Territorial Dispute –

NSA's perspective on APT landscape

v1.00 (March 2018)

Technical Report

by

Laboratory of Cryptography and System Security (CrySyS Lab)

http://www.crysys.hu/

Authors: Boldizsár Bencsáth + analysis team of Ukatemi and CrySyS Lab

Table of contents

Introduction

This document is based on a specific part of the “Shadow Broker” leaks. The unknown party, calling itself “Shadow Brokers” leaked information about stolen information from NSA a number of times. See https://en.wikipedia.org/wiki/The_Shadow_Brokers on the details.

In the Fifth leak of the group, which was named "Lost in Translation", some very interesting modules were included, some of them referred to as “Territorial Dispute”. A common understanding is that the leak contains information stolen from U.S. agency NSA, hence we will reflect the source as NSA, although we have no proofs on that, but we make no further marks on the possible attribution problem on it.

The leak is not a single set of tools, as parts are replicated over at least two different toolsets in the leaked material. However, the goal is clear. These tools are set to be used by operators to scan attacked computers (hacked targets of NSA) to check if the target has already been hacked by an outsider adversary (nation state backed targeted attack actor). In case of external attack detected, the operator is called to make special attention (in some related cases wording is “please pull back” or ask for supervisor’s advice.)

The size of the leak is huge, and there are tens of different tools and modules among them, most of them to infect computers, retrieve data, and similar. But some tools are designed to get a general knowledge about the infected computers, particularly about software, security software and malware installed on it.

While there are some other parts in the leak where the attackers (the NSA) are looking for signs of traditional cyber-crime software (malware) attacks, the Territorial Dispute part of the leak seems the most interesting. We believe they have the same goal: avoid duel between parties and minimalize the risk of detection of the attack of the governmental organization. Our work, however, focuses on APT detection information - that can help to understand what NSA knows about APT attacks from external governmental targeted attack operators.

1. Details

The tools, and scripts that the NSA used to detect other third parties (governmental actors) on the target computers are very simple tools. They check for the existence of specific files, windows registry entries, and other signs that could show the existence of external attacker (targeted, state backed actors) presence on the actual computers. These checks are considered in the term of the security community as IoC, Indicator of Compromise.

For an APT attack we can generally define IoCs in the number of tens or hundreds, but NSA tools generally contained only very few IoCs, around 1-5, which is strange. Why do they trust information from such closed set of indicators and not broaden it with multiple checks? In general, if we find a piece of malware and want to hunt for similar ones, we try to define 5-10 or even more different specific features, signatures to detect similar attacks. Then it can be set, that the search tool should only mark something important if 6 of 10 signs are found in the sample. The same could stand for an infected computer: One single registry key or existence of a single file named something common like “ipfilter.dll” might not be a good idea to make a detection based on it. But still, as we mentioned, the detection IoCs are very limited in number.

One trivial answer is that while they had probably more information, and ideas for detection, they utilized the process in a way to give as little information as possible to the operators. The operators of the leaked tools can check the source code and hence they can examine the IoCs inside. So, operators have a chance to find clues about the attacks. But once an operator could pinpoint that SIG8 is an attack against the nuclear program of Iran, who and how should inform him to keep it secret? It is a good idea to avoid such findings by limitation of the available information, and reduce IoCs in the tool to as few as possible. Still, it is a question why Stuxnet was enlisted as external attack (if the SIGs refer only targeted attacks by external parties), if possibly NSA also contributed to it? It is possible that Stuxnet attack was so hidden, that only very few at NSA knew about that and they really mis-attributed their own attack thinking belonging to external parties, hence it is part of the list, which list consists of attacks from external parties.

The naming convention for the findings also reflect this fact. All these detections are referred to as SIGX, where X stands for 1 to 45. Operators should not know about operation names, they should handle the situation according to the plan.

As mentioned already, the “detection engine”, the IoC scanning tools are very simplistic, they are looking for only a very few number of indicators, and it is not impossible, that they detect some infections of external adversaries, but they cannot detect others. It is a very strange decision, but maybe within the organization they already made a risk analysis and it showed that there is a risk that external party could stole, use, or leak this information. The attackers maybe though it was a good idea to limit the presence of IoCs in their tools to lower this risk.

IoC, scanner, public information

From the leak, we can extract the IoC information, the indicators of compromise, or in normal wording the things they are looking for. But Territorial Dispute module looks for targeted APT attacks, and there is a lot of public information uncovered about targeted attacks. The module

contains detection for the samples we really well know, as BME CrySyS Lab uncovered the Duqu attack, worked on MiniDuke, TeamSpy, Duqu2 or others.

As there is a public set of information about APT attacks uncovered by security professionals with a limited scope, and there must be a stack of information about the same attacks and more at the intelligence community.

This leak can uncovers some of the gap between the knowledge of public (through publications of the security community, mainly by the contribution of AV companies, and research labs like us at BME CrySyS), and other organizations and can shed light on the amount of difference of knowledge among these parties. Some 20 years before it was known how many math experts were hired by NSA and by later it was understood that NSA is at least 10 years beyond current public crypto research results. However, how much NSA (and others) are beyond gathering information on APT attacks was not uncovered yet. This leak helps us to shed light on the timeline how NSA found traces to attackers and how public information was available on the same attacks.

Please note, this leak was available to all kind of stakeholders on the internet for almost a year, hence this publication will not add new information for most of the governmental parties, and hence we believe it does not influence of any nation state's security or safety. However, common understanding of the situation at the public level is essential to avoid confusion and to help public to make democratic decisions on procedures of the governmental institutions. In contrast, one could expect, that based on the information in the leak, previously unknown APT attacks could have been already uncovered, and it is not impossible that even some still working 0-days could have been identified by professionals based on the leak. Also, it is a question if that was a good idea not to distribute information about discovered APTs by the government agency to help avoid further attacks.

Of course, sharing information about ongoing attacks could be debated. First of all, sharing information might influence the attacker to change strategy and tools and hence agencies cannot continue to closely observe their activity. Also, too many revealing could have speed up other governments to build up capabilities to handle attacks similar to those that NSA is capable to do. Finally, analysis of pros and cons of the sharing might have been resulted positive for hiding information, as that should be a default decision for such entities.

Work method

The goal of our work is to boost interest on this topic and help other researchers to work on the results. This means, we are unable to check those thousands of traces that the 45 IoCs of the original leaks produces. We tried to make one step after the initial information and share by this document to initiate research to widen results.

- For some known APT attacks, the findings can extend knowledge, e.g. by adding new known kernel driver names to Stuxnet attacks
- For some, only very little information was available publicly yet, but based on the IoCs malware samples, more could be uncovered and public knowledge about these could be extended, although it is very unlikely that information about the victims will be uncovered
- For some attacks, additional IoCs can start up uncovering the attack, as before of that traces were unavailable and hence APT research finished up in very short reports stating "XY used this attack as targeted attack, from now on we refer to this under the name of W" like reports.
- On some IoCs, we never had public knowledge about the classification of a targeted (APT) attack. Based on the current results, some attacks, samples, or even hundreds of samples will get to be identified as part of some APT attacks that were previously unknown or partially unknown.

Initially we tried to collect information from traditional open-source OPSEC sources, like google search. We also tried to collect information by Yara rules applied to our malware repository, which consists of at least 150 TB of known malicious binaries.

Of course, information from one source is a basis to find more information bases on the results of the previous; hence we continued to track traces. However, the set of information is just too wide so we definitely don't clam the "extensive research" or "full research" tag, our part of the story is to make "initial research".

In the rest of the document, we mainly publish links, short information strips, and hashes. This all means, we publish possibly next steps, reasoning on the origin of the attack, and all kind of additional information that can help others to go forward. We don't think we can or could have made the best document based of the available facts, so we appreciate if anybody would work on this and extend the common knowledge by their results.

Hence, we are happy to help others to publish their extensions on our work.

The current document plans to share information to professionals. Hence, in addition to the public information (in multiple types), hashes of samples are included in the results. The hashes might be partially usable, we do not have a clear vision if the samples found are really connected to the attacks.

The tools

The tools related to "Territorial Dispute" and other APT related information can be found in the following files and directories of the Shadow Brokers leak:

The **windows\Resources\TeDi\PyScripts** contains multiple files. Three of them are utility scripts, while the most interesting python program is **sigs.py,** which contains very simple 'signatures' (named SIG1-SIG45), which link to known and unknown APT campaigns from the recent years. The individual subroutines in this file are find_01 to find_45.

```
import datastore
import utils
import dsz.cmd
import dsz.lp
import os
from utils import limitedget, file_exists, reg_exists

def find_01():
    result = utils.reg_exists('L', 'software\\microsoft\\windows\\currentversion\\StrtdCfg', None, True)
    if result:
        return True
    for key in datastore.HKEY_USERS_DATA:
        result = utils.reg_exists('U', ('%s\\software\\microsoft\\windows\\currentversion\\StrtdCfg' % key), None, True)
        if result:
            return True
    return False

def find_02():
    result = utils.reg_exists('L', 'System\\CurrentControlSet\\Control\\CrashImage', None, True)
    if result:
        return True
    return False

def find_03():
    if ('driver32' in datastore.SYSTEMROOT_FILE_SET):
        return True
    return False
```

For example, find_08 relates to the Stuxnet attack, as demonstration, the subroutine is very simple and short:

```
def find_08():
    if ('s7otbxsx.dll' in datastore.SYSTEMROOT_FILE_SET):
        return True
    if ('mrxcls' in datastore.SERVICE_NAME_SET):
        return True
    if utils.file_exists(('%s\\inf' % datastore.SYSPATH_STR), 'mdmcpq3.pnf'):
        return True
    return False
```

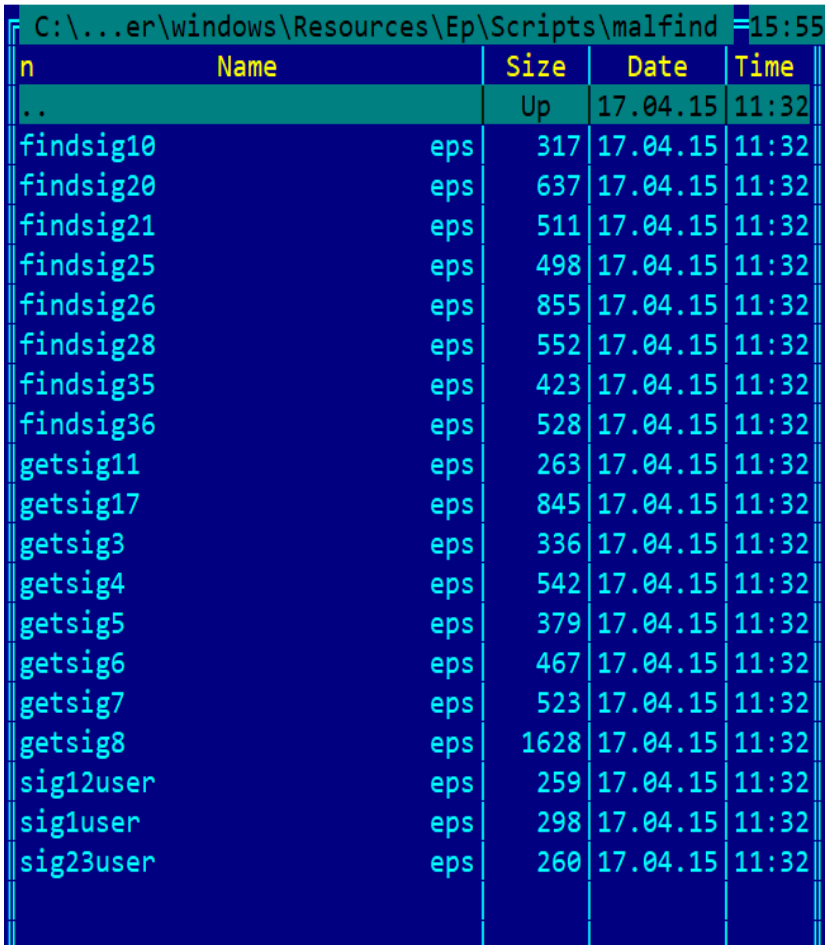
A piece of code resolves the abbreviation, 'TeDi' to Territorial Dispute:

```
tedilog = getLogger('TERRITORIALDISPUTE')
```

windows/Resources/TeDi/PyScripts/utils.py#9

In addition to the TeDi scanners, some other files also contain important information related to targeted attacks.

