**LAB REPORTS**

1. **Docker Forensics Labs**

Steps followed before analysis:

* Docker pull vulnerables/web-dvwa (DVWA)
* Run & perform XSS Injection.

**Docker Analysis**

1. **Web Logs**

[+] Starting mysql...

Starting MariaDB database server: mysqld ..

[+] Starting apache

Starting Apache httpd web server: apache2AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message

.

==> /var/log/apache2/access.log <==

==> /var/log/apache2/error.log <==

[Tue Aug 18 04:58:44.151145 2020] [mpm\_prefork:notice] [pid 303] AH00163: Apache/2.4.25 (Debian) configured -- resuming normal operations

[Tue Aug 18 04:58:44.151232 2020] [core:notice] [pid 303] AH00094: Command line: '/usr/sbin/apache2'

==> /var/log/apache2/other\_vhosts\_access.log <==

==> /var/log/apache2/access.log <==

172.17.0.1 - - [18/Aug/2020:04:59:09 +0000] "GET / HTTP/1.1" 302 337 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:09 +0000] "GET /login.php HTTP/1.1" 200 1048 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:26 +0000] "POST /login.php HTTP/1.1" 302 337 "http://localhost/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:26 +0000] "GET /setup.php HTTP/1.1" 200 2044 "http://localhost/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

==> /var/log/apache2/error.log <==

[Tue Aug 18 04:59:30.610985 2020] [:error] [pid 308] [client 172.17.0.1:54912] PHP Notice: Constant DVWA\_WEB\_PAGE\_TO\_ROOT already defined in /var/www/html/dvwa/includes/DBMS/MySQL.php on line 9, referer: http://localhost/setup.php

==> /var/log/apache2/access.log <==

172.17.0.1 - - [18/Aug/2020:04:59:30 +0000] "POST /setup.php HTTP/1.1" 302 337 "http://localhost/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:31 +0000] "GET /setup.php HTTP/1.1" 200 2179 "http://localhost/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:36 +0000] "GET /login.php HTTP/1.1" 200 1051 "http://localhost/setup.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:43 +0000] "POST /login.php HTTP/1.1" 302 337 "http://localhost/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:43 +0000] "GET /index.php HTTP/1.1" 200 3036 "http://localhost/login.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:04:59:47 +0000] "GET /vulnerabilities/xss\_s/ HTTP/1.1" 200 1975 "http://localhost/index.php" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:05:00:13 +0000] "POST /vulnerabilities/xss\_s/ HTTP/1.1" 200 2000 "http://localhost/vulnerabilities/xss\_s/" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

172.17.0.1 - - [18/Aug/2020:05:00:23 +0000] "GET /vulnerabilities/xss\_r/ HTTP/1.1" 200 1753 "http://localhost/vulnerabilities/xss\_s/" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"

**172.17.0.1 - - [18/Aug/2020:05:00:47 +0000] "GET /vulnerabilities/xss\_r/?name=name%3Cimg+src%3D1+onerror%3D%22alert%28document.cookie%29%22%3E HTTP/1.1" 200 1788 "http://localhost/vulnerabilities/xss\_r/" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"**

**172.17.0.1 - - [18/Aug/2020:05:00:47 +0000] "GET /vulnerabilities/xss\_r/1 HTTP/1.1" 404 512 "http://localhost/vulnerabilities/xss\_r/?name=name%3Cimg+src%3D1+onerror%3D%22alert%28document.cookie%29%22%3E" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"**

**172.17.0.1 - - [18/Aug/2020:05:01:12 +0000] "GET /vulnerabilities/xss\_r/?name=%3Cscript%3Ealert%28%22xss\_attack%22%29%3C%2Fscript%3E HTTP/1.1" 200 1780 "http://localhost/vulnerabilities/xss\_r/?name=name%3Cimg+src%3D1+onerror%3D%22alert%28document.cookie%29%22%3E" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"**

**172.17.0.1 - - [18/Aug/2020:05:01:23 +0000] "GET /logout.php HTTP/1.1" 302 337 "http://localhost/vulnerabilities/xss\_r/?name=%3Cscript%3Ealert%28%22xss\_attack%22%29%3C%2Fscript%3E" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"**

**172.17.0.1 - - [18/Aug/2020:05:01:23 +0000] "GET /login.php HTTP/1.1" 200 1074 "http://localhost/vulnerabilities/xss\_r/?name=%3Cscript%3Ealert%28%22xss\_attack%22%29%3C%2Fscript%3E" "Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:79.0) Gecko/20100101 Firefox/79.0"**

# Bold logs show that there was an XSS attack.

1. **Image Listing**

{

"Repositories": {

"vulnerables/web-dvwa": {

"vulnerables/web-dvwa:dvwa": "sha256:ab0d83586b6e8799bb549ab91914402e47e3bcc7eea0c5cdf43755d56150cc6a",

"vulnerables/web-dvwa:latest": "sha256:ab0d83586b6e8799bb549ab91914402e47e3bcc7eea0c5cdf43755d56150cc6a",

"vulnerables/web-dvwa@sha256:dae203fe11646a86937bf04db0079adef295f426da68a92b40e3b181f337daa7": "sha256:ab0d83586b6e8799bb549ab91914402e47e3bcc7eea0c5cdf43755d56150cc6a"

}

}

}

1. **Image Metadata**

{"architecture":"amd64","config":{"Hostname":"","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"ExposedPorts":{"80/tcp":{}},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"],"Cmd":null,"ArgsEscaped":true,"Image":"sha256:273b6cd2c559fd7f4a6e9989c73a6ced44bd3d4787146cb0b02b77d299de0d91","Volumes":null,"WorkingDir":"","Entrypoint":["/main.sh"],"OnBuild":null,"Labels":{"maintainer":"opsxcq@strm.sh"}},"container":"f5d00def67f63b78455d80e80d07048d6c4177e9f1e6766e706752890bf9c037","container\_config":{"Hostname":"f5d00def67f6","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"ExposedPorts":{"80/tcp":{}},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"],"Cmd":["/bin/sh","-c","#(nop) ","ENTRYPOINT [\"/main.sh\"]"],"ArgsEscaped":true,"Image":"sha256:273b6cd2c559fd7f4a6e9989c73a6ced44bd3d4787146cb0b02b77d299de0d91","Volumes":null,"WorkingDir":"","Entrypoint":["/main.sh"],"OnBuild":null,"Labels":{"maintainer":"opsxcq@strm.sh"}},"created":"2018-10-12T17:49:01.240444043Z","docker\_version":"18.03.1-ee-3","history":[{"created":"2017-11-04T05:26:40.421915785Z","created\_by":"/bin/sh -c #(nop) ADD file:a71e077a42995a68ffe4834d85cfe26af4ea12aa8ed43decc03cc487124b1f70 in / "},{"created":"2017-11-04T05:26:40.778734274Z","created\_by":"/bin/sh -c #(nop) CMD [\"bash\"]","empty\_layer":true},{"created":"2018-10-12T17:44:51.568417068Z","created\_by":"/bin/sh -c #(nop) LABEL maintainer=opsxcq@strm.sh","empty\_layer":true},{"created":"2018-10-12T17:48:40.112819571Z","created\_by":"/bin/sh -c apt-get update \u0026\u0026 apt-get upgrade -y \u0026\u0026 DEBIAN\_FRONTEND=noninteractive apt-get install -y debconf-utils \u0026\u0026 echo mariadb-server mysql-server/root\_password password vulnerables | debconf-set-selections \u0026\u0026 echo mariadb-server mysql-server/root\_password\_again password vulnerables | debconf-set-selections \u0026\u0026 DEBIAN\_FRONTEND=noninteractive apt-get install -y apache2 mariadb-server php php-mysql php-pgsql php-pear php-gd \u0026\u0026 apt-get clean \u0026\u0026 rm -rf /var/lib/apt/lists/\*"},{"created":"2018-10-12T17:48:41.572499443Z","created\_by":"/bin/sh -c #(nop) COPY file:e1162a50525b284972b663daef5ca505c724673da0dda9a707bc8f67e4ec1220 in /etc/php5/apache2/php.ini "},{"created":"2018-10-12T17:48:43.817849479Z","created\_by":"/bin/sh -c #(nop) COPY dir:9c23b23aaae913c12ab3d2659b4d45398ee5652ed113267814c49d9ba501992a in /var/www/html "},{"created":"2018-10-12T17:48:44.34086818Z","created\_by":"/bin/sh -c #(nop) COPY file:55e9d94279708ad763c17a1ca775e225829b275ace5716ca8a0aff69c70161a4 in /var/www/html/config/ "},{"created":"2018-10-12T17:48:49.325818591Z","created\_by":"/bin/sh -c chown www-data:www-data -R /var/www/html \u0026\u0026 rm /var/www/html/index.html"},{"created":"2018-10-12T17:49:00.231082545Z","created\_by":"/bin/sh -c service mysql start \u0026\u0026 sleep 3 \u0026\u0026 mysql -uroot -pvulnerables -e \"CREATE USER app@localhost IDENTIFIED BY 'vulnerables';CREATE DATABASE dvwa;GRANT ALL privileges ON dvwa.\* TO 'app'@localhost;\""},{"created":"2018-10-12T17:49:00.560515018Z","created\_by":"/bin/sh -c #(nop) EXPOSE 80","empty\_layer":true},{"created":"2018-10-12T17:49:00.941597385Z","created\_by":"/bin/sh -c #(nop) COPY file:f24e7713eb6c0568608bea3ff7b52edda86305cfd5bef0ac4e57efdb15792202 in / "},{"created":"2018-10-12T17:49:01.240444043Z","created\_by":"/bin/sh -c #(nop) ENTRYPOINT [\"/main.sh\"]","empty\_layer":true}],"os":"linux","rootfs":{"type":"layers","diff\_ids":["sha256:a75caa09eb1f7d732568c5d54de42819973958589702d415202469a550ffd0ea","sha256:80f9a8427b1826f014f873dc471b6a89916ff79550bcd1c94aadd78c3f5bbdc7","sha256:97a1040801c3e87c036ef26da36a8dcbce61c0c8a6b4b3c8d9dda3409e7dfffe","sha256:acf8abb873cedff7e2aad9da561c592a5aac1938cb2bf0f8c4f6c97406c92a17","sha256:9713610e6ec4cbca7ade219f3efc5df93bd74b21d60c4754d6f400dad226f02f","sha256:73e92d5f2a6cf8a95578e6191222aaa8ade9a5cd792e9b3ed8a2b6a023bb8259","sha256:585e40f29c46d8ef2ecbccb870654b76e0910da9123bff93457011eebbc5cf6c","sha256:deeea3c4d56f1bbb10d3bd44879305d2fbef6678aa6c20947bd99576fe85fd45"]}}

