00 00 00 0D 69 48 44 52  %PNG♪◙→◙   ♪iHDR
90: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
A0: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
B0: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
C0: 89 50 4E 47 0D 0A 1A 0A │ 00 00 00 0D 69 48 44 52  %PNG♪◙→◙   ♪iHDR
D0: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
E0: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
F0: 00 00 00 00 00 00 00 00 │ 00 00 00 00 00 00 00 00
```

Most of the files that were wiped contain this specific pattern that repeats over and over. Interestingly, it did not overwrite the entire file. In some cases some portions of the file remained intact, every header of the files were destroyed in the first place. This was probably caused by the size of the file. The wiping algorithm was designed to quickly destroy as many files as possible.

Based on the pattern that we know had been used when wiping files, we collected Kaspersky Security Network (KSN) statistics on which files had been destroyed.

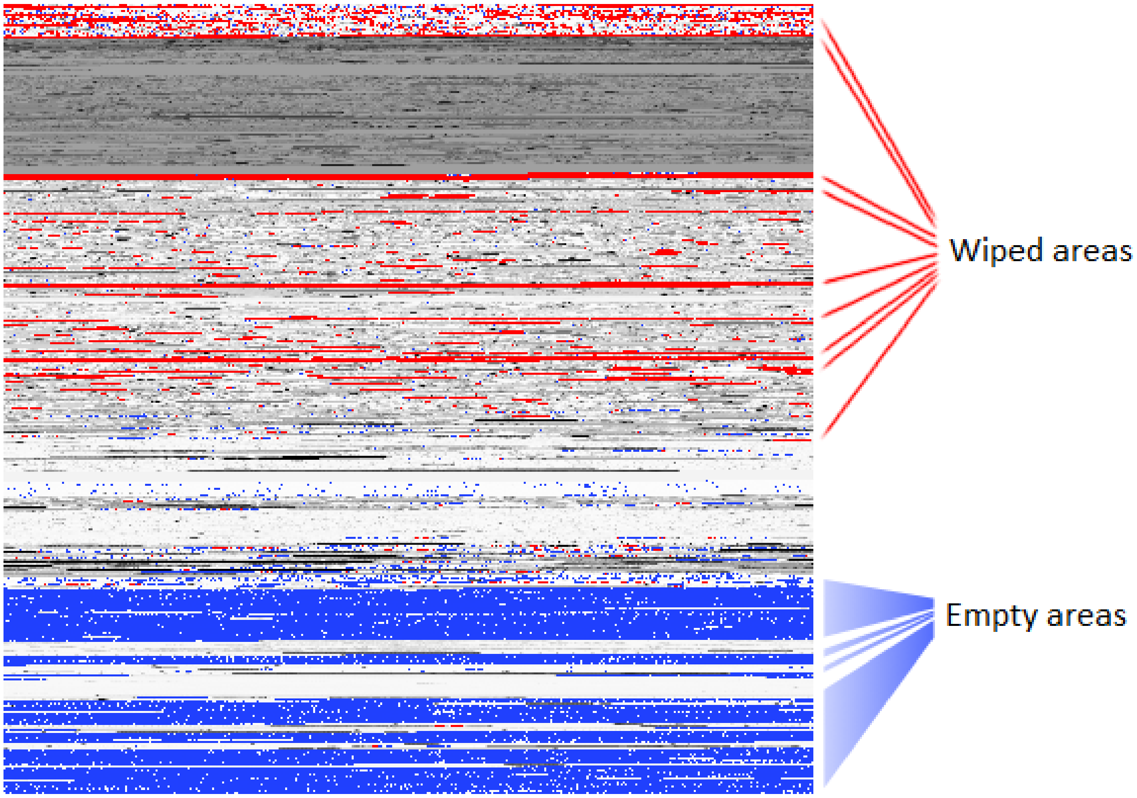
In an attempt to reconstruct the Wiper algorithm we came up with the following sequence:

1. Searching for and wiping files based on their extensions.
   List of file extensions:

accdb	cdx	dmp	H	js	pnf	rom	tif	wmdb
acl	cfg	doc	hlp	json	png	rpt	tiff	wmv
acm	chk	docx	hpi	lnk	pps	rsp	tlb	xdr
amr	com	dot	htm	log	ppt	sam	tmp	xls
apln	cpl	drv	html	lst	pptx	scp	tsp	xlsx
asp	cpx	dwg	hxx	m4a	pro	scr	txt	xml
avi	dat	eml	ico	mid	psd	sdb	vbs	xsd
ax	db	exe	inc	nls	rar	sig	wab	zip
bak	dbf	ext	Ini	one	rar	sql	wab~	=
bin	dbx	fdb	jar	pdf	rdf	sqlite	wav	=
bmp	dll	gif	jpg	pip	resources	theme	wma	=

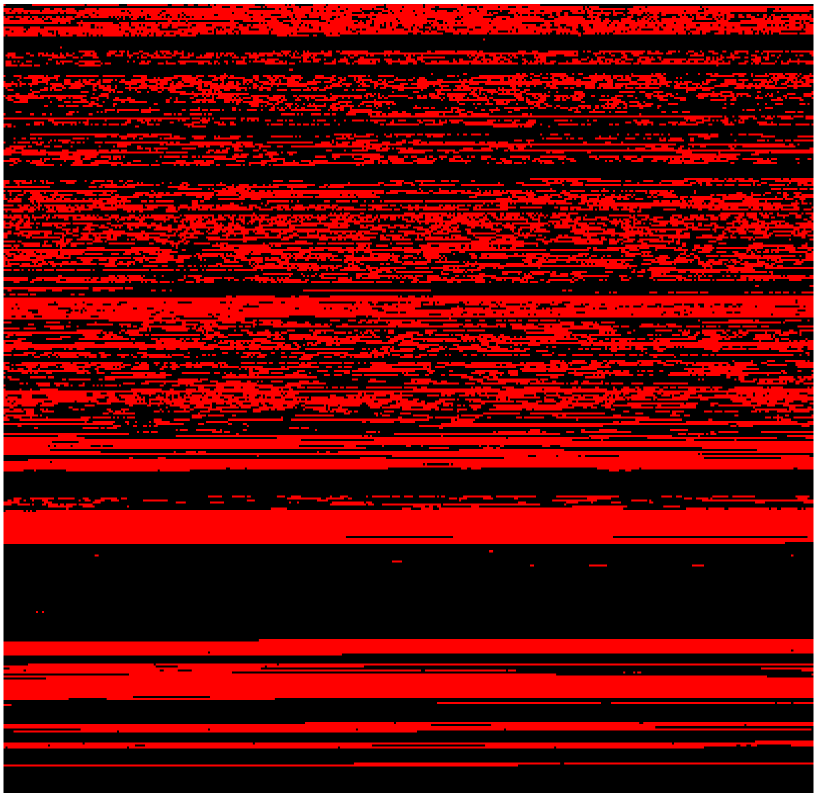
2. Searching for and wiping all files in certain folders (e.g. in Documents and Settings, Windows, Program Files) and on all available USB drives connected to the computer.
3. Wiping disk sectors (possibly using a bootkit module).

Wiping a disk that is several hundred gigabytes in size might take hours. So the creators of the malware were careful to select wiping algorithms that could achieve maximum efficiency. For example, let-s take a look at the following disk which was wiped by Wiper. We-ve used a statistical representation (Shannon entropy in blocks of 256K) to represent entropy on disk. The lighter areas have higher entropy, the darker areas, lower. The areas in red have very high entropy (highly random data).



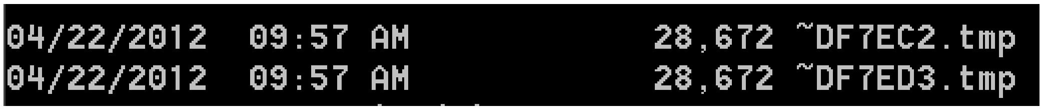
As you can see, Wiper managed to do a pretty good job of destroying most of the disk. One can observe a red-filled stripe at the top which indicates an area that has been cleaned well. Although no clear pattern is visible, a large amount of the disk has been filled with unusable data. The wiping operation obviously focused on the beginning of the disk, then it affected the middle of the disk, before the system finally crashed.

Another view can be obtained by looking for sectors which have been filled with the known ?%PNG / iHDR pattern. Red marks the sector blocks which have been overwritten with this pattern:



As you can see, more than three-quarters of the disk was affected by the wiper, with the vast majority of the data being lost forever.