Another directory **windows\Resources\Ep\Scripts\malfind** contains individual tools for scanning for signs of APT attacks and extracting information:



C:\...er\windows\Resources\Ep\Scripts\malfind 15:55

n	Name	Size	Date	Time
..		Up	17.04.15	11:32
findsig10	eps	317	17.04.15	11:32
findsig20	eps	637	17.04.15	11:32
findsig21	eps	511	17.04.15	11:32
findsig25	eps	498	17.04.15	11:32
findsig26	eps	855	17.04.15	11:32
findsig28	eps	552	17.04.15	11:32
findsig35	eps	423	17.04.15	11:32
findsig36	eps	528	17.04.15	11:32
getsig11	eps	263	17.04.15	11:32
getsig17	eps	845	17.04.15	11:32
getsig3	eps	336	17.04.15	11:32
getsig4	eps	542	17.04.15	11:32
getsig5	eps	379	17.04.15	11:32
getsig6	eps	467	17.04.15	11:32
getsig7	eps	523	17.04.15	11:32
getsig8	eps	1628	17.04.15	11:32
sig12user	eps	259	17.04.15	11:32
sig1user	eps	298	17.04.15	11:32
sig23user	eps	260	17.04.15	11:32

For example, we identified that SIG25 is most likely the APT attack known as “Dark Hotel”. The related scanning tool is a very simple script:

```
string $docsandsettings = GetEnv("SYSTEMROOT");
$docsandsettings = "$docsandsettings\\..\\Documents and Settings";

@record on;
`dir * -path "$docsandsettings"`;
@record off;

string $subkeys = GetCmdData('name');
string $subkey;

foreach $subkey ($subkeys)
{
        if ($subkey == ".")
        {
                continue;
        }

        if ($subkey == "..")
        {
                continue;
        }

        if (`script dirwrapper.eps "$docsandsettings\\$subkey\\Application Data\\winver32.exe"`)
        {
                return true;
        }

}

return false;
```

As we can see, this script looks for the existence of an actual file “winver32.exe” in the very specific **$docsandsettings\\$subkey\\Application Data\\winver32.exe** path. Interestingly, using google search to find connection between winver32.exe and Dark Hotel does not currently show up any information about the connection, so this link might be a new finding based on the leaked information.

The related “get” information gathering scripts are also interesting. For example, related to Stuxnet (SIG8) the script contains the following file names:

```
@include "_FileExists.epm";
@include "DropboxAPI.epm";
string $syspath = GetEnv("SYSPATH");
string $f1 = "$syspath\\s7otbxdx.dll";
string $f2 = "$syspath\\s7otbxsx.dll";
string $f3 = "$syspath\\drivers\\mrxcls.sys";
string $f4 = "$syspath\\..\\inf\\mdmcpq3.pnf";
bool $f1exist = _FileExists($f1, "");
bool $f2exist = _FileExists($f2, "");
bool $f3exist = _FileExists($f3, "");
bool $f4exist = _FileExists($f4, "");

if ($f1exist) {
        @record on;
        `dir $f1`;
        @record off;
        int $size_f1 = GetCmdData("size");
        f1($f1,$size_f1);
}
```

If one of the files found on the target, the operator might decide to get a copy of the file. (Note the “DropboxAPI” call, most likely this is the channel for the file transfer). Related code:

```
if ($f4exist) {
        f4($f4);
}

@record off;

sub f1(IN string $f1, IN int $size_f1) {

        if (prompt "SIG8 was detected. Do you want to grab the files? \n $f1, size: $size_f1 \n") {
                `get $f1`;
        }
}

sub f2(IN string $f2, IN int $size_f2) {
        if (prompt "SIG8 was detected. Do you want to grab the files? \n $f2, size: $size_f2 \n") {
                `get $f2`;
        }
}
```

Another tool for scanning uses an external file with definitions to find related SIGs: **windows/Resources/Ep/Scripts/ifthen/gwdef_other_peeps.txt** contains mostly the same detection rules but in a different format. A sample screen on the tool:

```
MODE
PS
ups32.exe|lpsetenv -option SIG11FOUND -value 1
utilman32.exe|lpsetenv -option SIG11FOUND -value 1
taskbar.exe|lpsetenv -option SIG14FOUND -value 1
MsgQueue.exe|lpsetenv -option SIG14FOUND -value 1
SndTray.exe|lpsetenv -option SIG14FOUND -value 1
msserv.exe|lpsetenv -option SIG14FOUND -value 1

MODE
DIR
#|any number of dir's in the same directory adds zero overhead, which is why we're looking for the same file more than once
SYSPATH\driver32|lpsetenv -option SIG3FOUND -value 1
SYSTEMROOT\$NtUninstallQ817473$|lpsetenv -option SIG4FOUND -value 1
SYSTEMROOT\..\Program Files\common files\microsoft shared\msaudio|lpsetenv -option SIG9FOUND -value 1
SYSTEMROOT\..\Program Files\common files\microsoft shared\mssecuritymgr|lpsetenv -option SIG9FOUND -value 1
SYSTEMROOT\..\Program Files\common files\micfosoft shared\MSAPackages|lpsetenv -option SIG9FOUND -value 1
SYSPATH\s7otbxsx.dll|lpsetenv -option SIG8FOUND -value 1
SYSTEMROOT\inf\mdmcpq3.pnf|lpsetenv -option SIG8FOUND -value 1
SYSPATH\icsvnt32.dll|lpsetenv -option SIG10FOUND -value 1
SYSPATH\ups32.exe|lpsetenv -option SIG11FOUND -value 1
SYSPATH\utilman32.exe|lpsetenv -option SIG11FOUND -value 1
SYSPATH\utliman32.exe|lpsetenv -option SIG11FOUND -value 1
SYSPATH\drivers\ups.exe|lpsetenv -option SIG11FOUND -value 1
SYSPATH\msvcp11.dll|lpsetenv -option SIG11FOUND -value 1
SYSPATH\msxml10.dll|lpsetenv -option SIG11FOUND -value 1
SYSTEMROOT\..\Documents and Settings\All Users\Application Data\Network|lpsetenv -option SIG12FOUND -value 1
SYSPATH\winview.ocs|lpsetenv -option SIG13FOUND -value 1
```

The file **DriverList.db (windows\Resources\Ops\Databases\DriverList.db),** contains a list of drivers related to APT attacks and also a list of Antivirus product drivers, hardware drivers and some interesting ones, e.g.: information on U.S./NSA related attack tools with remarks/commands for operators. A similar file in text format can also be found at **windows\Resources\Ops\Data\drv_list.txt** and a copy of it at **windows\Resources\Ep\drv_list.txt.**

The driver list most likely contains known windows kernel drivers, and remarks reveal the connection with some APT attacks. For example, it seems that “biosfix” and “bitcheck” might be related to SIG25 APT attack. From the indicators, we think SIG25 is the APT attack known as “Dark Hotel”.

```
"bfsdrv","!!! PSP: 360Safe Security Center !!!"
"BHDrvx86","!!! PSP: Symantec BASH Driver !!!"
"bidpoda","*** UNKNOWN - PLEASE PULL BACK ***"
"bifsgcom","*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***"
"bihokpkg","*** UNKNOWN - PLEASE PULL BACK ***"
"BIOS","BIOSTAR I/O Interface Driver"
"biosfix","*** SIG25 - FOLLOW GUIDANCE ***"
"BisonCam","BisonCam USB 2.0 Camera Driver"
"bitcheck","*** SIG25 - FOLLOW GUIDANCE ***"
"BlackCat","!!! PSP: RealSecure IDS !!!"
```

There are remarks for own tools:

*"mscnsp","*** FORMALRITE/UNITEDRAKE ***"*

*"mscoreep","*** FOGGYBOTTOM/UNITEDRAKE ***"*

and other interesting remarks:

*"msfcvr32","*** DANGEROUS MALWARE - SEEK HELP ASAP ***"*

*"msrsfler","*** UNKNOWN - PLEASE PULL BACK ***"*

*"wmiapvrr", "*** FRIENDLY TOOL - SEEK HELP ASAP ***"*

*"bsdnfs", "*** SEEK HELP IMMEDIATELY ***"*

More similar remarks can be found in the end of this document.

2. Summary table of SIG marked attacks and timeline

SIG no.	Possible APT other name	First public report	remarks
SIG1	Agent.BTZ (Turla?)	2008.06.X ? 2008.11.19.	
SIG2	Turla	2008.11.X. 2014.02.15. ?	
SIG3	ShipUp?	2008.10.29.	
SIG4	Snake/Uroburos	2014.02.28.	dated 3+ years old
SIG5	Trojan dropper Agent.ikcb Turla tool?	2013.10.15.	
SIG6	?	?	
SIG7	GhoTex	2007.03.04.	Octa-B?
SIG8	Stuxnet 2 drivers unknown s7otbxdxa.sys s7obxsx.sys	2010.06.15.	Dated dev.: 2005~
SIG9	Flame	2012.05.28.	Dated dev.: 2010~
SIG10	miniFlame	2012.10.15.	
SIG11	?	?	
SIG12	Spuler?	2012.11.26?	
SIG13	Agent.BTZ?	see 1	
SIG14	?	?	
SIG15	Turla/Snake/Uroburos	PDF:2015	
SIG16	Flame	2012.05.28.	
SIG17	SunFlower / Chesire Cat / Flowershop	~2015	samples point back to 2002
SIG18	Moonflower / Chesire Cat / Flowershop (sunflower moonflower)	?	
SIG19	?	?	
SIG20	Animal Farm	2015.03.06.	in use since 2013?
SIG21	?	?	
SIG22	Aurora/Hydraq	2010.01.12.	Op: 2009.06-12
SIG23	Turla (Epic Turla)	2014.08.07.	Under analysis for 10 months
SIG24	?	?	
SIG25	Dark Hotel	2014.11.10.	
SIG26	?	?	
SIG27	?	?	
SIG28	Rotinom	2011.01.11.	
SIG29	?	?	
SIG30	Exforel	2012.11.28.	
SIG31	?	?	
SIG32	?	2008.06.13.	
SIG33	?	?	
SIG34	?	2014.05.14.	
SIG35	Duqu	2011.09.01.	
SIG36	Stuxnet/Duqu?	see 8 / 35	
SIG37	IronTiger_ASPXSpy	?	
SIG38	?	?	
SIG39	Teamspy	2013.03.10.	
SIG40	Sednit/Sofacy	2015.02.09.	
SIG41	?	2011.03.29.	
SIG42	?	?	

SIG43	Turla	see 2, 2014.01.X	
SIG44	?	?	
SIG45	?	?	

..

..

Details

3. SIG1

IoC	type, method	remarks
software\microsoft\windows\currentversion\StrtdCfg	reg.key.	

Table 1 – IoC list in leaked material – SIG1

This might be Agent.BTZ, which is an old attack associated with Waterbug/Turla group (most common attribution: Russia) https://www.f-secure.com/v-descs/worm_w32_agent_btz.shtml https://www.wired.com/2008/11/army-bans-usb-d/ http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html

Table 2 – Related links, information – SIG1

please check separate file with hash list too. Note, there should be many FPs.

Table 3 – hashes of possibly related files – SIG1

4. SIG2

IoC	type, method	remarks
System\CurrentControlSet\Control\CrashImage	reg. key.	
atmarpd.sys	driver	

Table 4 – IoC list in leaked material – SIG2

Might be Turla (most common attribution: Russia) https://totalhash.cymru.com/analysis/?4dd95ce1ec9941f362d4a6ceb65ab915dbfd9458 https://virustotal.com/hu/file/71eb7c15a026d011cca82fed8b634c10b569bb6b0cda1af532287218b9ee110f/analysis/ The analysis shows „crashimage” registry key This sample also has CC servers: pressbrig1[.]tripod.com and www[.]scifi.pages.at/wordnew

Table 5 – Related links, information – SIG2

4dd95ce1ec9941f362d4a6ceb65ab915dbfd9458 71eb7c15a026d011cca82fed8b634c10b569bb6b0cda1af532287218b9ee110f please check separate file with hash list too. Note, there should be many FPs.