1. **Container Metadata**

{"StreamConfig":{},"State":{"Running":false,"Paused":false,"Restarting":false,"OOMKilled":false,"RemovalInProgress":false,"Dead":false,"Pid":0,"ExitCode":137,"Error":"","StartedAt":"2020-08-18T05:48:42.837552652Z","FinishedAt":"2020-08-18T05:50:27.05989372Z","Health":null},"ID":"69b7f0d24367fe1cfdc674fe47f7c5fbb347f7615f1ed8570b6e22cbf8b69118","Created":"2020-08-18T04:58:32.707677489Z","Managed":false,"Path":"/main.sh","Args":[],"Config":{"Hostname":"69b7f0d24367","Domainname":"","User":"","AttachStdin":false,"AttachStdout":true,"AttachStderr":true,"ExposedPorts":{"80/tcp":{}},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"],"Cmd":null,"Image":"vulnerables/web-dvwa:dvwa","Volumes":null,"WorkingDir":"","Entrypoint":["/main.sh"],"OnBuild":null,"Labels":{"maintainer":"[opsxcq@strm.sh](mailto:opsxcq@strm.sh)"}},"Image":"sha256:ab0d83586b6e8799bb549ab91914402e47e3bcc7eea0c5cdf43755d56150cc6a","NetworkSettings":{"Bridge":"","SandboxID":"626365f2c6c124305189794d84cac9bc935080757c372c3613f23cce50b451cc","HairpinMode":false,"LinkLocalIPv6Address":"","LinkLocalIPv6PrefixLen":0,"Networks":{"bridge":{"IPAMConfig":null,"Links":null,"Aliases":null,"NetworkID":"7a1941af2be8834b085cf48dee93f866aa0c2952055415f30e58e3ad0a5bd90c","EndpointID":"","Gateway":"","IPAddress":"","IPPrefixLen":0,"IPv6Gateway":"","GlobalIPv6Address":"","GlobalIPv6PrefixLen":0,"MacAddress":"","DriverOpts":null,"IPAMOperational":false}},"Service":null,"Ports":null,"SandboxKey":"/var/run/docker/netns/626365f2c6c1","SecondaryIPAddresses":null,"SecondaryIPv6Addresses":null,"IsAnonymousEndpoint":false,"HasSwarmEndpoint":false},"LogPath":"/var/lib/docker/containers/69b7f0d24367fe1cfdc674fe47f7c5fbb347f7615f1ed8570b6e22cbf8b69118/69b7f0d24367fe1cfdc674fe47f7c5fbb347f7615f1ed8570b6e22cbf8b69118-json.log","Name":"/dvwa","Driver":"overlay2","OS":"linux","MountLabel":"","ProcessLabel":"","RestartCount":0,"HasBeenStartedBefore":true,"HasBeenManuallyStopped":true,"MountPoints":{},"SecretReferences":null,"ConfigReferences":null,"AppArmorProfile":"docker-default","HostnamePath":"/var/lib/docker/containers/69b7f0d24367fe1cfdc674fe47f7c5fbb347f7615f1ed8570b6e22cbf8b69118/hostname","HostsPath":"/var/lib/docker/containers/69b7f0d24367fe1cfdc674fe47f7c5fbb347f7615f1ed8570b6e22cbf8b69118/hosts","ShmPath":"","ResolvConfPath":"/var/lib/docker/containers/69b7f0d24367fe1cfdc674fe47f7c5fbb347f7615f1ed8570b6e22cbf8b69118/resolv.conf","SeccompProfile":"","NoNewPrivileges":false}

1. **Container Process Memory**

UID PID PPID C STIME TTY TIME CMD

root 51176 51158 0 11:18 ? 00:00:00 /bin/bash /main.sh

root 51254 51176 0 11:18 ? 00:00:00 /bin/bash /usr/bin/mysqld\_safe

systemd+ 51400 51254 0 11:18 ? 00:00:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86\_64-linux-gnu/mariadb18/plugin --user=mysql --skip-log-error --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306

root 51401 51254 0 11:18 ? 00:00:00 logger -t mysqld -p daemon error

root 51525 51176 0 11:18 ? 00:00:00 /usr/sbin/apache2 -k start

www-data 51534 51525 0 11:18 ? 00:00:00 /usr/sbin/apache2 -k start

www-data 51535 51525 0 11:18 ? 00:00:00 /usr/sbin/apache2 -k start

www-data 51536 51525 0 11:18 ? 00:00:00 /usr/sbin/apache2 -k start

www-data 51537 51525 0 11:18 ? 00:00:00 /usr/sbin/apache2 -k start

www-data 51538 51525 0 11:18 ? 00:00:00 /usr/sbin/apache2 -k start

root 51544 51176 0 11:18 ? 00:00:00 tail -f /var/log/apache2/access.log /var/log/apache2/error.log /var/log/apache2/other\_vhosts\_access.log

**Docker Analysis using OSquery**

1. **DOCKER\_CONTAINERS**

$ sudo osqueryi "select name, pid, command, privileged, security\_options from docker\_containers;"

+-------+-------+----------+------------+------------------+

| name | pid | command | privileged | security\_options |

+-------+-------+----------+------------+------------------+

| /dvwa | 55767 | /main.sh | 0 | |

+-------+-------+----------+------------+------------------+

1. **DOCKER CONTAINER ENVIRONMENT VARIABLE**

$ sudo osqueryi "select name, env\_variables from docker\_containers;"

+-------+-------------------------------------------------------------------+

| name | env\_variables |

+-------+-------------------------------------------------------------------+

| /dvwa | PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin |

+-------+-------------------------------------------------------------------+

1. **DOCKER CONTAINERS NETWORKS**

$ sudo osqueryi "select c.name as c\_name, n.name, n.gateway, n.ip\_address, n.ip\_prefix\_len, n.mac\_address, p.port, p.host\_ip, p.host\_port from docker\_containers c, docker\_container\_networks n left outer join docker\_container\_ports p on c.id=p.id where c.id=n.id;"

+--------+--------+------------+------------+---------------+-------------------+------+---------+-----------+

| c\_name | name | gateway | ip\_address | ip\_prefix\_len | mac\_address | port | host\_ip | host\_port |

+--------+--------+------------+------------+---------------+-------------------+------+---------+-----------+

| /dvwa | bridge | 172.17.0.1 | 172.17.0.2 | 16 | 02:42:ac:11:00:02 | 80 | 0.0.0.0 | 80 |

+--------+--------+------------+------------+---------------+-------------------+------+---------+-----------+

1. **CONTAINERS THAT ARE RUNNING WITH A ROOT PROCESS**

$ SELECT containers.name, processes.pid, processes.name, cmdline, user FROM docker\_container\_processes processes JOIN docker\_containers containers ON containers.id=processes.id WHERE processes.id IN ( SELECT id FROM docker\_containers ) AND user="root";

+-------------+-------+-------------+---------------------------------------------------------------------------------------------------------+------+

| name | pid | name | cmdline | user |

+-------------+-------+-------------+---------------------------------------------------------------------------------------------------------+------+

| main.sh | 55767 | main.sh | /bin/bash /main.sh | root |

| mysqld\_safe | 55842 | mysqld\_safe | /bin/bash /usr/bin/mysqld\_safe | root |

| logger | 55989 | logger | logger -t mysqld -p daemon error | root |

| apache2 | 56092 | apache2 | /usr/sbin/apache2 -k start | root |

| tail | 56119 | tail | tail -f /var/log/apache2/access.log /var/log/apache2/error.log /var/log/apache2/other\_vhosts\_access.log | root |

**2. Malware Analysis using REMnux**

Steps followed before analysis:

* Installed REMnux on virtual Box.
* Downloaded sample malware files (TrickBot-2019-08).