In some cases, Wiper misfired - for instance, we saw one 64-bit system where Wiper failed to activate. In this case, we discovered two files in %TEMP% which were wiped with the known PNG/iHDR pattern, but not the whole disk:



```
04/22/2012  09:57 AM            28,672 ~DF7EC2.tmp
04/22/2012  09:57 AM            28,672 ~DF7ED3.tmp
```

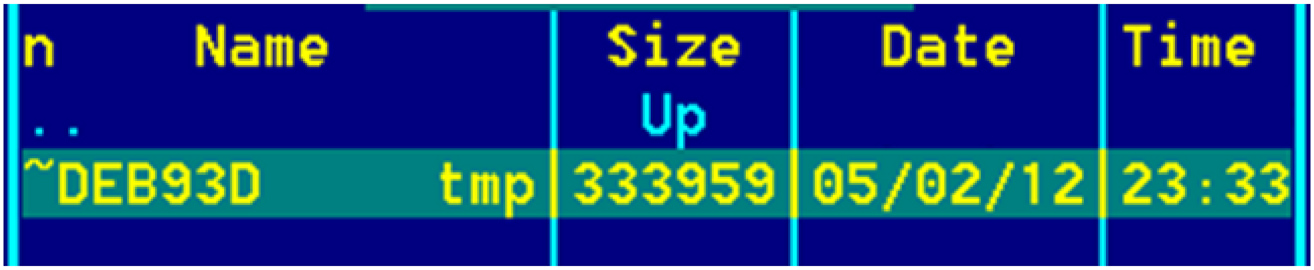
We presume these two files, out of the thousands in %TEMP%, must have been destroyed because they contained data important to the Wiper attack. In another system we analyzed, in addition to these 20K-ish files, we saw two 512 byte files named ?~DF820A.tmp and ?~DF9FAF.tmp, which have also been wiped beyond recovery.

Interesting enough, on some systems we noticed that all PNF files in the INF Windows folder were wiped with a higher priority than other files. Once again, this is a connection to Duqu and Stuxnet, which kept their main body in encrypted ?.PNF files.

If the purpose of the attackers was to make sure the Wiper malware could never be discovered, it makes sense to first wipe the malware components, and only then to wipe other files in the system which could make it crash.

Links with Flame

While searching for this elusive malware, we came across something else. We suspected Wiper used filenames such as ?~DF*.tmp or ?~DE*.tmp in the TEMP folder, so we started looking for them via KSN. During this process we noticed that an abnormally large number of machines contained the same file name: ~DEB93D.tmp:



```
n      Name         │  Size   │   Date   │ Time
..                  │   Up    │          │
~DEB93D         tmp │ 333959  │ 05/02/12 │ 23:33
```

The name seemed like a good indicator that the file was part of the Tilded platform, and related to Duqu and Stuxnet. The file appeared to be encrypted, but we quickly noticed something:

Duqu (Nov 3, 2010):
00: ED **6F C8** DA 30 EE D5 01

~DEB93D:
00: **6F C8** FA AA 40 C5 03 B8

By complete chance, we noticed that this file started with bytes ?6F C8, which were also present at the beginning of the Duqu PNF main body, in encrypted format, loaded by the driver compiled on Nov 3, 2010. If it wasn-t for this, maybe we-d have never paid attention to ~DEB93D.tmp, since the content looked like trash.

The encryption algorithm was weak and a pattern appeared to be repeating every 4096 bytes. Since the algorithm was weak we managed to decrypt it by using statistical crypto-analysis, a common technique used for decrypting files during malware analysis. After decrypting the file, we noticed what appeared to be sniffer logs. This made us check further and we found other files, modified on the same date, with names such as ?mssecmgr.ocx, ?EF_trace.log or ?to961.tmp. The rest, as it is said, is history. This is exactly how we discovered Flame.

So, what was Wiper?

There is no doubt that there was a piece of malware known as Wiper that attacked computer systems in Iran (and maybe in other parts of the world) until late April 2012.

The malware was so well written that once it was activated, no data survived. So, although we-ve seen traces of the infection, the malware is still unknown because we have not seen any additional wiping incidents that followed the same pattern as Wiper, and no detections of the malware have appeared in the proactive detection components of our security solutions.

Conclusions:

- It may be possible that we will never find out what Wiper was but based on our experience, we are reasonably sure that it existed, and that it was not related to Flame.
- It-s possible that some machines exist somewhere where the malware has somehow escaped being wiped, but if there is such a case, we haven-t seen it yet.
- Wiper may have been related to Duqu and Stuxnet, given the common filenames, but we cannot be sure of this.
- What is certain is that Wiper was extremely effective and has sparked potential copycats such as Shamoon.
- The fact that the use of Wiper led to the discovery of the 4- or 5-year-old Flame cyber-espionage campaign raises a major question. If the same people who created Duqu/Stuxnet/Flame also created Wiper, was it worth blowing the cover of a complex cyber-espionage campaign such as

Flame just to destroy a few computer systems?