Table 6 – hashes of possibly related files – SIG2

5. SIG3

IoC	type, method	remarks
SYSPATH\driver32	directory	
SYSPATH\driver32\ldf	directory	
SYSPATH\driver32\ldf*	file	

Table 7 – IoC list in leaked material – SIG3

```
https://www.trendmicro.com/vinfo/us/threat-
encyclopedia/archive/malware/troj_shipup.ar
https://www.mcafee.com/threat-intelligence/malware/default.aspx?id=141194

mwrepos mintak shipup vtn
```

Table 8 – Related links, information – SIG3

```
most interesting ones:
bf9eba33cf5f161ae8260732ba0a80fbfacac99957d6b9fd4ca36795175dc798
b3df5e63a72bf60c5ffda75e663037463874ccd446f123fca3630e7ce3f3b23a
febc132c608fe85ecf4b235b80426cf2d722143fbfee5996fdaa167509115e60
9e97a774cfc8a92e9f2dd6e074784dea215eceaf3dc90a560164aad98b9f9052
53c0d4d159aad1022bd8c7df263921c9799bd31ee75515c84d05a77584ccf539
d431ba45cc2182f7c9e153586a6b153a286ccfcd4f26d83d246c3611d48fced9

Please check separate file with hash list too. Note, there should be many FPs.
```

Table 9 – hashes of possibly related files – SIG3

6. SIG4

IoC	type, method	remarks
SYSTEMROOT\$NtUninstallQ817473$	directory	
\\.\Hd1	file	
\\.\Hd2	file	
\\.\IdeDrive1	file	
\\.\IdeDrive2	file	
fdisk.sys	driver	

Table 10 – IoC list in leaked material – SIG4

```
http://blog.talosintelligence.com/2014/04/snake-campaign-few-words-about-
uroburos.html
http://thehackernews.com/2014/03/uroburos-rootkit-most-sophisticated-3.html
etc.
```

Table 11 – Related links, information – SIG4

33460a8f849550267910b7893f0867afe55a5a24452d538f796d9674e629acc4 please check separate file with hash list too. Note, there should be many FPs.

Table 12 – hashes of possibly related files – SIG4

7. SIG5

IoC	type, method	remarks
systmgmt	service	
syswpsvc.sys	driver	
system\currentcontrolset\services\systmgmt\Parameters\ ServiceDll	reg.key – value name	

Table 13 – IoC list in leaked material – SIG5

https://home.mcafee.com/virusinfo/virusprofile.aspx?key=4367516#none

Table 14 – Related links, information – SIG5

453F502CF1DB45BF234600D50127EC8FAD1003A6 please check separate file with hash list too. Note, there should be many FPs.

Table 15 – hashes of possibly related files – SIG5

8. SIG6

IoC	type, method	remarks
Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\ipmontr	reg. key	
Software\Microsoft\WinKernel\Explorer\Run\ipmontr	reg.key	
ipconfhlp.sys	driver	
SYSPATH\ipmontr.exe	file	
SYSPATH\ipconfhlp.dll	file	

Table 16 – IoC list in leaked material – SIG6

Win32.Lucuis.A relationship? http://telussecuritylabs.com/threats/show/TSL20120120-06

Table 17 – Related links, information – SIG6

63d5d58cb833f84c4c2687a7cb8303ca1306022ba01f68337d2180fd6521def8 please check separate file with hash list too. Note, there should be many FPs.

Table 18 – hashes of possibly related files – SIG6

9. SIG7

IoC	type, method	remarks
Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\Internet32	reg. key	might be a typo in the NSA IOC?
internat.sys	driver	
SYSPATH\internat32.exe	file	
SYSPATH\sbool\msadp32.exe	file	
SYSPATH\Internat.dll	file	

Table 19 – IoC list in leaked material – SIG7

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Octa-B/detailed-analysis.aspx Ghotexinternat.sys https://www.symantec.com/security_response/writeup.jsp?docid=2003-040713-2623-99&tabid=2 Ghotex https://www.symantec.com/security_response/writeup.jsp?docid=2003-040713-2623-99&tabid=2

Table 20 – Related links, information – SIG7

please check separate file with hash list too. Note, there should be many FPs.

Table 21 – hashes of possibly related files – SIG7

10. SIG8

IoC	type, method	remarks
SYSPATH\s7otbxsx.dll	file	
SYSTEMROOT\inf\mdmcpq3.pnf	file	
mrxcls	service	
s7otbxsx.sys	driver	
mrxcls.sys	driver	
mrxnet.sys	driver	
s7otbxdxa.sys	driver	
jmidebs.sys	driver	
_LPDIR_LOGS\Get_Files	directory	

Table 22 – IoC list in leaked material – SIG8

StuxNet driver list contains: "mrxnet","*** SIG8 - FOLLOW GUIDANCE ***"

Table 23 – Related links, information – SIG8

b834ebeb777ea07fb6aab6bf35cdf07f ad19fbaa55e8ad585a97bbcddcde59d4 f8153747bae8b4ae48837ee17172151e cc1db5360109de3b857654297d262ca1 7a4e2d2638a454442efb95f23df391a1 5b855cff1dba22ca12d4b70b43927db7 ad19fbaa55e8ad585a97bbcddcde59d4 d102bdad06b27616babe442e14461059 b834ebeb777ea07fb6aab6bf35cdf07f please check separate file with hash list too. Note, there should be many FPs.

Table 24 – hashes of possibly related files – SIG8

11. SIG9

IoC	type, method	remarks
SYSTEMROOT\..\Program Files\common files\microsoft shared\msaudio	file/dir?	
SYSTEMROOT\..\Program Files\common files\microsoft shared\mssecuritymgr	file/dir?	
SYSTEMROOT\..\Program Files\common files\micfosoft shared\MSAPackages	file/dir?	

Table 25 – IoC list in leaked material – SIG9

https://securelist.com/blog/incidents/34344/the-flame-questions-and-answers-51/ https://www.crysys.hu/skywiper/skywiper.pdf

Table 26 – Related links, information – SIG9

please check separate file with hash list too. Note, there should be many FPs.

Table 27 – hashes of possibly related files – SIG9

12. SIG10

IoC	type, method	remarks
SYSPATH\icsvnt32.dll	file	
system\currentcontrolset\control\timezoneinformation\standarddatebias	reg. key	
system\currentcontrolset\control\timezoneinformation\standardtimebias	reg. key	
icsvnt32.sys	driver	

Table 28 – IoC list in leaked material – SIG10

https://securelist.com/analysis/publications/68560/miniflame-aka-spe-elvis-and-his-friends/3/ https://www.wired.com/2012/10/miniflame-espionage-tool/

Table 29 – Related links, information – SIG10

ce792f3ed7eaa53b1a26bf0d879e861f645413c7f629e6db8e14a5feff61e517 miniflame by ESET, 1st upload 2008 please check separate file with hash list too. Note, there should be many FPs.

Table 30 – hashes of possibly related files – SIG10

13. SIG11

IoC	type, method	remarks
ups32.exe	process	
utilman32.exe	process	
SYSPATH\ups32.exe	file/driver	
SYSPATH\utilman32.exe	file	
SYSPATH\utliman32.exe	file	
SYSPATH\drivers\ups.exe	file	
SYSPATH\msvcp11.dll	file	
SYSPATH\msxml10.dll	file	

Table 31 – IoC list in leaked material – SIG11

too general file names.

Table 32 – Related links, information – SIG11

Please check separate file with hash list too. Note, there should be many FPs.

Table 33 – hashes of possibly related files – SIG11

14. SIG12

IoC	type, method	remarks
SYSTEMROOT\..\Documents and Settings\All Users\Application Data\Network	directory	
Software\Microsoft\MSFix	reg. key	
w3ssl.sys	driver	

Table 34 – IoC list in leaked material – SIG12

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_dloadr.yq ? https://home.mcafee.com/virusinfo/virusprofile.aspx?key=1727735#none

Table 35 – Related links, information – SIG12

8805f1d7d603face71d5c926af7d7e84e7120456
c924855408cca3dc55555f5b9ad1e1f2ab3b3d1558e13e8464f3db4578d41056
12f5968b1d551f7a35adc482f5cfe957b1caf0513daba9c6c7187b478ddc81a7
23be7e7eeb654533ca82bd6564a6ddf53a31eb61f4793856106da7d979764fa8
9344b0b20a28fd50e28025c984cbeaff8216cfaab247dbca57f680f1356eec2a
9363ae91667316a3bbffaf47d181d84c8a832812b4d89a56e942b32337f76b9a
6e3a7fe487b928726fb55907faa344dcfd10b0e3c0bfc3c2e8268bd5baef19d1
ba5f55cca1d119fa602cc21b5b3dfbe2a47f5416ecdcf5c165ef635d5a4eeb62
Please check separate file with hash list too. Note, there should be many FPs.

Table 36 – hashes of possibly related files – SIG12

15. SIG13

IoC	type, method	remarks
SYSPATH\winview.ocs	file	
SYSPATH\Mfc42l00.pdb	file	
SYSPATH\ISUninst.bin	file	
SYSPATH\mswmpdat.tlb	file	
SYSPATH\wmmini.swp	file	
SYSPATH\wowmgr.exe	file	
SYSTEMROOT\winstat.pdr	file	
WOWmanager	service	

Table 37 – IoC list in leaked material – SIG13

```
Might be also Agent.BTZ related

('winstat.pdr' in datastore.SYSPATH_FILE_SET):
   return True
earch_set = set(('winview.ocs', 'Mfc42l00.pdb', 'ISUninst.bin',
'mswmpdat.tlb', 'wmmini.swp', 'wowmgr.exe'))

"The files "winview.ocx" and "mswmpdat.tlb" holds the log of the files
and their location that the malware has installed. The content of these
file are encrypted. The file "muxbde40.dll" is the malware itself with a
different name." – Origin: ??

https://www.mcafee.com/threat-intelligence/malware/default.aspx?id=305192
```