**Files:**

1. 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698.txt
2. 16429e95922c9521f7a40fa8f4c866444a060122448b243444dd2358a96a344c.txt
3. 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt
4. 666515eec773e200663fbd5fcad7109e9b97be11a83b41b8a4d73b7f5c8815ff.txt
5. 970b135b4c47c12f97bc3d3bbdf325f391b499d03fe19ac9313bcace3a1450d2.txt

**md5sum**

1. d9fda66b46a73a3ddefdce3c7ea5ae1e
2. e36380d824811bc28fbc26ea84c1a868
3. a69fd5f2b4db98824821232231522d16
4. 310731c5fce818f867bb0a32a1bec8be
5. 0134c3c684eb26cd2e677c4c5ea3628b

**sha1sum**

1. 17d9aab1623aedf734d6f77cec409e3055adaa47
2. 19d5fc16cfabae3b3c26bbb4f5798da42733a2fa
3. 7fbacf7961976d32694cf89e238f23cf64cdf37f
4. 3aff9ac6f76ff6306ca484433430ff7c5ec46039
5. d362c282d808285f5a5535a56cbc78d74165cd06

**FileTypes**

1. 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698.txt: **PE32 executable (GUI) Intel 80386, for MS Windows**
2. 16429e95922c9521f7a40fa8f4c866444a060122448b243444dd2358a96a344c.txt: **Microsoft Word 2007+**
3. 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt: **Microsoft Word 2007+**
4. 666515eec773e200663fbd5fcad7109e9b97be11a83b41b8a4d73b7f5c8815ff.txt: **Microsoft Word 2007+**
5. 970b135b4c47c12f97bc3d3bbdf325f391b499d03fe19ac9313bcace3a1450d2.txt: **ASCII text, with CRLF, LF line terminators**

**File 1: 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698.txt**

**Static Analysis:**

Exiftool

ExifTool Version Number : 12.00

File Name : 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698.txt

Directory : .

File Size : 250 kB

File Modification Date/Time : 2020:08:21 00:04:18-04:00

File Access Date/Time : 2020:08:21 00:31:38-04:00

File Inode Change Date/Time : 2020:08:21 00:04:18-04:00

File Permissions : rwxr-xr-x

File Type : Win32 EXE

File Type Extension : exe

MIME Type : application/octet-stream

Machine Type : Intel 386 or later, and compatibles

Time Stamp : 2019:07:12 08:43:14-04:00

Image File Characteristics : No relocs, Executable, 32-bit

PE Type : PE32

Linker Version : 9.0

Code Size : 6656

Initialized Data Size : 240640

Uninitialized Data Size : 0

Entry Point : 0x2463

OS Version : 5.0

Image Version : 0.0

Subsystem Version : 5.0

Subsystem : Windows GUI

File Version Number : 6.1.7600.16385

Product Version Number : 6.1.7600.16385

File Flags Mask : 0x003f

File Flags : (none)

File OS : Windows NT 32-bit

Object File Type : Dynamic link library

File Subtype : 0

Language Code : English (U.S.)

Character Set : Unicode

Company Name : Microsoft Corporation

File Description : Media Foundation AAC Encoder

File Version : 6.1.7600.16385 (win7\_rtm.090713-1255)

Internal Name : Media Foundation AAC Encoder

Legal Copyright : © Microsoft Corporation. All rights reserved.

Original File Name : mfAACEnc.dll

Product Name : Microsoft® Windows® Operating System

Product Version : 6.1.7600.16385

Manalyze

Summary:

--------

Architecture: IMAGE\_FILE\_MACHINE\_I386

Subsystem: IMAGE\_SUBSYSTEM\_WINDOWS\_GUI

Compilation Date: 2019-Jul-12 12:43:14

Detected languages: English - United States

German - Germany

CompanyName: Microsoft Corporation

FileDescription: Media Foundation AAC Encoder

FileVersion: 6.1.7600.16385 (win7\_rtm.090713-1255)

InternalName: Media Foundation AAC Encoder

LegalCopyright: © Microsoft Corporation. All rights reserved.

OriginalFilename: mfAACEnc.dll

ProductName: Microsoft® Windows® Operating System

ProductVersion: 6.1.7600.16385

Peframe

File Information (time: 0:00:02.075976)

--------------------------------------------------------------------------------

filename 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698.txt

filetype PE32 executable (GUI) Intel 80386, for MS Windows

filesize 256312

hash sha256 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698

virustotal /

imagebase 0x400000

entrypoint 0x2463

imphash 8ddfc9cac41317bdeb147cb16bade57b

datetime 2019-07-12 12:43:14

dll False

directories import, tls, resources, relocations, sign

sections .rdata, .data, .text \*, .rsrc \*

features antidbg, packer

--------------------------------------------------------------------------------

Yara Plugins

--------------------------------------------------------------------------------

IsPE32

IsWindowsGUI

HasOverlay

HasDigitalSignature

HasRichSignature

--------------------------------------------------------------------------------

Behavior

--------------------------------------------------------------------------------

anti dbg

Xor

rat webcam

--------------------------------------------------------------------------------

Packer

--------------------------------------------------------------------------------

Visual Cpp 2005 Release Microsoft

VC8 Microsoft Corporation

Microsoft Visual Cpp 8

--------------------------------------------------------------------------------

Anti Debug

--------------------------------------------------------------------------------

IsDebuggerPresent

TerminateProcess

UnhandledExceptionFilter

--------------------------------------------------------------------------------

Sections Suspicious

--------------------------------------------------------------------------------

.text 6.06

.rsrc 6.04

--------------------------------------------------------------------------------

Metadata

--------------------------------------------------------------------------------

CompanyName Microsoft Corporation

FileDescription Media Foundation AAC Encoder

FileVersion 6.1.7600.16385 (win7\_rtm.090713-1255)

InternalName Media Foundation AAC Encoder

LegalCopyright © Microsoft Corporation. All rights reserved.

OriginalFilename mfAACEnc.dll

ProductName Microsoft® Windows® Operating System

ProductVersion 6.1.7600.16385

--------------------------------------------------------------------------------

Import function

--------------------------------------------------------------------------------

AVICAP32.dll 2

KERNEL32.dll 27

USER32.dll 34

GDI32.dll 1

COMDLG32.dll 1

SHELL32.dll 1

MSVCP90.dll 2

MSVCR90.dll 32

--------------------------------------------------------------------------------

Signature

--------------------------------------------------------------------------------

serial\_number 0f7884261206c694e64f3204e97da0a4

common\_name VIEW 4 ME UK LIMITED

country GB

locality LONDON

organization VIEW 4 ME UK LIMITED

email

valid\_from Jul 10 00:00:00 2019 GMT

valid\_to Jul 9 23:59:59 2020 GMT

--------------------------------------------------------------------------------

Possibile Breakpoint

--------------------------------------------------------------------------------

CopyFileW

CreateFileMappingW

ExitProcess

FindResourceA

GetCurrentProcess

GetCurrentProcessId

GetModuleFileNameW

GetProcAddress

GetStartupInfoA

GetTickCount

IsDebuggerPresent

LoadLibraryW

LockResource

MapViewOfFile

MessageBoxA

ShellExecuteW

Sleep

TerminateProcess

UnhandledExceptionFilter

--------------------------------------------------------------------------------

Url

--------------------------------------------------------------------------------

http://t2.symcb.com0

https://www.thawte.com/repository0W

https://www.digicert.com/CPS0

http://crl3.digicert.com/DigiCertAssuredIDCA-1.crl08642http://crl4.digicert.com/DigiCertAssuredIDCA-1.crl0w

http://tl.symcd.com0&

http://ocsp.digicert.com0C

http://tl.symcb.com/tl.crt0

http://cacerts.digicert.com/DigiCertAssuredIDCA-1.crt0

https://www.thawte.com/cps0/

http://tl.symcb.com/tl.crl0

http://ocsp.digicert.com0A

http://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt0

http://www.digicert.com/ssl-cps-repository.htm0

http://crl3.digicert.com/DigiCertAssuredIDRootCA.crl0:864http://crl4.digicert.com/DigiCertAssuredIDRootCA.crl0

http://t1.symcb.com/ThawtePCA.crl0

--------------------------------------------------------------------------------

File

--------------------------------------------------------------------------------

%04d.bmp Image

AVICAP32.dll Library

KERNEL32.dll Library

USER32.dll Library

GDI32.dll Library

COMDLG32.dll Library

SHELL32.dll Library

MSVCP90.dll Library

MSVCR90.dll Library

\*.bmp Image

\*.avi Video

**Deobfuscation:**

Bbcrack

Following 10 files were found as the output of bbcrack analysis.

3 out of 10 were win32 executable and the rest of the 7 files were data files.

