Latex Report for VirusShare_0a1343ce3eb87312cc162ed400422a96

Cuckoo Sandbox

April 30, 2021

0.1 Introduction

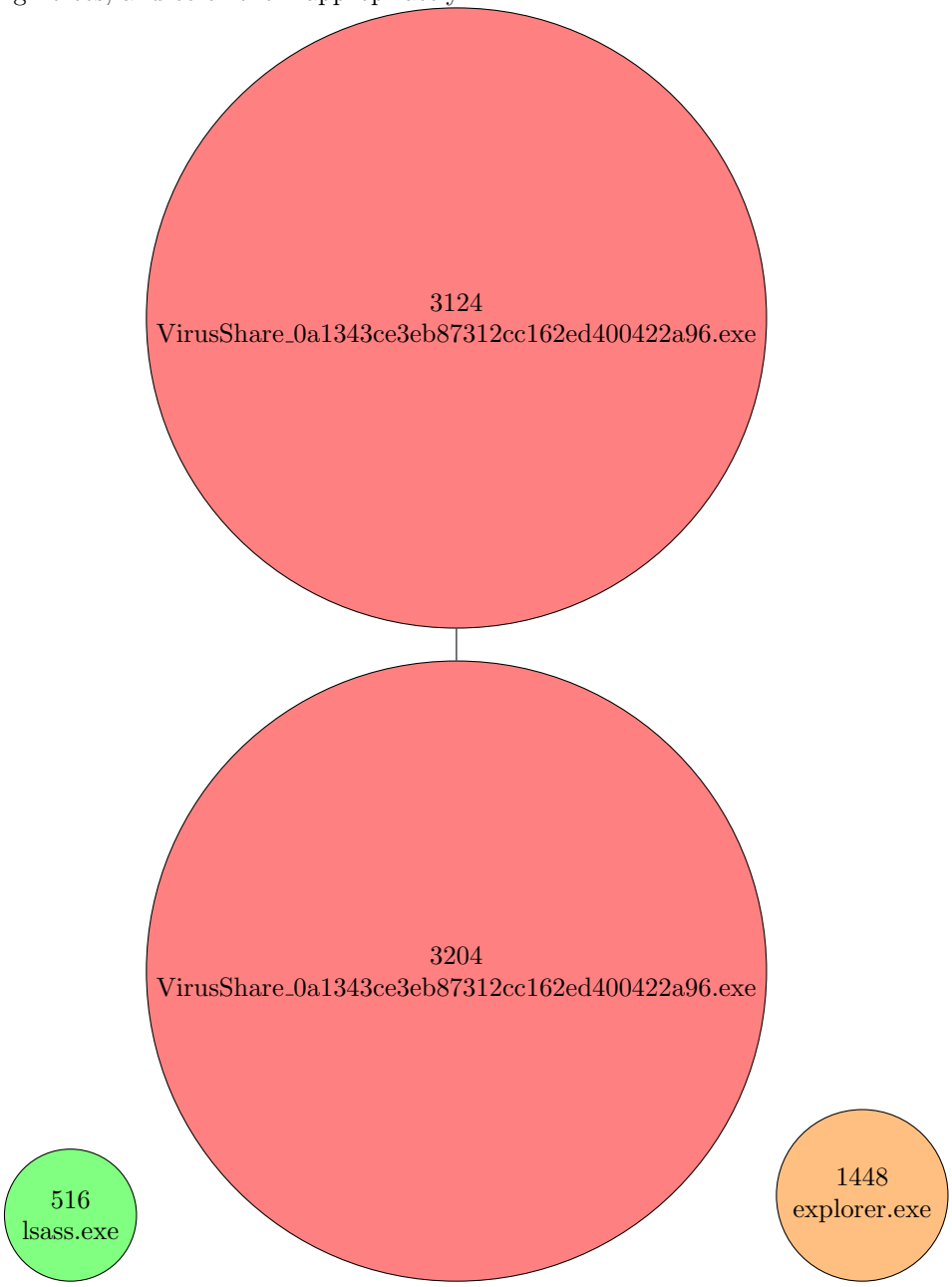
This report contains a summary of various activities and artifacts documented by the cuckoo sandbox report. This report came from executing a file called VirusShare_0a1343ce3eb87312cc162ed400422a96 on a VirtualBox VM for 0:04:24. It was given a score of 7.4. The sections are: signatures, process tree, PE File, API Calls, File System Activity, Registry Activity.