Table 38 – Related links, information – SIG13

```
6b3f6b6fb370836ea78bbfb68f00308d374a897c
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 39 – hashes of possibly related files – SIG13

16. SIG14

IoC	type, method	remarks
taskbar.exe	process	
MsgQueue.exe	process	
SndTray.exe	process	
msserv.exe	process	
SYSPATH\taskbar.exe	file	
SYSPATH\MsgQueue.exe	file	
SYSPATH\SndTray.exe	file	
SYSPATH\msserv.exe	file	
SYSPATH\sed.exe	file	
SYSPATH\winip.drv	file	
SYSPATH\winext32.dll	file	
SYSPATH\rpclog.dll	file	
c:\win\drivers\slidebar.exe	file	
Recover	service	
rpclog.sys	driver	
winext32.sys	driver	
winip.sys	driver	
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ newval	reg. key	
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ WindowsFirewallSecurityServ	reg. key	
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ slidebar	reg. key	
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ MSDeviceDriver	reg. key	
c:\\applicationdata\\appdata1\\logFile.txt	file	
%USERPROFILE%\\MyHood\\btmn\\system\\temp\\cnf.txt	file	
c:\\syslog\\temp\\012tg7\\system\\cnf.txt	file	

Table 40 – IoC list in leaked material – SIG14

No clue

Table 41 – Related links, information – SIG14

Please check separate file with hash list too. Note, there should be many FPs.

Table 42 – hashes of possibly related files – SIG14

17. SIG15

IoC	type, method	remarks
SYSPATH\tlbcon32.exe	file	
SYSPATH\con32.nls	file	
TlbControl	service	
Software\Postman	reg. key	

Table 43 – IoC list in leaked material – SIG15

https://webcache.googleusercontent.com/search?q=cache:8oUmzaCr0zoJ:https://kam.lt/download/48227/assessment%2520of%2520threat%2520to%2520national%2520security%25202015.pdf+&cd=3&hl=en&ct=clnk&gl=hu „According to the AOTD (which takes into account the trends in modification and development of the spyware observed in a number of years, also the technical details of computer investiga- tions into the spyware, and its characteristics), agent.btz and its latest versions (Snake rootkit, Turla, Uroburos) are the espionage tools developed by Russian cyber specialists and intended for strate- gic goals (the main ways to detect the spyware are provided in the annex)”

Table 44 – Related links, information – SIG15

Please check separate file with hash list too. Note, there should be many FPs.

Table 45 – hashes of possibly related files – SIG15

18. SIG16

IoC	type, method	remarks
SYSPATH\indsvc32.ocx	file	
SYSTEMROOT\temp\indsvc32.ocx	file	

Table 46 – IoC list in leaked material – SIG16

indsvc32.ocx / This should be Flame

Table 47 – Related links, information – SIG16

554924ebdde8e68cb8d367b8e9a016c5908640954ec9fb936ece07ac4c5e1b75 333875eb8a6baa773d69e38e8f05d914def30750fdec3d9f2c8fbb01efa80fe1 9bae0b89aa47f37f199d0b38ca8631020c9d221ea3e66aafecb7105c064ae343 c6776d9ebe91b2d33b3ac36c845528fd7a81b35095beffbd2ea080fe6eab67cf Please check separate file with hash list too. Note, there should be many FPs.

Table 48 – hashes of possibly related files – SIG16

19. SIG17

IoC	type, method	remarks
SYSPATH\ADWM.DLL	file	
SYSPATH\ASFIPC.DLL	file	
SYSPATH\BROWUI.DLL	file	
SYSPATH\CAPESPN.DLL	file	
SYSPATH\CFGKRNL3.DLL	file	
SYSPATH\CRYPTKRN.DLL	file	
SYSPATH\DESKKRNE.DLL	file	
SYSPATH\DSKMGR.DLL	file	
SYSPATH\EXPLORED.DLL	file	
SYSPATH\FMEM.DLL	file	
SYSPATH\HDDBACK4.DLL	file	
SYSPATH\HWMAP.DLL	file	
SYSPATH\ipnetd.dll	file	
SYSPATH\IPNETD.DLL	file	
SYSPATH\KNRLADD.DLL	file	
SYSPATH\MAILAPIC.DLL	file	
SYSPATH\MSGRTHLP.DLL	file	
SYSPATH\MSIAXCPL.DLL	file	
SYSPATH\MSID32.DLL	file	
SYSPATH\MSRECV40.DLL	file	
SYSPATH\NCFG.DLL	file	
SYSPATH\PARALEUI.DLL	file	
SYSPATH\secur16.dll	file	
SYSPATH\SECUR16.DLL	file	
SYSPATH\SOUNDLOC.DLL	file	
SYSPATH\WINF.DLL	file	
SYSPATH\WMCRT.DLL	file	
Lnkfile\shellex\IconHandler\OptionFlags	reg. key – value name	
ndisalex.sys	driver	
ndisio32.sys	driver	
paravdm.sys	driver	
SYSPATH\wbem\logs	file	
SYSTEMROOT\help*	file	
SYSTEMROOT\..\Program Files\common files\system\msadc*	file	

igure 49 – IoC list in leaked material – SIG17

SIG17 and SIG18 might be Flowershop related SunFlower and MoonFlower samples. AKA Cheshire Cat. They are also called „Flowershop”. Might be related to Duqu, Stuxnet and might attributed to Israel. https://github.com/Yara-Rules/rules/blob/master/malware/APT_CheshireCat.yar See https://malware-research.org/prepare-father-of-stuxnet-news-are-coming/

Table 50 – Related links, information – SIG17

32159d2a16397823bc882ddd3cd77ecdbabe0fde934e62f297b8ff4d7b89832a 63735d555f219765d486b3d253e39bd316bbcb1c0ec595ea45ddf6e419bef3cb c074aeef97ce81e8c68b7376b124546cabf40e2cd3aff1719d9daa6c3f780532 dc18850d065ff6a8364421a9c8f9dd5fcce6c7567f4881466cee00e5cd0c7aa8 ec41b029c3ff4147b6a5252cb8b659f851f4538d4af0a574f7e16bc1cd14a300 Please check separate file with hash list too. Note, there should be many FPs.

Table 51 – hashes of possibly related files – SIG17

20. SIG18

IoC	type, method	remarks
SYSTEMROOT\..\Documents and Settings\All Users\Application Data\msncp.exe	file	
SYSTEMROOT\..\Documents and Settings\All Users\Application Data\netsvcs.exe	file	
SYSPATH\msprnt.exe	file	
SYSPATH\fmem.dll	file	
SYSTEMROOT\..\Program Files\common files\microsoft shared\Triedit\htmlprsr.exe	file	
SYSTEMROOT\..\Program Files\common files\microsoft shared\Triedit\dhtmled.dll	file	
SYSTEMROOT\..\Program Files\common files\microsoft shared\Triedit\TRIEDIT.TLB	file	
pnppci	service	
ethio	service	
ntdos505	service	
ndisio	service	
dhtmled.sys	driver	
ethio.sys	driver	
fmem.sys	driver	
ntdos505.sys	driver	
pnppci.sys	driver	
triedit.sys	driver	
vgx.sys	driver	

Table 52 – IoC list in leaked material – SIG18

Moonflower / FlowerShop

Table 53 – Related links, information – SIG18

6719FF0EAB92F8C88C0E34CB54EA92BB (questionable) Please check separate file with hash list too. Note, there should be many FPs. Also note the lot of IoCs and the lack of public knowledge about FlowerShop. It should be investigated in depth if possible.

Table 54 – hashes of possibly related files – SIG18

21. SIG19

IoC	type, method	remarks
SYSPATH\nsecm.dll	file	
nsecm.sys	driver	

Table 55 – IoC list in leaked material – SIG19

No clue

Table 56 – Related links, information – SIG19

Please check separate file with hash list too. Note, there should be many FPs.

Table 57 – hashes of possibly related files – SIG19

22. SIG20

IoC	type, method	remarks
SYSPATH\Microsoft\Windows Management Infrastructure	directory	
WinMI32	service	
Software\Microsoft\WinMI	reg. key	
SYSTEMROOT\svchost00000000-0000-0000-0000-0000-00000000.dat	file	
PROFILE_PATH\All Users\update.msi	file	
PROFILE_PATH\All Users\Application Data\update.msi	file	
$(ProgramData)\MSI\update.msi	file	
PROGRAM_FILES\Common Files\wusvcd.exe	file	
PROGRAM_FILES\Common Files\wusvcd\wusvcd.exe	file	
SYSTEMROOT\Microsoft\ Windows Management Infrastructure	directory	
SYSTEMROOT\..\ Documents and Settings\ *\Application Data\Microsoft\wmimgnt.dll	file	
SYSTEMROOT\..\ Documents and Settings\ *\Application Data\Microsoft\wmimgnt.exe	file	

Table 58 – IoC list in leaked material – SIG20

https://www.welivesecurity.com/2015/06/30/dino-spying-malware-analyzed/ https://securelist.com/blog/research/69114/animals-in-the-apt-farm/

Animal farm is possibly attack of french intelligence. „Dino” „Babar” „Dinotransport” „Evilbunny” and others are part of it. In Snowden released document canadian sources also noted it is french. Check for „SnowGlobe”.

Table 59 – Related links, information – SIG20

7ba09403e9d7122a20fa510de11f7809822e6e11efb164414e2148b762cf4e75 Please check separate file with hash list too. Note, there should be many FPs.

Table 60 – hashes of possibly related files – SIG20

23. SIG21

IoC	type, method	remarks
SYSTEMROOT\temp\temp56273.pdf	file	
SYSTEMROOT\..\ Documents and Settings\ *\Local Settings\History\cache\iecache.dll	file	

Table 61 – IoC list in leaked material – SIG21

No clue

Table 62 – Related links, information – SIG21

Please check separate file with hash list too. Note, there should be many FPs.

Table 63 – hashes of possibly related files – SIG21

24. SIG22

IoC	type, method	remarks
SYSPATH\drivers\etc\network.ics	file	
SYSPATH\acelpvc.dll	file	
Software\Sun\1.1.2\AppleTlk	reg. key	
Software\Sun\1.1.2\AppleTlk	reg. key – value name	
Software\Sun\1.1.2\IsoTp	reg. key	
Software\Sun\1.1.2\IsoTp	reg. key – value name	
acelpvc.sys	driver	

Table 64 – IoC list in leaked material – SIG22

```
The IoCs:
    HKEY_LOCAL_MACHINE\Software\Sun\1.1.2\"IsoTp"
    HKEY_LOCAL_MACHINE\Software\Sun\1.1.2\"AppleTlk
    acelpvc.sys
can relate to Hydraq, which possibly relates to the Aurora attack.

https://www.symantec.com/security_response/writeup.jsp?docid=2010-011114-1830-
99&tabid=2
https://www.wired.com/2010/03/source-code-hacks/

https://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-
exploit

https://www.symantec.com/connect/blogs/trojanhydraq-incident
```

Table 65 – Related links, information – SIG22

```
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 66 – hashes of possibly related files – SIG22

25. SIG23

IoC	type, method	remarks
software\microsoft\NetWin	reg. key	

Table 67 – IoC list in leaked material – SIG23

```
https://malwr.com/analysis/ZTdlNjRmMGNhMzQzNGE5ZjhkM2Q5YmM1MjQzYzAwOWI/
http://www.crysys.hu/turlaepiccc/turla_epic_cc_v1.pdf
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/
```

Table 68 – Related links, information – SIG23

```
2007aa72dfe0c6c93beb44f737b85b6cd487175e7abc6b717dae9344bed46c6c
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 69 – hashes of possibly related files – SIG23

26. SIG24

IoC	type, method	remarks
SYSPATH\drivers\mfc64comm.sys	file	
SYSPATH\drivers\adap64info.sys	file	
adap64info.sys	driver	
mfc64comm.sys	driver	

Table 70 – IoC list in leaked material – SIG24

```
No clue
```

Table 71 – Related links, information – SIG24

```
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 72 – hashes of possibly related files – SIG24

27. SIG25

IoC	type, method	remarks
HP003044	service	
NetBIOS2010	service	
SYSTEMROOT\winver32.exe SYSPATH\actmove.exe SYSPATH\appned.exe SYSPATH\boof.exe SYSPATH\gflash.exe SYSPATH\lnetcpl.exe SYSPATH\qernet.exe SYSPATH\serves.exe SYSPATH\secury.exe SYSPATH\webhelp.exe SYSPATH\autocheck.exe SYSPATH\xflash.exe SYSPATH\inetcpl.exe SYSPATH\activemov.exe SYSPATH\xmlhelp.exe SYSPATH\winspooler.exe SYSPATH\xsocket.exe SYSPATH\actmove.exe SYSPATH\appned.exe SYSPATH\qernet.exe SYSPATH\boof.exe SYSPATH\gflash.exe SYSPATH\lnetcpl.exe SYSPATH\serves.exe SYSPATH\secury.exe SYSPATH\actmove.exe SYSPATH\appned.exe SYSPATH\boof.exe SYSPATH\gflash.exe SYSPATH\lnetcpl.exe SYSPATH\qernet.exe SYSPATH\serves.exe SYSPATH\secury.exe SYSPATH\actmove.sys SYSPATH\appned.sys SYSPATH\boof.sys SYSPATH\gflash.sys SYSPATH\lnetcpl.sys SYSPATH\qernet.sys SYSPATH\serves.sys SYSPATH\secury.sys SYSPATH\webhelp.sys SYSPATH\autocheck.sys SYSPATH\xflash.sys SYSPATH\inetcpl.sys SYSPATH\activemov.sys SYSPATH\xmlhelp.sys SYSPATH\winspooler.sys SYSPATH\xsocket.sys	file	