PE32 executable (GUI) Intel 80386, for MS Windows

Filetype: win32 EXE

Original File Name: mfAACEnc.dll

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_add80\_xor80.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_identity.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_xor80\_add80.txt

File Format Error

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_add60\_xorA0.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_add70\_xorB0.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_xor20\_add20.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_xor30\_add10.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_addE0\_xor20.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_addF0\_xor30.txt

0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698\_xorA0\_addA0.txt

**Code Emulation:**

Capa

+------------------------+------------------------------------------------------------------------------------+

| md5 | d9fda66b46a73a3ddefdce3c7ea5ae1e

| path | 0242ebb681eb1b3dbaa751320dea56e31c5e52c8324a7de125a8144cc5270698.txt

+------------------------+------------------------------------------------------------------------------------+

+------------------------+------------------------------------------------------------------------------------+

| ATT&CK Tactic | ATT&CK Technique |

|------------------------+------------------------------------------------------------------------------------|

| DEFENSE EVASION | Obfuscated Files or Information [T1027] |

| EXECUTION | Shared Modules [T1129] |

+------------------------+------------------------------------------------------------------------------------+

+------------------------------------------------------+------------------------------------------------------+

| CAPABILITY | NAMESPACE |

|------------------------------------------------------+------------------------------------------------------|

| encode data using XOR | data-manipulation/encoding/xor |

| contain a resource (.rsrc) section | executable/pe/section/rsrc |

| extract resource via kernel32 functions | executable/resource |

| copy file | host-interaction/file-system/copy |

| create process | host-interaction/process/create |

| terminate process (2 matches) | host-interaction/process/terminate |

| link function at runtime | linking/runtime-linking |

| parse PE header | load-code/pe |

+------------------------------------------------------+------------------------------------------------------+

**Disassemble/Decompile:**

Ghidra

void \_\_cdecl FUN\_00401000(int param\_1,size\_t param\_2)

{

char cVar1;

void \*pvVar2;

int iVar3;

int iVar4;

uint uVar5;

int iVar6;

uint uVar7;

int local\_8;

pvVar2 = malloc(param\_2);

iVar3 = 0;

local\_8 = 0;

if (0 < (int)param\_2) {

do {

uVar7 = 0;

iVar4 = 0;

iVar6 = 0;

do {

cVar1 = \*(char \*)(iVar3 + param\_1 + iVar6);

if (cVar1 != '=') {

uVar7 = uVar7 << 6;

iVar4 = iVar4 + 6;

}

if ((cVar1 < 'A') || ('Z' < cVar1)) {

if (('`' < cVar1) && (cVar1 < '{')) {

uVar5 = (int)cVar1 - 0x47;

goto LAB\_00401071;

}

if (('/' < cVar1) && (cVar1 < ':')) {

uVar5 = (int)cVar1 + 4;

goto LAB\_00401071;

}

if (cVar1 == '+') {

uVar7 = uVar7 | 0x3e;

}

else {

if (cVar1 == '/') {

uVar7 = uVar7 | 0x3f;

}

else {

uVar7 = (int)uVar7 >> 2;

iVar4 = iVar4 + -2;

}

}

}

else {

uVar5 = (int)cVar1 - 0x41;

LAB\_00401071:

uVar7 = uVar7 | uVar5;

}

iVar6 = iVar6 + 1;

} while (iVar6 < 4);

while (iVar4 != 0) {

iVar4 = iVar4 + -8;

\*(undefined \*)(local\_8 + (int)pvVar2) = (char)((int)uVar7 >> ((byte)iVar4 & 0x1f));

local\_8 = local\_8 + 1;

}

iVar3 = iVar3 + 4;

} while (iVar3 < (int)param\_2);

}

\*(undefined \*)(local\_8 + (int)pvVar2) = 0;

return;