0.2 Signatures

This section outlines information about the different signatures observed during sample execution. These signatures are created by the Cuckoo community, so make note of all of them.The description for each signature is given, along with relevant 'marks', which provide more details about what activity occurred. Description: Queries for the computername

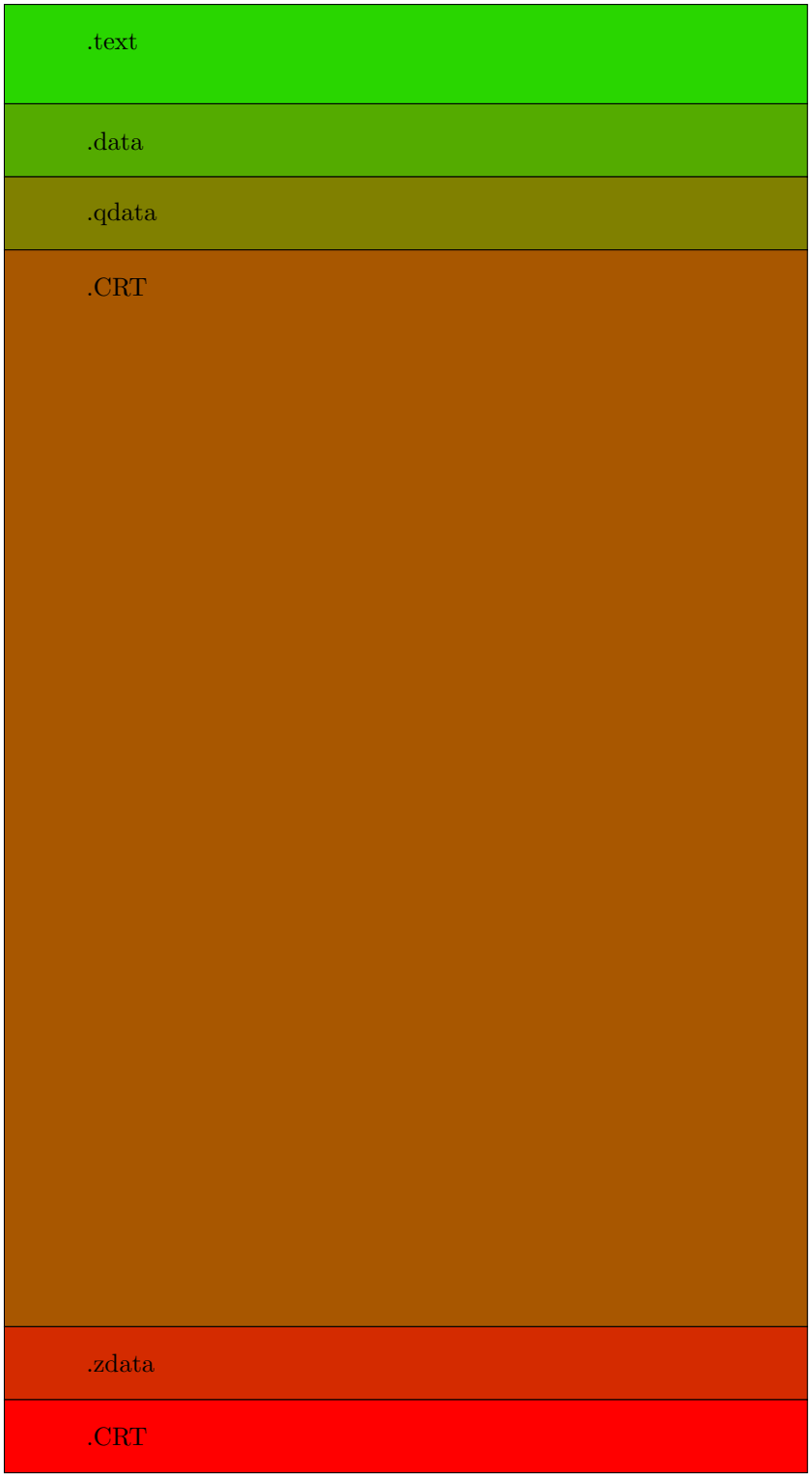
0.3 Process Tree

This is a set of processes observed during sample execution. The tree in red is the one containing the sample. The tree in green is lsass, which is responsible for starting the sample execution. All other trees are in orange. At some point additional functionality may be added to identify definitively malicious or benign trees, and color them appropriately.