SYSPATH\actmove.sys SYSPATH\appned.sys SYSPATH\qernet.sys SYSPATH\boof.sys SYSPATH\gflash.sys SYSPATH\lnetcpl.sys SYSPATH\serves.sys SYSPATH\secury.sys SYSPATH\actmove.sys SYSPATH\appned.sys SYSPATH\boof.sys SYSPATH\gflash.sys SYSPATH\lnetcpl.sys SYSPATH\qernet.sys SYSPATH\serves.sys SYSPATH\secury.sys SYSPATH\DivXfix.dll SYSPATH\dbdebug.dll SYSPATH\countryfix.dll SYSPATH\cdboot.dll SYSPATH\bitcheck.dll SYSPATH\biosfix.dll SYSPATH\actproxy.dll SYSPATH\activems.dll SYSPATH\dbdebug.dll SYSPATH\countryfix.dll SYSPATH\cdboot.dll SYSPATH\bitcheck.dll SYSPATH\DivXfix.dll SYSPATH\biosfix.dll SYSPATH\actproxy.dll SYSPATH\dsound4d.dll SYSPATH\actmove.dll SYSPATH\appned.dll SYSPATH\qernet.dll SYSPATH\boof.dll SYSPATH\gflash.dll SYSPATH\lnetcpl.dll SYSPATH\serves.dll SYSPATH\secury.dll SYSPATH\actmove.dll SYSPATH\appned.dll SYSPATH\boof.dll SYSPATH\gflash.dll SYSPATH\lnetcpl.dll SYSPATH\qernet.dll SYSPATH\serves.dll SYSPATH\secury.dll		
activemov.sys activems.sys actmove.sys actproxy.sys appned.sys autocheck.sys biosfix.sys bitcheck.sys boof.sys	driver	

cdboot.sys countryfix.sys dbdebug.sys divxfix.sys dsound4d.sys gflash.sys lnetcpl.sys qernet.sys secury.sys serves.sys webhelp.sys winspooler.sys xflash.sys xmlhelp.sys xsocket.sys		
SYSTEMROOT\..\ Documents and Settings*\Application Data\winver32.exe		

Table 73 – IoC list in leaked material – SIG25

It is most likely DarkHotel APT (most common attribution: DPKR) IoC related information: https://www.virustotal.com/hu/file/de4ff8901766e8fc89e8443f8732394618bf925ce29b6a8a afe1d60f496e7f0e/analysis/ Additional links: http://securelist.com/blog/research/66779/the-darkhotel-apt/ https://blog.kaspersky.com/darkhotel-apt/6613/

Table 74 – Related links, information – SIG25

de4ff8901766e8fc89e8443f8732394618bf925ce29b6a8aafe1d60f496e7f0e Please check separate file with hash list too. Note, there should be many FPs.

Table 75 – hashes of possibly related files – SIG25

28. SIG26

IoC	type, method	remarks
Software\Adobe\Fix	reg. key	
PROFILE_PATH*\Local Settings\Temp\result.dat	file	
PROFILE_PATH*\Local Settings\Temp\data.dat	file	
PROFILE_PATH*\Local Settings\Temp\Acrobat.dll	file	
PROFILE_PATH*\Local Settings\Temp\first.tmp	file	

Table 76 – IoC list in leaked material – SIG26

No clue

Table 77 – Related links, information – SIG26

Please check separate file with hash list too. Note, there should be many FPs.

Table 78 – hashes of possibly related files – SIG26

29. SIG27

IoC	type, method	remarks
SYSTEMROOT\qtlib.sqt	file	
SYSTEMROOT\zl4vq.sqt	file	
SYSTEMROOT\dfrgntfs5.sqt	file	
SYSTEMROOT\msvcrt58.sqt	file	

Table 79 – IoC list in leaked material – SIG27

No Clue. Sqt might be related to SAP. Some think maybe it is connected to Lazarus attacks.

Table 80 – Related links, information – SIG27

Please check separate file with hash list too. Note, there should be many FPs.

Table 81 – hashes of possibly related files – SIG27

30. SIG28

IoC	type, method	remarks
SYSTEMROOT\..\ Documents and Settings*\Local Settings\Application Data\S-1-5-31-1286970278978-5713669491-166975984-320*	file	

igure 82 – IoC list in leaked material – SIG28

```
very limited information available.

https://www.symantec.com/security_response/writeup.jsp?docid=2011-011117-0057-
99&tabid=2
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_hidfile.ab

Rotinom.A https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-
description?Name=%0A%09%09%09%09Trojan:Win32/Rotinom.A%0A%09%09%09%09&ThreatID=%0A%
09%09%09%09-2147413137%0A%09%09%09%09
https://www.mcafee.com/threat-intelligence/malware/default.aspx?id=253485
https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_cmse.a
```

Table 83 – Related links, information – SIG28

```
4f9786ddd6e75750221c59dcecc6e84822cf6050
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 84 – hashes of possibly related files – SIG28

31. SIG29

IoC	type, method	remarks
SYSPATH\ieloader.dll	file	
SYSPATH\orepst.dll	file	
SYSPATH\pstore.dll	file	

igure 85 – IoC list in leaked material – SIG29

```
No clue
```

Table 86 – Related links, information – SIG29

Please check separate file with hash list too. Note, there should be many FPs.

Table 87 – hashes of possibly related files – SIG29

32. SIG30

IoC	type, method	remarks
SYSPATH\msdxofg.dll	file	
SYSPATH\ocmsiecon.hlp	file	
SYSPATH\atllib.dll	file	
ndisxapi.sys	driver	

Table 88 – IoC list in leaked material – SIG30

```
Most likely, this is „Exforel”
http://sha1.virscan.org/492dc600e22de6da96898e097566bc01309b5996.html
http://artemonsecurity.blogspot.hu/2012/12/analysis-of-virtoolwinntexforela-
rootkit.html
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-
description?Name=VirTool:WinNT/Exforel.A
Exforel might be related some top secret space project espionage
public information is scarce
```

Table 89 – Related links, information – SIG30

```
b338b7f6fdaa187583ce858cd0dcfee08e4dc66edebad321d3f5bd23548b2fb5 40960 bytes
5e49440b907b271eb952101b5d337625b890d88a76a232ce04a2276542dfb4b0
668ce24473d788791d2bfee0caec2d10dca52b5bc8c021bf06f9eb3527688ade
6f8e344bb529364ca5bab7f0d73216437040e9922917e2e85a862bcb2a90929c
some texts in them relate to China. Maybe victim related.
```

Table 90 – hashes of possibly related files – SIG30

33. SIG31

IoC	type, method	remarks
SYSTEMROOT\temp\~MS1E.tmp	file	
SYSTEMROOT\temp\~FMIFEN.tmp	file	
SYSPATH\wpa.dbl.bak	file	
SYSPATH\sslkey.exe	file	
SYSTEMROOT\WindowsUpdate.old	directory	
Software\Microsoft\Windows\CurrentVersion\Explorer\Streams \Desktop\Default Statusbar Sign	reg. key	
Software\Microsoft\Windows\CurrentVersion\Explorer\Streams \Desktop\Default MenuBars Sign	reg. key	

Software\Microsoft\Windows\CurrentVersion\Explorer\Streams \Desktop\Default Taskbar Sign	reg. key	
Software\Microsoft\Windows\CurrentVersion\Explorer\Streams \Desktop\Default Zone	reg. key	

Table 91 – IoC list in leaked material – SIG31

No clue

Table 92 – Related links, information – SIG31

Please check separate file with hash list too. Note, there should be many FPs.

Table 93 – hashes of possibly related files – SIG31

34. SIG32

IoC	type, method	remarks
Software\Microsoft\Active Setup\Installed Components\{FB083534-2709-3378-0000-F0FCD03BA387}	reg. key	
Software\Microsoft\Active Setup\Installed Components\{FB083534-2709-3378-0001-F0FCD03BA387}	reg. key	

Table 94 – IoC list in leaked material – SIG32

```
https://home.mcafee.com/virusinfo/virusprofile.aspx?key=145695#none

https://www.trendmicro.com/vinfo/us/threat-
encyclopedia/archive/malware/bkdr_horst.jw
```

Table 95 – Related links, information – SIG32

```
192805e26bb4b8ecb7579bb38fdc1adc2d63f55f03b1c221a377d72ca3ef29f0 36864 bytes
417542fd4be726db4e9ce3c24eb26f9b7c82cfaea1f918ced567c67a098fd2a6 5052 bytes
5cda2f749e59cd4e364ff54d347f776dee78632fc75e7f949e0f36429571fa68 134744 bytes
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 96 – hashes of possibly related files – SIG32

35. SIG33

IoC	type, method	remarks
SYSPATH\INI	directory	

Table 97 – IoC list in leaked material – SIG33

```
No Clue
```

Table 98 – Related links, information – SIG33

```
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 99 – hashes of possibly related files – SIG33

36. SIG34

IoC	type, method	remarks
System\CurrentControlSet\Services\Windows Installer Management	reg. key	

Table 100 – IoC list in leaked material – SIG34

```
https://www.virustotal.com/en/file/2db467faac6a4a29d735a61e62310a0d5090019d72bebf79
3684c7c36817de3c/analysis/
https://home.mcafee.com/virusinfo/virusprofile.aspx?key=7825284
Not clear
```

Table 101 – Related links, information – SIG34

```
2db467faac6a4a29d735a61e62310a0d5090019d72bebf793684c7c36817de3c
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 102 – hashes of possibly related files – SIG34

37. SIG35

IoC	type, method	remarks
adpu321.sys	driver	
hpnd5x86.sys	driver	
igdkmd16b.sys	driver	
msgdi32.sys	driver	
mssfdr.sys	driver	
mssloct.sys	driver	
mssygx.sys	driver	This might be a 2007 year old duqu dirver
ntrbos.sys	driver	
qd240x86.sys	driver	
qd260x86.sys	driver	

Table 103 – IoC list in leaked material – SIG35

```
This SIG is most likely related to Duqu.

Looks for kernel driver of 9472 bytes. Very strange check, we are not aware of any
Duqu kernel driver that was 9472 bytes long.
```

Table 104 – Related links, information – SIG35

Please check separate file with hash list too. Note, there should be many FPs.

Table 105 – hashes of possibly related files – SIG35

38. SIG36

IoC	type, method	remarks
LOGDIRECTORY\Data*processinfo*\kernel32.dll.aslr	file	
LOGDIRECTORY\Data*processinfo*\sort*.nls	file	
LOGDIRECTORY\Logs*processinfo*\kernel32.dll.aslr	file	
LOGDIRECTORY\Logs*processinfo*\kernel32.dll.aslr	file	

Table 106 – IoC list in leaked material – SIG36

Maybe Stuxnet. But why separate detection. Why those indicators?