}

Libraries Present

avicap32.dll kernel32.dll

user32.dll gdi32.dll

comdlg32.dll shell32.dll

msvcp90.dll msvcr90.dll

Base64dump

ID Size Encoded Decoded md5 decoded

-- ---- ------- ------- -----------

1: 4 This N.. 501e2a2fa18a6fc751a2c926cfd87f8d

2: 4 mode ..^ fb5d311465160621672451ab9138b859

3: 4 text ..m d235bf01945835d5f31a59b90c1a3a9f

4: 4 data u.Z 359f5eaf26fbf0327b38595ddede06e2

5: 4 rsrc ... cbdc1d6e9334099f97fedfbbecef6356

6: 4 jLh6 ..z ce8e628009db72c6997aaab9db33ce1c

7: 4 WWWV Ye. 0c7bede65ccd8ec54cd28b570b916bfe

8: 4 SShG I(F d2fe3e06fa1f66ac2c8a6f7792c76450

9: 4 SShF I(E 6f867cc3f4309b598df59235c9072e54

10: 4 SSh2 I(v 8cb7e1e869ab8fad9d2a50da0f50f8c9

11: 4 SSh3 I(w 63db90343b8e0d5136640a5894e00059

12: 4 jLh6 ..z ce8e628009db72c6997aaab9db33ce1c

13: 4 jLh6 ..z ce8e628009db72c6997aaab9db33ce1c

14: 4 jLh6 ..z ce8e628009db72c6997aaab9db33ce1c

15: 4 HHtp .{i 594d6f2bbc95a71fef136a76b23f56a7

16: 4 jLh6 ..z ce8e628009db72c6997aaab9db33ce1c

17: 4 VVhH UXG 40194232f98a843612616cf0d62c6e06

18: 4 YWSP ad. c12f6138194e659fe5458f71edf90af1

19: 4 VVVj UUc 2b713502da2a38064f66e8cdca5b6d10

20: 4 VVVj UUc 2b713502da2a38064f66e8cdca5b6d10

21: 4 VWVj Uec 8c8a093b56ff1e61cde70ff19c4294ba

22: 4 VVVj UUc 2b713502da2a38064f66e8cdca5b6d10

23: 4 XPVj \.c 9ab322d9d1660414020368cc84abcdfe

24: 4 8csm ..& b4e1a81f33107c76ace78f4c82e3cae4

25: 4 wird .\*. a560269c0656a8d4fd25d9f6fde9aff5

26: 4 back m.$ 0ffc6771dfd7d363d071d4429af1d23b

27: 8 previous ...... f4e13bf436c3636d50a133609907a875

28: 4 File .)^ 3a0e86c02de046ba4ee4a3ff0ddaf325

29: 4 init .x. 229319ba89eadfd2a8b0bf8720392e58

30: 8 Programm >. ... 1363d41178dbddb2f61496afe321a69e

31: 20 CryptAcquireCont .....\*.\*....{.@ fca442fa0c7ae26c5552299daf61e62d

32: 24 capGetDriverDesc q.Fz.........\*m. 9675e96d88ca8140c9c09c626708a544

33: 8 AVICAP32 .R.... 29b9b155e81ea83da0735e80df763d41

34: 8 lstrcatA ..kq.@ 8b4351187bc64e34e364a597264c90e8

35: 8 lstrcpyA ..kr.. a226480ee299f08bfa7189c2b13fbb41

36: 12 LoadLibraryW ....&.j.. f06dc46453cef34f902177df95bf7cb3

37: 12 LockResource ..$E.(... 40991762fa11d18f9b127d9b48ef65ed

38: 12 LoadResource ...E.(... cfc17288968848660906c9a0a852975e

39: 8 KERNEL32 (DM... 4d4b2515f9fbc64660b482fb5f9ac80d

40: 12 SetWindowPos I.V.wh.., ea14d83317fd9e7022f360b51b2bbef7

41: 12 SendMessageA I..1.,j.. 0b7693a1b20132587afe0f016cb94988

42: 8 IsWindow "....0 6e583e811f64eb8c839fe50a52fafca4

43: 8 SetTimer I.S.g. a11e59aa78cdf529838a1529e87e218e

44: 8 EndPaint .wOj). ec794af80fa0566fdd3f514984e21857

45: 16 DispatchMessageA .+)j.!1.,j.. 4d0b867f8468e9f558720503ac281c7a

46: 16 TranslateMessage N...V.x..... 231c0f24bf8d84aeeeba737108118deb

47: 12 UpdateWindow R.Z.....0 96881b0d6196f2ce1ce3ba4db746c743

48: 16 GetSaveFileNameA ..Rj...W.jg. a146a5e91f78b9eb8c1235c01ba83194

49: 8 COMDLG32 ...,m. 1a9b8c5ae66909fa3a8a62d30c0fd55e

50: 4 char r.. d965a0ce455990b724e04245b768b7ba

51: 4 char r.. d965a0ce455990b724e04245b768b7ba

52: 4 atoi j." 18f78bdb30739c0c2fa87dcaeecbba53

53: 4 free ~.. 2f5166a160f684ca93d7e268e22f4f98

54: 4 amsg jk 04f6d61f7ca50bf61b2f46ad168a715c

55: 4 exit {.. 8b59084389a5bb47c84d9e51b2ec214c

56: 4 exit {.. 8b59084389a5bb47c84d9e51b2ec214c

57: 4 exit {.. 8b59084389a5bb47c84d9e51b2ec214c

58: 8 initterm .x.... be72469e41bb5430f327329998241182

59: 8 initterm .x.... be72469e41bb5430f327329998241182

60: 4 fdiv }.. e162b7b7aefcc5e4dc8272ba7e44448b

61: 4 type .\*^ 3a4d52be883686b8f4d8e600de9bba00

62: 8 debugger u..... cb74310d6b79074ded0f89e6fc6ebdf1

63: 4 hook ..$ 8b1a75feab48f21bf4084838ef6d512c

64: 4 lock ..$ 4faeffa515cb621f2bb5332d5e4acb9c

65: 8 handler4 ...... 22e1ad6408d18dd32508ea3ddc010302

66: 16 TerminateProcess M...v.x..q., 7e50e40f0508d1174c12fae78cf45c4d

67: 24 UnhandledExcepti RxZ..^tL\z.b.qb. 357654aabc6d52a0579ba284a3890e1e

68: 12 GetTickCount ..S...... 89f98205e036c10c0705d3a2b586c6f2

69: 226648 Qd793ycDD2ovXSrB A...'..j/]\*...|. 5e6cbbb9c6bb91e68401c6884367211d

70: 5932 AfK7wK8HOmJ0/hhN ......:bt..M3?7. abedaf62d52488342105d879f4c88014

71: 8 assembly j....r 18f48e3349683c1c83213a713175e10a

72: 16 manifestVersion= ...}.-U.... c79f78f9cc6a44d32e93ef8f45bb114a

73: 8 security ....+r 7b7046e81624d6b2198322957d539ffd

74: 24 /requestedExecut .....-y.1y.....z 342f75f187102269c86c458145d80335

75: 20 /requestedPrivil .....-y.....z.. cf1544b68e0282ca88ed6032a194cbc9

76: 16 assemblyIdentity j....r!...+r 5247102280526c482016a0ab38bfca15

77: 4 VC90 T/t b839b8c8c84be83efdcb5de0995a083b

78: 8 version= ..... e785bc51de0d390cd253667578713e63

79: 16 1fc8b3b9a1e18e3b ..<ov.kW.... db59e838f4ab9d88bf266967603be840

80: 8 Services I..... 14973340cf3594f091db88d63b721b7b

81: 12 Division1806 .+..\*'..: 2bbd7d7d9e5899297c1867a68646c8ad

82: 4 2006 .M: 5a6dcbec7c4074fd8c701a762c658eff

83: 4 Root F.- bdecd08d41b380e34369dae316c8971c

84: 8 Services I..... 14973340cf3594f091db88d63b721b7b

85: 12 Division1806 .+..\*'..: 2bbd7d7d9e5899297c1867a68646c8ad

86: 4 2006 .M: 5a6dcbec7c4074fd8c701a762c658eff

87: 4 Root F.- bdecd08d41b380e34369dae316c8971c

88: 4 WHP0 Xs. a68553d0f943873234ba19eef7da5438

89: 8 Services I..... 14973340cf3594f091db88d63b721b7b

90: 12 Division1806 .+..\*'..: 2bbd7d7d9e5899297c1867a68646c8ad

91: 4 2006 .M: 5a6dcbec7c4074fd8c701a762c658eff

92: 4 Root F.- bdecd08d41b380e34369dae316c8971c

93: 16 231209235959Z0L1 .}v.....}gB. fd10f2064fbb5aa123413e222c70e394

94: 4 Code ..^ 7ed6fe519cf4ce24e8ed7e7d6b00e527

95: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

96: 4 //t2 ..v 395a46fee6e893ab9d4d8ad6c9901357

97: 4 com0 r.. e13e76d20f485da7422f4bb740f6ad04

98: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

99: 4 //t1 ..u 5a37af6bdf2a2c0395a0957b340608bc

100: 4 crl0 r.t c26592d9efb4609635cce57b15e9c6fe

101: 4 5680 ..4 14d0cfb7f8b3d4b08b49e3d864c347fa

102: 4 WHP0 Xs. a68553d0f943873234ba19eef7da5438

103: 4 Code ..^ 7ed6fe519cf4ce24e8ed7e7d6b00e527

104: 4 VIEW T.. d1178ed3e94959e8b6a7569459024f2b

105: 8 LIMITED1 ,..L@. 9e0d6db7978e8cd5275149639d41c5b3

106: 4 VIEW T.. d1178ed3e94959e8b6a7569459024f2b

107: 8 LIMITED0 ,..L@. 8e861221d8abaf7bf95159866b3f6db0

108: 4 NhCX 6.. 92a01b6d05d75c7819c7ecdbb46cc5c8

109: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

110: 4 //tl ..e b2756e111cdf4ecefd6d29004bcb9c3f

111: 4 crl0 r.t c26592d9efb4609635cce57b15e9c6fe

112: 16 com/repository0W r....h.+h.-. 0a015f76242234f6b9aa64b90f4ec238

113: 4 K0I0 +B4 1e330f7438083eec3859cf39fb2d95d7

114: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

115: 4 //tl ..e b2756e111cdf4ecefd6d29004bcb9c3f

116: 4 com0 r.. e13e76d20f485da7422f4bb740f6ad04

117: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

118: 4 //tl ..e b2756e111cdf4ecefd6d29004bcb9c3f

119: 4 crt0 r.t 0737c48913ed450a5977733e3125fc6f

120: 4 PIGH <.. 7dca235ff5950b079a700b8d007cf99f

121: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

122: 4 Inc1 "w5 76db41b95aaf2bce8b63f404b93c1841

123: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

124: 4 com1 r.. 63bdceefcb756160d9280aa4bd88f32f

125: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

126: 16 241022000000Z0G1 ..t.m4.M4gA. 5f47775ae3c33c4c6b77361c3b993252

127: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

128: 4 4/1w ..p a09abf4ad70f84db82fb1387a3d62b40

129: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

130: 8 com/CPS0 r..... 49c70ae3290e2d9361ff68a6d5cf000a

131: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

132: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

133: 4 k0i0 .H. dc477f4dc5964b8e23f7c92e9a0b8c46

134: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

135: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

136: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

137: 4 crt0 r.t 0737c48913ed450a5977733e3125fc6f

138: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

139: 4 Inc1 "w5 76db41b95aaf2bce8b63f404b93c1841

140: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

141: 4 com1 r.. 63bdceefcb756160d9280aa4bd88f32f

142: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

143: 4 Root F.- bdecd08d41b380e34369dae316c8971c

144: 16 211110000000Z0b1 .]u.M4.M4gF. 169dbe0a81e05d04de201e779ad3b080

145: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

146: 4 Inc1 "w5 76db41b95aaf2bce8b63f404b93c1841

147: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

148: 4 com1 r.. 63bdceefcb756160d9280aa4bd88f32f

149: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

150: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

151: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

152: 4 htm0 ... 49143f140e001636fb339d9d030538ea

153: 4 m0k0 .I4 4b15b07ded099e42a7abb8d243ffeb8c

154: 4 http ..i 2faea3830bd577168ebb98f7276d37cc

155: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

156: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

157: 4 crt0 r.t 0737c48913ed450a5977733e3125fc6f

158: 4 z0x0 .Lt d91c81f7fde77c957036cdb204bdfd09

159: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

160: 4 crl0 r.t c26592d9efb4609635cce57b15e9c6fe

161: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

162: 4 crl0 r.t c26592d9efb4609635cce57b15e9c6fe

163: 4 Code ..^ 7ed6fe519cf4ce24e8ed7e7d6b00e527

164: 4 zVhD .XC 91452a63587dbaced25ca6389799750c

165: 4 aUX4 iE. 843515c79da2423bd64acbb18ef8a604

166: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

167: 4 Inc1 "w5 76db41b95aaf2bce8b63f404b93c1841

168: 8 digicert v("q.. b9971430c321df5670ccd826ed6f0989

169: 4 com1 r.. 63bdceefcb756160d9280aa4bd88f32f

170: 8 DigiCert .("... abfb4487f1a55822f3f904cca95ae184

**File 2: 16429e95922c9521f7a40fa8f4c866444a060122448b243444dd2358a96a344c.txt**

**Exiftool**

ExifTool Version Number : 12.00

File Name : 16429e95922c9521f7a40fa8f4c866444a060122448b243444dd2358a96a344c.txt

Directory : ..