Table 107 – Related links, information – SIG36

f0d2306186da1e0d73e95eb098a2a63d1026671359433831cc57d6de853ebfd5 a1daf65f9c6042b347bf6df3eef7c04c19eb6086176c8fee6196bc4d1af13a13 3de70d94e6448752a7758484d887e80fd0c42a370c7a3f9cdb1cff103308df43

Table 108 – hashes of possibly related files – SIG36

39. SIG37

IoC	type, method	remarks
SYSTEMROOT\godown.dll	file	
SYSPATH\godown.dll	file	

Table 109 – IoC list in leaked material – SIG37

```
IronTiger_ASPXSpy
https://www.virustotal.com/#/file/fb253831862d882b0d22cb2cb2a80d423cae92a6218ac3d12
6fafcadf75afd0b/community
https://repo.cryptam.com/reports/fb253831862d882b0d22cb2cb2a80d423cae92a6218ac3d126
fafcadf75afd0b.html
```

Table 110 – Related links, information – SIG37

```
fb253831862d882b0d22cb2cb2a80d423cae92a6218ac3d126fafcadf75afd0b
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 111 – hashes of possibly related files – SIG37

40. SIG38

IoC	type, method	remarks
SYSPATH\winns.exe	file	
SYSPATH\kbdarpe.dll	file	
SYSTEMROOT\winns.exe	file	
SYSTEMROOT\kbdarpe.dll	file	

Table 112 – IoC list in leaked material – SIG38

```
No clue
```

Table 113 – Related links, information – SIG38

```
Please check separate file with hash list too. Note, there should be many FPs.
```

Table 114 – hashes of possibly related files – SIG38

41. SIG39

IoC	type, method	remarks
Software\\Microsoft\\MS QAG\\U11	reg. key	
Software\\Microsoft\\MS QAG\\U12	reg. key	

Table 115 – IoC list in leaked material – SIG39

Teamspy: https://www.crysys.hu/teamspy/teamspy.pdf

Table 116 – Related links, information – SIG39

Please check separate file with hash list too. Note, there should be many FPs.

Table 117 – hashes of possibly related files – SIG39

42. SIG40

IoC	type, method	remarks
Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad	reg. key	
Software\Microsoft\Windows\\CurrentVersion\ShellServiceObjectDelayLoad\NetIDS	reg. key – value name	

Table 118 – IoC list in leaked material – SIG40

https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Sednit-C/detailed-analysis.aspx https://virustotal.com/en/file/7f6f9645499f5840b59fb59525343045abf91bc57183aae459dca98dc8216965/analysis/

Table 119 – Related links, information – SIG40

7f6f9645499f5840b59fb59525343045abf91bc57183aae459dca98dc8216965

Please check separate file with hash list too. Note, there should be many FPs.

Table 120 – hashes of possibly related files – SIG40

43. SIG41

IoC	type, method	remarks
PROGRAM_FILES\common files\Log	file/directory?	
PROGRAM_FILESX86\common files\Log	file/directory?	
software\microsoft\windows nt\currentversion\ winlogon\Userinit == svchost	reg. key – value	

Table 121 – IoC list in leaked material – SIG41

https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/troj_swisyn.smfp https://www.virustotal.com/en/file/322cc4328e46bad28f12d1e4aa781c1cc6bcfb22fa24bb6a2eac6bd07fa8fc44/analysis/ https://home.mcafee.com/virusinfo/virusprofile.aspx?key=964778 https://www.symantec.com/security_response/writeup.jsp?docid=2006-071111-0646-99

Table 122 – Related links, information – SIG41

bad7b98554f38ad3883d3f864777c8806f7797a0 Please check separate file with hash list too. Note, there should be many FPs.

Table 123 – hashes of possibly related files – SIG41

44. SIG42?

IoC	type, method	remarks

Table 124 – IoC list in leaked material – SIG42

Table 125 – Related links, information – SIG42

aaaaa

Table 126 – hashes of possibly related files – SIG42

45. SIG43

IoC	type, method	remarks
%appdata%Help\\system32\cryptapi32.dll	file	
SYSTEM\CurrentControlSet\Control\DType0	reg.key – value name	
SYSPATH\cryptapi32.dll	file	
SYSTEMROOT\cryptapi32.dll	file	
%system%\mtmon.sdb	file	

Table 127 – IoC list in leaked material – SIG43

Sounds like turla, but not sure

Table 128 – Related links, information – SIG43

aaaaa

Table 129 – hashes of possibly related files – SIG43

46. SIG44

IoC	type, method	remarks
SYSPATH\rasmgr.dll	file	
SYSTEMROOT\rasmgr.dll	file	
SYSPATH\raseap.dll	file	
SYSTEMROOT\raseap.dll	file	
%windir%\AppPatch\rasmain.sdb	file	
%ProgramFiles%\Common Files\System\ado\msado39.tlb	file	
%ProgramFiles%\Common Files\System\ado\msado29.tlb	file	

Table 130 – IoC list in leaked material – SIG44

Flowershop? Or FP ransomware: https://www.virustotal.com/#/file/9d9697509adfd039f214b036497c16c21395f97eb8a58847ae46e7f37846414a/details

Table **131 – Related links, information – SIG44**

9d9697509adfd039f214b036497c16c21395f97eb8a58847ae46e7f37846414a 8131e0ad082a7c0f0c8ecd1699f4d7480e6e535c04e1514543727ca31d630a1d cdcb5144c36c3aee7604fbafa191c51475ff11eaf7e2fba1bdf4f836edc4cda5

e9dd6420aa2db28ae5eeb3963d020e1873de8e3109bfcb38e9116b9e51377969 47a49caaa6bd9bb4014f311369a610bdd0405eb36b19ed5f88ef232b0ac43483 ce363e58b8654642fee57ea84e9b3ca82393bb621d4822b964487912e1cf3f53 Please check separate file with hash list too. Note, there should be many FPs.

Table 132 – hashes of possibly related files – SIG44

47. SIG45

IoC	type, method	remarks
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ Internet	reg.key – value name	
C:\WINDOWS\system32\Microsoft\Protect\Windows\svshost.exe	file	
C:\WINDOWS\system32\Microsoft\Protect\Windows\svchost.exe	file	
%windir%\AppPatch\rasmain.sdb	file	

Table 133 – IoC list in leaked material – SIG45

No clue

Table 134 – Related links, information – SIG45

Please check separate file with hash list too. Note, there should be many FPs.

Table 135 – hashes of possibly related files – SIG45

Related samples found in our malware repository

We made Yara rules based on the SIG detections and ran a scan across on our malware database. The database contains around 150 TB malware samples. After finishing the scan process some 290 000 malware samples were collected. Many of them are evidently false positives, e.g. the string adobe.dll can be found in many thousands of samples.

The yara rules we used were based on the IoCs. However, as malware samples won't contain whole path, we had to transform the IoCs into some strings that have a chance to be found in malicious binaries.

We tried to clean up those items that seemed to be very likely false positives. At the end we have a collection of **5162** possibly related samples. The table below shows the number of possible related hashes found by this method for each SIG.

sig2	14
sig3	6
sig4	300
sig5	1
sig6	370
sig7	139
sig8	186
sig9	794
sig10	1
sig12	6
sig13	21
sig15	60
sig16	4
sig17	770
sig19	1
sig20	15
sig22	25
sig25	695
sig28	7
sig30	25
sig31	112
sig35	4
sig38	41
sig40	2
sig44	6
sig45	1557

Note, that this list contains not all known samples for each attack (e.g. for Stuxnet there are hundreds of thousands known files), this only contains those, that contain the IoCs known from the Shadow Brokers leak.

Many of these files might still false positive, but still, only a few files found for a previously unknown APT campaign can be useful to start up detailed investigations and find additional traces.

The full list of hashes with some basic tags is attached in a text file for easier use. The tags are from matches to Yara rules available at https://github.com/Neo23x0/signature-base .

Interesting drivers from DriverList.db

The file driverlist.db contains a list of windows kernel driver files, for some, with very interesting remarks.

When to seek help

In some cases, operators are asked to seek help:

```
"bsdnfs",         "*** SEEK HELP IMMEDIATELY ***"
"compression",    "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"control",        "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"devpnp",         "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"devtdi",         "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"enctea",         "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"kbfilter",       "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"mnmdf",          "*** FRIENDLY TOOL - SEEK HELP ASAP ***"
"mrs",            "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"msfcvr32",       "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"mshk",           "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"msixctr",        "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"mxcpx32",        "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"printer",        "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"remote",         "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"scrnfltr",       "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"strfile",        "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"timer",          "*** DANGEROUS MALWARE - SEEK HELP ASAP ***"
"wmiapvrr",       "*** FRIENDLY TOOL - SEEK HELP ASAP ***"
```

When to pull back

In other cases, operators are asked to pull back:

```
"000008C6","*** UNKNOWN - PLEASE PULL BACK ***"
"000009ED","*** UNKNOWN - PLEASE PULL BACK ***"
"00000C06","*** POSSIBLE MALWARE - FOLLOW GUIDANCE ***"
"00000D61","*** UNKNOWN - PLEASE PULL BACK ***"
"0o8PMBlx","*** UNKNOWN - PLEASE PULL BACK ***"
"BNSMAF","*** UNKNOWN - PLEASE PULL BACK ***"
"CDRomFlt","*** UNKNOWN - PLEASE PULL BACK ***"
"CSDfeb731f","*** UNKNOWN - PLEASE PULL BACK ***"
"CSProcessHideDrv","*** UNKNOWN - PLEASE PULL BACK ***"
"CamFSSys","*** UNKNOWN - PLEASE PULL BACK ***"
"DiNs56K","*** UNKNOWN - PLEASE PULL BACK ***"
"ECCDetect","*** UNKNOWN - PLEASE PULL BACK ***"
"EdpEDisk","*** UNKNOWN - PLEASE PULL BACK ***"
"FTEVTNTF","*** UNKNOWN - PLEASE PULL BACK ***"
"GS","*** UNKNOWN - PLEASE PULL BACK ***"
"Gpdrv","*** UNKNOWN - PLEASE PULL BACK ***"
"GxV16","*** UNKNOWN - PLEASE PULL BACK ***"
"HMFAxCore0e2e09a6bf639d5ad8fcee29e32f3253","*** UNKNOWN - PLEASE PULL BACK ***"
"HPUSBMC","*** UNKNOWN - PLEASE PULL BACK ***"
"JiaoIO","*** UNKNOWN - PLEASE PULL BACK ***"
"KNLMON","*** UNKNOWN - PLEASE PULL BACK ***"
"KP_PLX","*** UNKNOWN - PLEASE PULL BACK ***"
```

```
"KcNtKrnl","*** UNKNOWN - PLEASE PULL BACK ***"
"Keyboard","*** UNKNOWN - PLEASE PULL BACK ***"
"KjavMon","*** UNKNOWN - PLEASE PULL BACK ***"
"MCAdriver_net","*** UNKNOWN - PLEASE PULL BACK ***"
"MEMIO","*** UNKNOWN - PLEASE PULL BACK ***"
"NICFSFD","*** UNKNOWN - PLEASE PULL BACK ***"
"NTOSBOOT","*** UNKNOWN - PLEASE PULL BACK ***"
"NetProt","*** UNKNOWN - PLEASE PULL BACK ***"
"NetUmf","*** UNKNOWN - PLEASE PULL BACK ***"
"Nsafepw","*** UNKNOWN - PLEASE PULL BACK ***"
"OHQxUb65","*** UNKNOWN - PLEASE PULL BACK ***"
"PCDNRelay","*** UNKNOWN - PLEASE PULL BACK ***"
"ParMon","*** UNKNOWN - PLEASE PULL BACK ***"
"Qi2KX32","*** UNKNOWN - PLEASE PULL BACK ***"
"R4tnicxp","*** UNKNOWN - PLEASE PULL BACK ***"
"S713PORT","*** UNKNOWN - PLEASE PULL BACK ***"
"SBSWAP2K","*** UNKNOWN - PLEASE PULL BACK ***"
"SINGKRNL","*** UNKNOWN - PLEASE PULL BACK ***"
"SRDFCE","*** UNKNOWN - PLEASE PULL BACK ***"
"SafeFW","*** UNKNOWN - PLEASE PULL BACK ***"
"Sp5nt","*** UNKNOWN - PLEASE PULL BACK ***"
"SysCheck","*** UNKNOWN - PLEASE PULL BACK ***"
"SysLog","*** UNKNOWN - PLEASE PULL BACK ***"
"TSV4WEX","*** UNKNOWN - PLEASE PULL BACK ***"
"TacV4Pci","*** UNKNOWN - PLEASE PULL BACK ***"
"UsbFlt","*** UNKNOWN - PLEASE PULL BACK ***"
"Vsr46","*** UNKNOWN - PLEASE PULL BACK ***"
"WebFilem","*** UNKNOWN - PLEASE PULL BACK ***"
"Wre22","*** UNKNOWN - PLEASE PULL BACK ***"
"acpiex","*** UNKNOWN - PLEASE PULL BACK ***"
"adefth","*** UNKNOWN - PLEASE PULL BACK ***"
"adnechk","*** UNKNOWN - PLEASE PULL BACK ***"
"afemsg","*** UNKNOWN - PLEASE PULL BACK ***"
"amdk92","*** UNKNOWN - PLEASE PULL BACK ***"
"apirmon","*** UNKNOWN - PLEASE PULL BACK ***"
"atikmpag","*** UNKNOWN - PLEASE PULL BACK ***"
"atipmdag","*** UNKNOWN - PLEASE PULL BACK ***"
"atldr349","*** UNKNOWN - PLEASE PULL BACK ***"
"atpommon","*** UNKNOWN - PLEASE PULL BACK ***"
"avcnet","*** UNKNOWN - PLEASE PULL BACK ***"
"azsflk12","*** UNKNOWN - PLEASE PULL BACK ***"
"bdisk","*** UNKNOWN - PLEASE PULL BACK ***"
"bidpoda","*** UNKNOWN - PLEASE PULL BACK ***"
"bihokpkg","*** UNKNOWN - PLEASE PULL BACK ***"
"brcd_fc","*** UNKNOWN - PLEASE PULL BACK ***"
"c3mse4","*** UNKNOWN - PLEASE PULL BACK ***"
"c44a0814","*** UNKNOWN - PLEASE PULL BACK ***"
"citsocmd","*** UNKNOWN - PLEASE PULL BACK ***"
"csctl50","*** UNKNOWN - PLEASE PULL BACK ***"
"cwid","*** UNKNOWN - PLEASE PULL BACK ***"
"cxbnzbzc","*** UNKNOWN - PLEASE PULL BACK ***"
"dedtasvr","*** UNKNOWN - PLEASE PULL BACK ***"
"demeapi","*** UNKNOWN - PLEASE PULL BACK ***"
"dermflt","*** UNKNOWN - PLEASE PULL BACK ***"
"dfx22","*** UNKNOWN - PLEASE PULL BACK ***"
"dmd","*** UNKNOWN - PLEASE PULL BACK ***"
"dofelsrv","*** UNKNOWN - PLEASE PULL BACK ***"
"dopedt","*** UNKNOWN - PLEASE PULL BACK ***"
```

```
"dotrres","*** UNKNOWN - PLEASE PULL BACK ***"
"drvbufsys","*** UNKNOWN - PLEASE PULL BACK ***"
"dyepatbb","*** UNKNOWN - PLEASE PULL BACK ***"
"efpescpt","*** UNKNOWN - PLEASE PULL BACK ***"
"elaseqry","*** UNKNOWN - PLEASE PULL BACK ***"
"elperpt","*** UNKNOWN - PLEASE PULL BACK ***"
"ennluk","*** UNKNOWN - PLEASE PULL BACK ***"
"esnpkg","*** UNKNOWN - PLEASE PULL BACK ***"
"eusbstub","*** UNKNOWN - PLEASE PULL BACK ***"
"exphraid","*** UNKNOWN - PLEASE PULL BACK ***"
"filemrx","*** UNKNOWN - PLEASE PULL BACK ***"
"fnoiok","*** UNKNOWN - PLEASE PULL BACK ***"
"fschk","*** UNKNOWN - PLEASE PULL BACK ***"
"gdtemu","*** UNKNOWN - PLEASE PULL BACK ***"
"gellpn","*** UNKNOWN - PLEASE PULL BACK ***"
"gkalgsrv","*** UNKNOWN - PLEASE PULL BACK ***"
"gopcsvr","*** UNKNOWN - PLEASE PULL BACK ***"
"gqicwwvh","*** UNKNOWN - PLEASE PULL BACK ***"
"gtrrki","*** UNKNOWN - PLEASE PULL BACK ***"
"hbffxp","*** UNKNOWN - PLEASE PULL BACK ***"
"hihtqnlt","*** UNKNOWN - PLEASE PULL BACK ***"
"hildigc","*** UNKNOWN - PLEASE PULL BACK ***"
"himokl","*** UNKNOWN - PLEASE PULL BACK ***"
"hpzsrv","*** UNKNOWN - PLEASE PULL BACK ***"
"hrz","*** UNKNOWN - PLEASE PULL BACK ***"
"i3omp","*** UNKNOWN - PLEASE PULL BACK ***"
"iavusbp","*** UNKNOWN - PLEASE PULL BACK ***"
"idadprx","*** UNKNOWN - PLEASE PULL BACK ***"
"imacch","*** UNKNOWN - PLEASE PULL BACK ***"
"inliln","*** UNKNOWN - PLEASE PULL BACK ***"
"intelrad","*** UNKNOWN - PLEASE PULL BACK ***"
"io","*** UNKNOWN - PLEASE PULL BACK ***"
"ipardprx","*** UNKNOWN - PLEASE PULL BACK ***"
"ipsecex","*** UNKNOWN - PLEASE PULL BACK ***"
"ipuwip","*** UNKNOWN - PLEASE PULL BACK ***"
"ipv6to4","*** POSSIBLE MALWARE - FOLLOW GUIDANCE ***"
"isataedt","*** UNKNOWN - PLEASE PULL BACK ***"
"iscesub","*** UNKNOWN - PLEASE PULL BACK ***"
"itendhlp","*** UNKNOWN - PLEASE PULL BACK ***"
"iwjfutde","*** UNKNOWN - PLEASE PULL BACK ***"
"iziuog","*** UNKNOWN - PLEASE PULL BACK ***"
"jhlsmmed","*** UNKNOWN - PLEASE PULL BACK ***"
"jmiide2","*** UNKNOWN - PLEASE PULL BACK ***"
"jminet3","*** UNKNOWN - PLEASE PULL BACK ***"
"kbdlt","*** UNKNOWN - PLEASE PULL BACK ***"
"kbipoupg","*** UNKNOWN - PLEASE PULL BACK ***"
"kcolcctl","*** UNKNOWN - PLEASE PULL BACK ***"
"kilqkm","*** UNKNOWN - PLEASE PULL BACK ***"
"kiymlrih","*** UNKNOWN - PLEASE PULL BACK ***"
"kkbcdrgi","*** UNKNOWN - PLEASE PULL BACK ***"
"klidmod","*** UNKNOWN - PLEASE PULL BACK ***"
"kpscc","*** UNKNOWN - PLEASE PULL BACK ***"
"kwpirpow","*** UNKNOWN - PLEASE PULL BACK ***"
"lamaapi","*** UNKNOWN - PLEASE PULL BACK ***"
"lamrkit","*** UNKNOWN - PLEASE PULL BACK ***"
"lawfenv","*** UNKNOWN - PLEASE PULL BACK ***"
"lidnui1","*** UNKNOWN - PLEASE PULL BACK ***"
"ljpcjd","*** UNKNOWN - PLEASE PULL BACK ***"
```

```
"ljqjqm","*** UNKNOWN - PLEASE PULL BACK ***"
"lontqos","*** UNKNOWN - PLEASE PULL BACK ***"
"ludsuvqd","*** UNKNOWN - PLEASE PULL BACK ***"
"malrsc","*** UNKNOWN - PLEASE PULL BACK ***"
"mc21FA","*** UNKNOWN - PLEASE PULL BACK ***"
"mc22","*** UNKNOWN - PLEASE PULL BACK ***"
"mc2E","*** UNKNOWN - PLEASE PULL BACK ***"
"mfesmfk01","*** UNKNOWN - PLEASE PULL BACK ***"
"miavedcg","*** UNKNOWN - PLEASE PULL BACK ***"
"micprp","*** UNKNOWN - PLEASE PULL BACK ***"
"mnasavsn","*** UNKNOWN - PLEASE PULL BACK ***"
"moxa","*** UNKNOWN - PLEASE PULL BACK ***"
"msdbm","*** UNKNOWN - PLEASE PULL BACK ***"
"msrsfler","*** UNKNOWN - PLEASE PULL BACK ***"
"nd3wy","*** UNKNOWN - PLEASE PULL BACK ***"
"ndis32","*** UNKNOWN - PLEASE PULL BACK ***"
"ndismplc","*** UNKNOWN - PLEASE PULL BACK ***"
"netne5","*** UNKNOWN - PLEASE PULL BACK ***"
"new","*** UNKNOWN - PLEASE PULL BACK ***"
"nfttgm","*** UNKNOWN - PLEASE PULL BACK ***"
"ngatastp","*** UNKNOWN - PLEASE PULL BACK ***"
"nicnah","*** UNKNOWN - PLEASE PULL BACK ***"
"nictext","*** UNKNOWN - PLEASE PULL BACK ***"
"nosr_2k","*** UNKNOWN - PLEASE PULL BACK ***"
"ntapicti","*** UNKNOWN - PLEASE PULL BACK ***"
"ntdfr","*** UNKNOWN - PLEASE PULL BACK ***"
"ntio410","*** UNKNOWN - PLEASE PULL BACK ***"
"nwrdrnt","*** UNKNOWN - PLEASE PULL BACK ***"
"o8e5FZqn","*** POSSIBLE MALWARE - FOLLOW GUIDANCE ***"
"obpocch","*** UNKNOWN - PLEASE PULL BACK ***"
"oenfqgqam","*** UNKNOWN - PLEASE PULL BACK ***"
"ohnmjs","*** UNKNOWN - PLEASE PULL BACK ***"
"ojqptn","*** UNKNOWN - PLEASE PULL BACK ***"
"omihar","*** UNKNOWN - PLEASE PULL BACK ***"
"omkeatl","*** UNKNOWN - PLEASE PULL BACK ***"
"ompmenv","*** UNKNOWN - PLEASE PULL BACK ***"
"omratcch","*** UNKNOWN - PLEASE PULL BACK ***"
"osdl_2k","*** UNKNOWN - PLEASE PULL BACK ***"
"owdrim","*** UNKNOWN - PLEASE PULL BACK ***"
"pamesp","*** UNKNOWN - PLEASE PULL BACK ***"
"panpen","*** UNKNOWN - PLEASE PULL BACK ***"
"pdjaj","*** UNKNOWN - PLEASE PULL BACK ***"
"pdvvijmw","*** UNKNOWN - PLEASE PULL BACK ***"
"pinesup","*** UNKNOWN - PLEASE PULL BACK ***"
"pinoapi","*** UNKNOWN - PLEASE PULL BACK ***"
"pisplst","*** UNKNOWN - PLEASE PULL BACK ***"
"pjbiuyqr","*** UNKNOWN - PLEASE PULL BACK ***"
"pjhhpn","*** UNKNOWN - PLEASE PULL BACK ***"
"pnigmlst","*** UNKNOWN - PLEASE PULL BACK ***"
"pnpsec","*** UNKNOWN - PLEASE PULL BACK ***"
"ptakan","*** UNKNOWN - PLEASE PULL BACK ***"
"pwloquow","*** UNKNOWN - PLEASE PULL BACK ***"
"qhInjectDrv32","*** UNKNOWN - PLEASE PULL BACK ***"
"rnagsg","*** UNKNOWN - PLEASE PULL BACK ***"
"rndismpc","*** UNKNOWN - PLEASE PULL BACK ***"
"rtnicvw","*** UNKNOWN - PLEASE PULL BACK ***"
"rtniczw","*** UNKNOWN - PLEASE PULL BACK ***"
"rx327rnj","*** UNKNOWN - PLEASE PULL BACK ***"
```