File Size : 211 kB

File Modification Date/Time : 2020:08:21 00:04:18-04:00

File Access Date/Time : 2020:08:22 13:29:08-04:00

File Inode Change Date/Time : 2020:08:21 00:04:18-04:00

File Permissions : rwxr-xr-x

File Type : DOCM

File Type Extension : docm

MIME Type : application/vnd.ms-word.document.macroEnabled

Zip Required Version : 20

Zip Bit Flag : 0

Zip Compression : Deflated

Zip Modify Date : 1980:01:01 00:00:00

Zip CRC : 0xc6337d17

Zip Compressed Size : 501

Zip Uncompressed Size : 2645

Zip File Name : [Content\_Types].xml

Template : Normal.dotm

Total Edit Time : 0

Pages : 176

Words : 103086

Characters : 587595

Application : Microsoft Office Word

Doc Security : None

Lines : 4896

Paragraphs : 1378

Scale Crop : No

Heading Pairs : Title, 1

Titles Of Parts :

Company :

Links Up To Date : No

Characters With Spaces : 689303

Shared Doc : No

Hyperlinks Changed : No

App Version : 14.0000

Creator :

Last Modified By :

Revision Number : 1

Create Date : 2019:07:08 09:55:00Z

Modify Date : 2019:07:09 12:20:00Z

**vmonkey Analysis**

{

"file\_name": "16429e95922c9521f7a40fa8f4c866444a060122448b243444dd2358a96a344c.txt",

"vba\_builtins": [

"CallByName",

"Chr",

"Close",

"CreateObject",

"MsgBox",

"Variables"

],

"potential\_iocs": [],

"actions": [

{

"action": "Found Entry Point",

"description": "",

"parameters": "document\_open"

},

{

"action": "OPEN",

"description": "Open File",

"parameters": "C:\\CURRENT\_FILE\_NAME.docmx"

},

{

"action": "Dropped File Hash",

"description": "File Name: C:/CURRENT\_FILE\_NAME.docmx",

"parameters": "f9c63977a1147e254ab0fd8c65119bc851e83531dc77461cb5632b477d51cdaa"

},

{

"action": "Found Entry Point",

"description": "",

"parameters": "document\_close"

},

{

"action": "Run",

"description": "Interesting Function Call",

"parameters": " /e:JScript \"C:\\CURRENT\_FILE\_NAME.docmx\""

},

{

"action": "Execute Command",

"description": "Shell function",

"parameters": "WScript /e:JScript \"C:\\CURRENT\_FILE\_NAME.docmx\""

}

]

}

**Olevba Scan**

olevba 0.55.1 on Python 3.6.9 - http://decalage.info/python/oletools

===============================================================================

FILE: ../16429e95922c9521f7a40fa8f4c866444a060122448b243444dd2358a96a344c.txt

Type: OpenXML

+----------+--------------------+---------------------------------------------+

|Type |Keyword |Description |

+----------+--------------------+---------------------------------------------+

|AutoExec |Document\_Close |Runs when the Word document is closed |

|AutoExec |Document\_New |Runs when a new Word document is created |

|AutoExec |Document\_Open |Runs when the Word or Publisher document is |

| | |opened |

|Suspicious|open |May open a file |

|Suspicious|Output |May write to a file (if combined with Open) |

|Suspicious|Print # |May write to a file (if combined with Open) |

|Suspicious|CreateObject |May create an OLE object |

|Suspicious|CallByName |May attempt to obfuscate malicious function |

| | |calls |

|Suspicious|Chr |May attempt to obfuscate specific strings |

| | |(use option --deobf to deobfuscate) |

|Suspicious|.Variables |May use Word Document Variables to store and |

| | |hide data |

|Suspicious|Base64 Strings |Base64-encoded strings were detected, may be |

| | |used to obfuscate strings (option --decode to|

| | |see all) |

+----------+--------------------+---------------------------------------------+

**Oledump**

A: word/vbaProject.bin

A1: 492 'PROJECT'

A2: 71 'PROJECTwm'

A3: M 4121 'VBA/NewMacros'

A4: M 1639 'VBA/ThisDocument'

A5: 2855 'VBA/\_VBA\_PROJECT'

A6: 1270 'VBA/\_\_SRP\_0'

A7: 96 'VBA/\_\_SRP\_1'

A8: 154 'VBA/\_\_SRP\_2'

A9: 382 'VBA/\_\_SRP\_3'

A10: 577 'VBA/dir'

**File 3: 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt**

**Exiftool**

ExifTool Version Number : 12.00

File Name : 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt

Directory : ..

File Size : 209 kB

File Modification Date/Time : 2020:08:21 00:04:18-04:00

File Access Date/Time : 2020:08:21 00:31:38-04:00

File Inode Change Date/Time : 2020:08:21 00:04:18-04:00

File Permissions : rwxr-xr-x

File Type : DOCM

File Type Extension : docm

MIME Type : application/vnd.ms-word.document.macroEnabled

Zip Required Version : 20

Zip Bit Flag : 0

Zip Compression : Deflated

Zip Modify Date : 1980:01:01 00:00:00

Zip CRC : 0xc6337d17

Zip Compressed Size : 501

Zip Uncompressed Size : 2645

Zip File Name : [Content\_Types].xml

Template : Normal.dotm

Total Edit Time : 0

Pages : 162

Words : 99033

Characters : 564491

Application : Microsoft Office Word

Doc Security : None

Lines : 4704

Paragraphs : 1324

Scale Crop : No

Heading Pairs : Title, 1

Titles Of Parts :

Company :

Links Up To Date : No

Characters With Spaces : 662200

Shared Doc : No

Hyperlinks Changed : No

App Version : 14.0000

Creator :

Last Modified By :

Revision Number : 1

Create Date : 2019:07:08 09:55:00Z

Modify Date : 2019:07:12 07:14:00Z

**Vmonkey analysis**

FILE: 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt

-------------------------------------------------------------------------------

VBA MACRO ThisDocument.cls

in file: word/vbaProject.bin - OLE stream: u'VBA/ThisDocument'

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

-------------------------------------------------------------------------------

-------------------------------------------------------------------------------

PARSING VBA CODE:

-------------------------------------------------------------------------------

TRACING VBA CODE (entrypoint = Auto\*):

Recorded Actions:

+-------------------+---------------------------+---------------------------+

| Action | Parameters | Description |

+-------------------+---------------------------+---------------------------+

| Found Entry Point | document\_open | |

| OPEN | C:\CURRENT\_FILE\_NAME.docm | Open File |

| | .ini | |

| Dropped File Hash | 3579f4d0efefcf7d1f0cc96e4 | File Name: C:/CURRENT\_FIL |

| | 53127c3aafde9058aef942b93 | E\_NAME.docm.ini |

| | 9c6a92220c735f | |

| Found Entry Point | document\_close | |

| CreateObject | ['Shell.Application'] | Interesting Function Call |

| Run | /e:JScript "C:\CURRENT\_FI | Interesting Function Call |

| | LE\_NAME.docm.ini" | |

| Execute Command | WScript /e:JScript "C:\CU | Shell function |

| | RRENT\_FILE\_NAME.docm.ini" | |

+-------------------+---------------------------+---------------------------+

VBA Builtins Called: ['CallByName', 'Chr', 'Close', 'CreateObject', 'MsgBox', 'Variables']

Finished analyzing 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt .

**Olevba**

FILE: 41cd7fec5eaad44d2dba028164b9b9e2d1c6ea9d035679651b3b344542c40d45.txt

Type: OpenXML

+----------+--------------------+---------------------------------------------+

|Type |Keyword |Description |

+----------+--------------------+---------------------------------------------+

|AutoExec |Document\_Close |Runs when the Word document is closed |

|AutoExec |Document\_New |Runs when a new Word document is created |

|AutoExec |Document\_Open |Runs when the Word or Publisher document is |

| | |opened |

|Suspicious|Open |May open a file |

|Suspicious|Output |May write to a file (if combined with Open) |

|Suspicious|Print # |May write to a file (if combined with Open) |

|Suspicious|CreateObject |May create an OLE object |

|Suspicious|CallByName |May attempt to obfuscate malicious function |

| | |calls |

|Suspicious|Chr |May attempt to obfuscate specific strings |

| | |(use option --deobf to deobfuscate) |

|Suspicious|.Variables |May use Word Document Variables to store and |

| | |hide data |

|Suspicious|Base64 Strings |Base64-encoded strings were detected, may be |

| | |used to obfuscate strings (option --decode to|

| | |see all) |

+----------+--------------------+---------------------------------------------+

**Oledump**

A: word/vbaProject.bin

A1: 490 'PROJECT'

A2: 71 'PROJECTwm'

A3: M 3354 'VBA/NewMacros'

A4: M 1795 'VBA/ThisDocument'

A5: 2934 'VBA/\_VBA\_PROJECT'

A6: 583 'VBA/dir'

**File 4: 666515eec773e200663fbd5fcad7109e9b97be11a83b41b8a4d73b7f5c8815ff.txt**

**Exiftool**

ExifTool Version Number : 12.00

File Name : 666515eec773e200663fbd5fcad7109e9b97be11a83b41b8a4d73b7f5c8815ff.txt

Directory : ..