```
"rxbridge","*** UNKNOWN - PLEASE PULL BACK ***"
"sarssrv","*** UNKNOWN - PLEASE PULL BACK ***"
"sata","*** UNKNOWN - PLEASE PULL BACK ***"
"satrsap","*** UNKNOWN - PLEASE PULL BACK ***"
"sdarlib","*** UNKNOWN - PLEASE PULL BACK ***"
"sgravnic","*** UNKNOWN - PLEASE PULL BACK ***"
"sgravpn","*** UNKNOWN - PLEASE PULL BACK ***"
"shiplsvr","*** UNKNOWN - PLEASE PULL BACK ***"
"sitdad","*** UNKNOWN - PLEASE PULL BACK ***"
"sitihlp","*** UNKNOWN - PLEASE PULL BACK ***"
"spldrx","*** UNKNOWN - PLEASE PULL BACK ***"
"spomui1","*** UNKNOWN - PLEASE PULL BACK ***"
"spsysx","*** UNKNOWN - PLEASE PULL BACK ***"
"swinsvc","*** UNKNOWN - PLEASE PULL BACK ***"
"symc648","*** UNKNOWN - PLEASE PULL BACK ***"
"tapesmsg","*** UNKNOWN - PLEASE PULL BACK ***"
"tdomnir","*** UNKNOWN - PLEASE PULL BACK ***"
"tifiole","*** UNKNOWN - PLEASE PULL BACK ***"
"tlingr","*** UNKNOWN - PLEASE PULL BACK ***"
"tmdrv","*** UNKNOWN - PLEASE PULL BACK ***"
"trarsc","*** UNKNOWN - PLEASE PULL BACK ***"
"tws_cpro","*** UNKNOWN - PLEASE PULL BACK ***"
"twscpm","*** UNKNOWN - PLEASE PULL BACK ***"
"ulkgghg","*** UNKNOWN - PLEASE PULL BACK ***"
"usbhubxp","*** UNKNOWN - PLEASE PULL BACK ***"
"usbubci","*** UNKNOWN - PLEASE PULL BACK ***"
"uxlhe","*** UNKNOWN - PLEASE PULL BACK ***"
"vdminfs","*** UNKNOWN - PLEASE PULL BACK ***"
"vfd[],"*** UNKNOWN - PLEASE PULL BACK ***"
"vga2k","*** UNKNOWN - PLEASE PULL BACK ***"
"viaio","*** UNKNOWN - PLEASE PULL BACK ***"
"viaipem","*** UNKNOWN - PLEASE PULL BACK ***"
"vianet","*** UNKNOWN - PLEASE PULL BACK ***"
"viauios","*** UNKNOWN - PLEASE PULL BACK ***"
"vpnpcap","*** UNKNOWN - PLEASE PULL BACK ***"
"vqzxbkfy","*** UNKNOWN - PLEASE PULL BACK ***"
"vs2KFile","*** UNKNOWN - PLEASE PULL BACK ***"
"vslib3k","*** UNKNOWN - PLEASE PULL BACK ***"
"wausbf","*** UNKNOWN - PLEASE PULL BACK ***"
"wgppnt","*** UNKNOWN - PLEASE PULL BACK ***"
"wido_2k","*** UNKNOWN - PLEASE PULL BACK ***"
"winmount","*** UNKNOWN - PLEASE PULL BACK ***"
"wlisplst","*** UNKNOWN - PLEASE PULL BACK ***"
"wpdifs","*** UNKNOWN - PLEASE PULL BACK ***"
"wpdusbex","*** UNKNOWN - PLEASE PULL BACK ***"
"xa14","*** UNKNOWN - PLEASE PULL BACK ***"
"xhordmi","*** UNKNOWN - PLEASE PULL BACK ***"
"xiaojiji","*** UNKNOWN - PLEASE PULL BACK ***"
"xinstall","*** UNKNOWN - PLEASE PULL BACK ***"
```

Internal tools

The following list of files might relate to NSA's own operations and tools:

```
"*** BEHAVEPEKING ***","mdnwdiag"
"*** CARBONFIBER ***","mf32"
"*** CARBONFIBER ***","mq32"
```

```
"*** CARBONFIBER ***","pnpscsi"
"*** DARKSKYLINE ***","tdip"
"*** DARKSKYLINE MENTAL ***","ac98intc"
"*** DARKSKYLINE MENTAL ***","adpux86"
"*** DARKSKYLINE MENTAL ***","amdk5"
"*** DARKSKYLINE MENTAL ***","dpti30"
"*** DARKSKYLINE MENTAL ***","exFat"
"*** DARKSKYLINE MENTAL ***","ip4fw"
"*** DARKSKYLINE MENTAL ***","iqvwx86"
"*** DARKSKYLINE MENTAL ***","irda32"
"*** DARKSKYLINE MENTAL ***","msahci"
"*** DARKSKYLINE MENTAL ***","nwlfi"
"*** DARKSKYLINE MENTAL ***","rasl2tcp"
c"*** DARKSKYLINE MENTAL ***","storvsc"
"*** DARKSKYLINE MENTAL ***","symc81x"
"*** DARKSKYLINE MENTAL ***","vmm32"
"*** DARKSKYLINE MENTAL ***","wanarpx86"
"*** DARKSKYLINE MENTAL ***","ws2ufsl"
"*** DEMENTIAWHEEL ***","agentcpd"
"*** DEMENTIAWHEEL TASKING ***","shlgina"
"*** DOLDRUMWRAPUP ***","rdpvrf"
"*** DOORMANGAUZE ***","ethip6"
"*** DOORMANGAUZE ***","perfnw"
"*** DOORWAYNAPKIN/STOWAGEWINK ***","dlcndi"
"*** DRAFTYPLAN ***","pdresy"
"*** DRILLERSKYLINE ***","serstat"
"*** DS MENTAL *** -OR- Microsoft DFS Namespace Client File","dfsc"
"*** DS MENTAL *** -OR- Microsoft Link-Layer I/O Driver","lltdio"
"*** DS MENTAL *** -OR- Microsoft RDP Redirector Bus Driver","rdpbus"
"*** DS MENTAL *** -OR- Microsoft TCP/IP Reg Compat Driver","tcpipreg"
"*** DS MENTAL *** -OR- Windows TDI Translation Driver","tdx"
"*** ELLIOTSPRINGE/FLEWAVENUE ***","mskbd"
"*** FINALDUET/UNITEDRAKE ***","rls1201"
"*** FLEWAVENUE (TEMP) ***","ntevt32"
"*** FLEWAVENUE ***","ntevt"
"*** FOGGYBOTTOM ***","xpinet30"
"*** FOGGYBOTTOM/UNITEDRAKE ***","mscoreep"
"*** FOGGYBOTTOM/UNITEDRAKE ***","rasapp"
"*** FORMALRITE/UNITEDRAKE ***","mscnsp"
"*** FRIENDLY TOOL - SEEK HELP ASAP ***","mnmdf"
"*** FRIENDLY TOOL - SEEK HELP ASAP ***","wmiapvrr"
"*** FULLMOON ***","ndis5mgr"
"*** GROK/UNITEDRAKE ***","msrtvd"
"*** GROK/UNITEDRAKE ***","wpl913h"
"*** HASSLEWITTPORT/UNITEDRAKE ***","msmps32"
"*** JEALOUSFRUIT ***","tapindis"
"*** KILLSUIT ***","mpdkg32"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","atpmmon"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","bifsgcom"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","cewdaenv"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","dasmkit"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","dehihdp"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","dlapaw"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","doccfg"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","gdisdsk"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","irtidvc"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","lhepfi"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","mipllst"
```

```
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","oplemflt"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","otpemod"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","risfclt"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","ropdir"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","segfib"
"*** KILLSUIT LAUNCHER DRIVER - REMOVE ME ***","tnesahs"
"*** KILLSUIT LOADER DRIVE - REMOVE ME ***","olok_2k"
"*** KILLSUIT LOADER DRIVER - REMOVE ME ***","adpkprp"
"*** LOCUSTTHREAT/UNITEDRAKE ***","inetcom32"
"*** MANTLESTUMP/UNITEDRAKE ***","jsdw776"
"*** MEM DUMP FOR DARKSKYLINE MENTAL ***","dump_msahci"
"*** MISTYVEAL ***","nethdlr"
"*** NETSPYDER ***","khlp807w"
"*** NOTHING TO SEE HERE - CARRY ON ***","fast16"
"*** OLYMPUS ***","Fdisk"
"*** PEDDLECHEAP ***","appinit"
"*** PEDDLECHEAP ***","msvcp56"
"*** PEDDLECHEAP ***","msvcp57"
"*** PEDDLECHEAP ***","msvcp58"
"*** PEDDLECHEAP ***","psxssdll"
"*** PEDDLECHEAP 2.0 ***","wship"
"*** SALVAGERABBIT ***","msrstd"
"*** SALVAGERABBIT ***","volrec"
"*** SALVAGERABBIT/OLYMPUS ***","cmib129u"
"*** SALVAGERABBIT/OLYMPUS ***","ds325gts"
"*** SALVAGERABBIT/OLYMPUS ***","scsi2mgr"
"*** SALVAGERABBIT/UNITEDRAKE ***","kbdclmgr"
"*** SALVAGERABBIT/UNITEDRAKE ***","mstkpr"
"*** SCOUTRUMMAGE/UNITEDRAKE ***","khlp894u"
"*** SCOUTRUMMAGE/UNITEDRAKE ***","netmst"
"*** SCOUTRUMMAGE/UNITEDRAKE ***","nls_295w"
"*** SCOUTRUMMAGE/UNITEDRAKE ***","nls_470u"
"*** SCOUTRUMMAGE/UNITEDRAKE ***","plugproc"
"*** SENTRYTRIBE ***","mstcp32"
"*** SENTRYTRIBE MENTAL ***","1394ohci"
"*** SENTRYTRIBE MENTAL ***","DXGHLP16"
"*** SENTRYTRIBE MENTAL ***","DXGHLP32"
"*** SENTRYTRIBE MENTAL ***","FAT32"
"*** SENTRYTRIBE MENTAL ***","ataport32"
"*** SENTRYTRIBE MENTAL ***","bootvid32"
"*** SENTRYTRIBE MENTAL ***","clfs32"
"*** SENTRYTRIBE MENTAL ***","devmgr32"
"*** SENTRYTRIBE MENTAL ***","dxg32"
"*** SENTRYTRIBE MENTAL ***","dxghlp16"
"*** SENTRYTRIBE MENTAL ***","ext2fs32"
"*** SENTRYTRIBE MENTAL ***","fastfat32"
"*** SENTRYTRIBE MENTAL ***","viac7"
"*** SENTRYTRIBE MENTAL ***","wceusbsh32"
"*** SENTRYTRIBE MENTAL ***","wdmaud32"
"*** SENTRYTRIBE MENTAL ***","wimmount"
"*** SHADOWFLEX/OLYMPUS ***","nls_895u"
"*** SMOGSTRUCK/OLYMPUS ***","nls_879u"
"*** SPINOFFCACTUS/OLYMPUS ***","khlp811u"
"*** SPINOFFCACUS/UNITEDRAKE ***","msrtvid32"
"*** SPITTINGSPYDER/UNITEDRAKE ***","msdtcs32"
"*** ST MENTAL *** -OR- Microsoft SMB 2.0 Redirector","mrxsmb20"
"*** ST MENTAL *** -OR- Microsoft SMB 2.0 Server Driver","srv2"
"*** ST MENTAL *** -OR- Microsoft System Attribute Cache","discache"
```

```
"*** ST MENTAL *** -OR- NETIO Legacy TDI Support Driver","NETIO"
"*** ST MENTAL *** -OR- NETIO Legacy TDI Support Driver","netio"
"*** ST MENTAL *** -OR- RAS Agile VPN Driver","Agilevpn"
"*** ST MENTAL *** -OR- RAS Agile VPN Driver","agilevpn"
"*** ST MENTAL *** -OR- Windows NSI Proxy Driver","nsiproxy"
"*** ST MENTAL *** -OR- Windows QoS Scheduler Driver","pacer"
"*** STORMTHUNDER ***","fld21"
"*** STOWAGEWINK/UNITEDRAKE ***","khlp755w"
"*** STOWAGEWINK/UNITEDRAKE ***","msrmdr32"
"*** STOWAGEWINK/UNITEDRAKE ***","wmpvmux9"
"*** STYLISHCHAMP/OLYMPUS ***","cmib113u"
"*** SUPERFLEX/OLYMPUS ***","nls_875u"
"*** UNITEDRAKE ***","atmdkdrv"
"*** UNITEDRAKE ***","hrlib"
"*** UNITEDRAKE 3.4 ***","MSNDSRV"
"*** UNITEDRAKE 3.4 ***","msndsrv"
"*** UTILITYBURST ***","prsecmon"
"*** UTILITYBURST ***","psecmon"
"*** VALIDATOR ***","msscd16"
"*** VALIDATOR ***","vregstr"
"*** YAK ***","kbpnp"
"*** YAK 2 ***","FSPRTX"
```