File Size : 214 kB

File Modification Date/Time : 2020:08:21 00:04:18-04:00

File Access Date/Time : 2020:08:21 00:31:38-04:00

File Inode Change Date/Time : 2020:08:21 00:04:18-04:00

File Permissions : rwxr-xr-x

File Type : DOCM

File Type Extension : docm

MIME Type : application/vnd.ms-word.document.macroEnabled

Zip Required Version : 20

Zip Bit Flag : 0

Zip Compression : Deflated

Zip Modify Date : 1980:01:01 00:00:00

Zip CRC : 0xc6337d17

Zip Compressed Size : 501

Zip Uncompressed Size : 2645

Zip File Name : [Content\_Types].xml

Template : Normal.dotm

Total Edit Time : 0

Pages : 161

Words : 99157

Characters : 565201

Application : Microsoft Office Word

Doc Security : None

Lines : 4710

Paragraphs : 1326

Scale Crop : No

Heading Pairs : Title, 1

Titles Of Parts :

Company :

Links Up To Date : No

Characters With Spaces : 663032

Shared Doc : No

Hyperlinks Changed : No

App Version : 14.0000

Creator :

Last Modified By :

Revision Number : 1

Create Date : 2019:07:08 09:55:00Z

Modify Date : 2019:07:16 10:47:00Z

**Vmonkey analysis**

FILE: 666515eec773e200663fbd5fcad7109e9b97be11a83b41b8a4d73b7f5c8815ff.txt

Recorded Actions:

+-------------------+-----------------------+---------------------------+

| Action | Parameters | Description |

+-------------------+-----------------------+---------------------------+

| Found Entry Point | document\_open | |

| Found Entry Point | document\_close | |

| Run | /e:JScript "" | Interesting Function Call |

| Execute Command | WScript /e:JScript "" | Shell function |

+-------------------+-----------------------+---------------------------+

**Olevba**

FILE: 666515eec773e200663fbd5fcad7109e9b97be11a83b41b8a4d73b7f5c8815ff.txt

Type: OpenXML

+----------+--------------------+---------------------------------------------+

|Type |Keyword |Description |

+----------+--------------------+---------------------------------------------+

|AutoExec |Document\_Close |Runs when the Word document is closed |

|AutoExec |Document\_New |Runs when a new Word document is created |

|AutoExec |Document\_Open |Runs when the Word or Publisher document is |

| | |opened |

|Suspicious|Open |May open a file |

|Suspicious|Output |May write to a file (if combined with Open) |

|Suspicious|Print # |May write to a file (if combined with Open) |

|Suspicious|CreateObject |May create an OLE object |

|Suspicious|CallByName |May attempt to obfuscate malicious function |

| | |calls |

|Suspicious|Chr |May attempt to obfuscate specific strings |

| | |(use option --deobf to deobfuscate) |

|Suspicious|.Variables |May use Word Document Variables to store and |

| | |hide data |

|Suspicious|Base64 Strings |Base64-encoded strings were detected, may be |

| | |used to obfuscate strings (option --decode to|

| | |see all) |

+----------+--------------------+---------------------------------------------+

**Oledump**

A: word/vbaProject.bin

A1: 492 'PROJECT'

A2: 71 'PROJECTwm'

A3: M 5420 'VBA/NewMacros'

A4: M 1579 'VBA/ThisDocument'

A5: 2961 'VBA/\_VBA\_PROJECT'

A6: 583 'VBA/dir'

**File 5: 970b135b4c47c12f97bc3d3bbdf325f391b499d03fe19ac9313bcace3a1450d2.txt**

**Exiftool**

ExifTool Version Number : 12.00

File Name : 970b135b4c47c12f97bc3d3bbdf325f391b499d03fe19ac9313bcace3a1450d2.txt

Directory : .

File Size : 301 kB

File Modification Date/Time : 2020:08:21 00:04:18-04:00

File Access Date/Time : 2020:08:21 00:31:38-04:00

File Inode Change Date/Time : 2020:08:21 00:04:18-04:00

File Permissions : rwxr-xr-x

File Type : TXT

File Type Extension : txt

MIME Type : text/plain

MIME Encoding : us-ascii

Newlines : Unix LF

Line Count : 4008

Word Count : 4301

**Peframe**

--------------------------------------------------------------------------------

File Information (time: 0:00:03.138274)

--------------------------------------------------------------------------------

filename 970b135b4c47c12f97bc3d3bbdf325f391b499d03fe19ac9313bcace3a1450d2.txt

filetype ASCII text, with CRLF, LF line terminators

filesize 308571

hash sha256 970b135b4c47c12f97bc3d3bbdf325f391b499d03fe19ac9313bcace3a1450d2

virustotal /

--------------------------------------------------------------------------------

Ip Address

--------------------------------------------------------------------------------

10.200.200.200

10.1.73.40

10.1.15.15

5.61.35.167

65.254.253.50

10.1.18.1

127.0.0.1

10.114.3.31

--------------------------------------------------------------------------------

Url

--------------------------------------------------------------------------------

https://10.200.200.200:443/cgi-mod/mark.cgi

--------------------------------------------------------------------------------

Fuzzing

--------------------------------------------------------------------------------

Possible connections

**3. Forensics of Tails VM Image**

**Tcpdump**

08:55:29.694383 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 1260379453:1260379996, ack 2300241, win 65535, length 543

08:55:29.694611 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 543, win 65535, length 0

08:55:34.099901 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 543:1086, ack 1, win 65535, length 543

08:55:34.100163 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 1086, win 65535, length 0

08:55:34.423695 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 1086:1629, ack 1, win 65535, length 543

08:55:34.423946 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 1629, win 65535, length 0

08:55:34.442386 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 1:544, ack 1629, win 65535, length 543

08:55:34.442474 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 544, win 65535, length 0

08:55:34.443308 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 1629:2172, ack 544, win 65535, length 543

08:55:34.443546 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 2172, win 65535, length 0

08:55:34.644943 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 544:1087, ack 2172, win 65535, length 543

08:55:34.644996 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 1087, win 65535, length 0

08:55:34.645768 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 2172:2715, ack 1087, win 65535, length 543

08:55:34.646038 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 2715, win 65535, length 0

08:55:34.850441 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 1087:1630, ack 2715, win 65535, length 543

08:55:34.850481 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 1630, win 65535, length 0

08:55:34.892483 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 2715:3258, ack 1630, win 65535, length 543

08:55:34.892727 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 3258, win 65535, length 0

08:55:35.054058 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 1630:2173, ack 3258, win 65535, length 543

08:55:35.054099 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 2173, win 65535, length 0

08:55:35.054849 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 3258:3801, ack 2173, win 65535, length 543

08:55:35.055074 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 3801, win 65535, length 0

08:55:35.258884 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 2173:2716, ack 3801, win 65535, length 543

08:55:35.260860 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 3801:4858, ack 2716, win 65535, length 1057

08:55:35.261089 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 4858, win 65535, length 0

08:55:35.464521 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 2716:3259, ack 4858, win 65535, length 543

08:55:35.508096 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 3259, win 65535, length 0

08:55:35.580227 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 3259:4707, ack 4858, win 65535, length 1448

08:55:35.580270 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 4707, win 65535, length 0

08:55:35.583584 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 4707:6155, ack 4858, win 65535, length 1448

08:55:35.583617 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 6155, win 65535, length 0

08:55:35.664652 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 6155:7429, ack 4858, win 65535, length 1274

08:55:35.664693 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 7429, win 65535, length 0

08:55:35.676465 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 4858:5401, ack 7429, win 65535, length 543

08:55:35.676688 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 5401, win 65535, length 0

08:55:35.688687 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 5401:6458, ack 7429, win 65535, length 1057

08:55:35.688899 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 6458, win 65535, length 0

08:55:36.086707 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 7429:7972, ack 6458, win 65535, length 543

08:55:36.086778 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 7972, win 65535, length 0

08:55:36.105605 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 7972:9420, ack 6458, win 65535, length 1448

08:55:36.105653 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 9420, win 65535, length 0

08:55:36.106517 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 9420:10868, ack 6458, win 65535, length 1448

08:55:36.106543 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 10868, win 65535, length 0

08:55:36.117133 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 10868:12316, ack 6458, win 65535, length 1448

08:55:36.117173 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 12316, win 65535, length 0

08:55:36.118284 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 12316:13764, ack 6458, win 65535, length 1448

08:55:36.118330 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 13764, win 65535, length 0

08:55:36.121506 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 13764:15212, ack 6458, win 65535, length 1448

08:55:36.121553 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 15212, win 65535, length 0

08:55:36.125792 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 15212:16660, ack 6458, win 65535, length 1448

08:55:36.125844 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 16660, win 65535, length 0

08:55:36.126881 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [P.], seq 16660:19556, ack 6458, win 65535, length 2896

08:55:36.126916 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [.], ack 19556, win 65535, length 0

08:55:36.128518 IP 10.0.2.15.45554 > 144.76.57.183.9001: Flags [P.], seq 6458:7001, ack 19556, win 65535, length 543

08:55:36.128733 IP 144.76.57.183.9001 > 10.0.2.15.45554: Flags [.], ack 7001, win 65535, length 0

**Netstat**

#kernel

IpInReceives 12532 0.0

IpInAddrErrors 2 0.0

IpInDelivers 12530 0.0

IpOutRequests 12037 0.0

IpOutDiscards 6 0.0

IpOutNoRoutes 10 0.0

IcmpInMsgs 4 0.0

IcmpInDestUnreachs 4 0.0

IcmpOutMsgs 4 0.0

IcmpOutDestUnreachs 4 0.0

IcmpMsgInType3 4 0.0

IcmpMsgOutType3 4 0.0

TcpActiveOpens 109 0.0

TcpPassiveOpens 103 0.0

TcpAttemptFails 1 0.0

TcpEstabResets 12 0.0

TcpInSegs 12526 0.0

TcpOutSegs 12275 0.0

TcpRetransSegs 7 0.0

TcpOutRsts 11 0.0

TcpExtTW 74 0.0

TcpExtDelayedACKs 190 0.0

TcpExtDelayedACKLost 1 0.0

TcpExtTCPHPHits 4948 0.0

TcpExtTCPPureAcks 1732 0.0

TcpExtTCPHPAcks 3688 0.0

TcpExtTCPLostRetransmit 5 0.0

TcpExtTCPTimeouts 7 0.0

TcpExtTCPLossProbes 1 0.0

TcpExtTCPBacklogCoalesce 59 0.0

TcpExtTCPDSACKOldSent 1 0.0

TcpExtTCPDSACKRecv 1 0.0

TcpExtTCPAbortOnData 6 0.0

TcpExtTCPAbortOnClose 5 0.0

TcpExtTCPAbortOnTimeout 1 0.0

TcpExtTCPDSACKIgnoredNoUndo 1 0.0

TcpExtTCPRcvCoalesce 805 0.0

TcpExtTCPAutoCorking 37 0.0

TcpExtTCPSynRetrans 6 0.0

TcpExtTCPOrigDataSent 5380 0.0

TcpExtTCPHystartTrainDetect 3 0.0

TcpExtTCPHystartTrainCwnd 55 0.0

TcpExtTCPKeepAlive 148 0.0

TcpExtTCPDelivered 5478 0.0

TcpExtTcpTimeoutRehash 1 0.0

IpExtInOctets 18495410 0.0

IpExtOutOctets 9072202 0.0

IpExtInNoECTPkts 19501 0.0

**Tor Logs**

Aug 23 08:47:51.000 [notice] Tor 0.4.3.5 opening new log file.

Aug 23 08:47:51.308 [notice] Tor 0.4.3.5 running on Linux with Libevent 2.1.8-stable, OpenSSL 1.1.1d, Zlib 1.2.11, Liblzma 5.2.4, and Libzstd 1.3.8.

Aug 23 08:47:51.309 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning

Aug 23 08:47:51.309 [notice] Read configuration file "/usr/share/tor/tor-service-defaults-torrc".

Aug 23 08:47:51.309 [notice] Read configuration file "/etc/tor/torrc".

Aug 23 08:47:51.309 [warn] Skipping obsolete configuration option "ControlListenAddress".

Aug 23 08:47:51.309 [warn] Skipping obsolete configuration option "TransListenAddress".

Aug 23 08:47:51.309 [warn] Skipping obsolete configuration option "WarnUnsafeSocks".

Aug 23 08:47:51.319 [notice] Opening Socks listener on 127.0.0.1:9050

Aug 23 08:47:51.319 [notice] Opened Socks listener on 127.0.0.1:9050

Aug 23 08:47:51.319 [notice] Opening Socks listener on 127.0.0.1:9062

Aug 23 08:47:51.319 [notice] Opened Socks listener on 127.0.0.1:9062

Aug 23 08:47:51.319 [notice] Opening Socks listener on 127.0.0.1:9150

Aug 23 08:47:51.319 [notice] Opened Socks listener on 127.0.0.1:9150

Aug 23 08:47:51.319 [notice] Opening DNS listener on 127.0.0.1:5353

Aug 23 08:47:51.319 [notice] Opened DNS listener on 127.0.0.1:5353

Aug 23 08:47:51.320 [notice] Opening Transparent pf/netfilter listener on 127.0.0.1:9040

Aug 23 08:47:51.320 [notice] Opened Transparent pf/netfilter listener on 127.0.0.1:9040

Aug 23 08:47:51.320 [notice] Opening Control listener on 127.0.0.1:9052

Aug 23 08:47:51.320 [notice] Opened Control listener on 127.0.0.1:9052

Aug 23 08:47:51.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.

Aug 23 08:47:52.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.

Aug 23 08:47:52.000 [notice] Bootstrapped 0% (starting): Starting

Aug 23 08:47:52.000 [notice] Starting with guard context "default"

Aug 23 08:47:52.000 [notice] Signaled readiness to systemd

Aug 23 08:47:52.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:52.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:53.000 [notice] Opening Control listener on /run/tor/control

Aug 23 08:47:53.000 [notice] Opened Control listener on /run/tor/control

Aug 23 08:47:53.000 [notice] Bootstrapped 5% (conn): Connecting to a relay

Aug 23 08:47:53.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:53.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:54.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:54.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:54.000 [notice] Bootstrapped 10% (conn\_done): Connected to a relay

Aug 23 08:47:54.000 [notice] Bootstrapped 14% (handshake): Handshaking with a relay

Aug 23 08:47:55.000 [notice] Bootstrapped 15% (handshake\_done): Handshake with a relay done

Aug 23 08:47:55.000 [notice] Bootstrapped 20% (onehop\_create): Establishing an encrypted directory connection

Aug 23 08:47:55.000 [notice] Bootstrapped 25% (requesting\_status): Asking for networkstatus consensus

Aug 23 08:47:55.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:55.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:55.000 [notice] Bootstrapped 30% (loading\_status): Loading networkstatus consensus

Aug 23 08:47:56.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:57.000 [notice] I learned some more directory information, but not enough to build a circuit: We have no usable consensus.

Aug 23 08:47:57.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:57.000 [notice] Bootstrapped 40% (loading\_keys): Loading authority key certs

Aug 23 08:47:57.000 [notice] The current consensus has no exit nodes. Tor can only build internal paths, such as paths to onion services.

Aug 23 08:47:57.000 [notice] Bootstrapped 45% (requesting\_descriptors): Asking for relay descriptors

Aug 23 08:47:57.000 [notice] I learned some more directory information, but not enough to build a circuit: We need more microdescriptors: we have 0/6582, and can only build 0% of likely paths. (We have 0% of guards bw, 0% of midpoint bw, and 0% of end bw (no exits in consensus, using mid) = 0% of path bw.)

Aug 23 08:47:57.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:58.000 [notice] Bootstrapped 50% (loading\_descriptors): Loading relay descriptors

Aug 23 08:47:58.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:59.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:47:59.000 [notice] The current consensus contains exit nodes. Tor can build exit and internal paths.

Aug 23 08:47:59.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:00.000 [notice] Bootstrapped 55% (loading\_descriptors): Loading relay descriptors

Aug 23 08:48:00.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:01.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:01.000 [notice] Bootstrapped 63% (loading\_descriptors): Loading relay descriptors

Aug 23 08:48:01.000 [notice] Bootstrapped 68% (loading\_descriptors): Loading relay descriptors

Aug 23 08:48:01.000 [notice] Bootstrapped 75% (enough\_dirinfo): Loaded enough directory info to build circuits

Aug 23 08:48:01.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:02.000 [notice] Bootstrapped 80% (ap\_conn): Connecting to a relay to build circuits

Aug 23 08:48:02.000 [notice] Bootstrapped 85% (ap\_conn\_done): Connected to a relay to build circuits

Aug 23 08:48:02.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:02.000 [notice] Bootstrapped 89% (ap\_handshake): Finishing handshake with a relay to build circuits

Aug 23 08:48:03.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:03.000 [notice] Bootstrapped 90% (ap\_handshake\_done): Handshake finished with a relay to build circuits

Aug 23 08:48:03.000 [notice] Bootstrapped 95% (circuit\_create): Establishing a Tor circuit

Aug 23 08:48:03.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:04.000 [notice] Bootstrapped 100% (done): Done

Aug 23 08:48:05.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:48:05.000 [notice] New control connection opened from 127.0.0.1.

Aug 23 08:53:40.000 [notice] New control connection opened.

Aug 23 08:53:41.000 [notice] New control connection opened.

Aug 23 08:53:43.000 [warn] Rejecting SOCKS request for anonymous connection to private address [scrubbed].

Aug 23 08:56:32.000 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit $6AD2D73B1A0A931AD792117D58A6C65EF411EBC2~Hugin at 185.214.167.254. Retrying on a new circuit.

Aug 23 08:56:47.000 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit $1D8DE4EF4BFA38D366FCE7249DC41A540D8E1EB9~TORKeFFORG4 at 45.154.255.69. Retrying on a new circuit.

Aug 23 08:57:02.000 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit $56850752096EE63711F99B2FA5A812477561697D~niftyafricagiantrat at 185.220.101.135. Retrying on a new circuit.

Aug 23 08:57:17.000 [notice] We tried for 15 seconds to connect to '[scrubbed]' using exit $5649CB2158DA94FB747415F26628BEC07FA57616~QuintexAirVPN8 at 199.249.230.122. Retrying on a new circuit.

**htpdate logs**

Running htpdate.

getUrlDateDiff: https://squat.net

getUrlDateDiff: https://getfedora.org

getUrlDateDiff: https://www.google.com

https://squat.net (took 2s) => diff = 1 second(s)

https://getfedora.org (took 2s) => diff = 1 second(s)

https://www.google.com (took 3s) => diff = 1 second(s)

Median diff: 1 second(s)

Setting time to 1598172489...