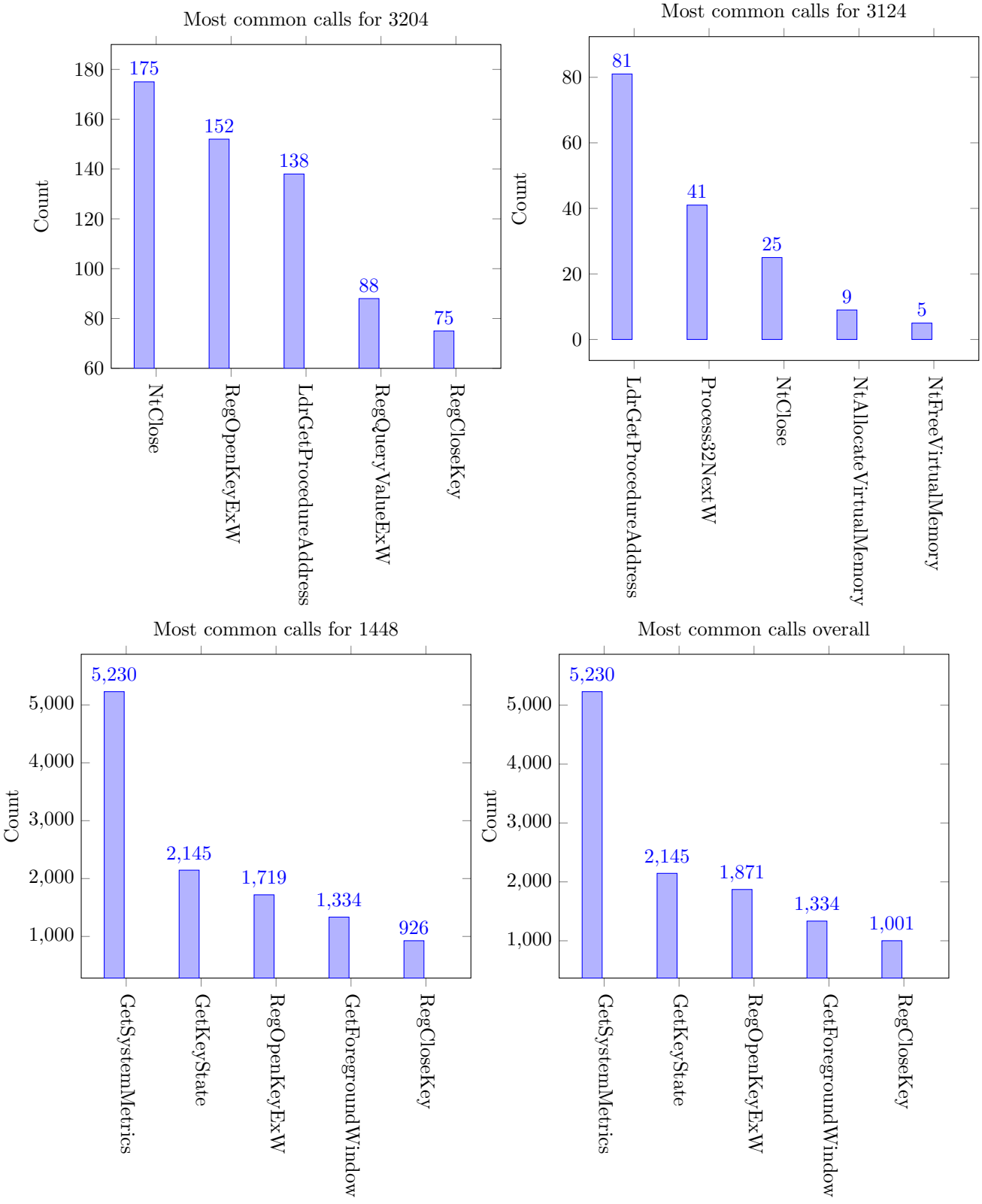
0.4 PE

This section is a display of the sections of the submitted sample. Each section is roughly proportional in size to how large it is in the file. This section is only for purposes of understanding the file sections and layout.



0.5 API Calls

This section is a series of graphs indicating the 5 most common API calls used by each process that was detected by cuckoo. API calls are how malware samples do a significant amount of their activity. These should be checked carefully for suspicious calls. Red columns are APIs that appeared as part of a signature (See section 0.2). These should be treated with extra suspicious. The last graph is the most common API calls overall. Additional functionality to identify potentially malicious API calls may be added at a later date.



0.6 File System Activity

This section outlines all the interactions processes made with the filesystem. This allows analysts to see activity with the same file spread across multiple processes. Additionally copied files have the activity for both their versions combined. Entries in red were handled by a process in the process tree containing the executed sample. These should be investigated further.

File	moved	created	opened	deleted	exists	failed	read
C: \Users \cuckoo \AppData \Local \Temp \VirusShare_0a1343ce3eb87312c aka C: \Windows \System32 \shlpexts.exe \	yes	no	yes	no	yes	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \WER \ERC \statecache.lock \	no	yes	no	no	no	no	no
C: \\	no	no	yes	no	yes	no	no
C: \Users \cuckoo \AppData \	no	no	yes	no	no	no	no
C: \Windows \System32 \	no	no	yes	no	yes	no	no
C: \Users \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \Burn \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Local \Temp \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Local \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \Caches \cversions.1.db \	no	no	yes	no	no	no	no
C: \Users \cuckoo \	no	no	yes	no	yes	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \WER \ERC \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Roaming \Microsoft \Windows \Themes \TranscodedWallpaper.jpg \	no	no	yes	no	no	no	no
C: \Users \desktop.ini \	no	no	yes	no	no	no	yes
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \Caches \AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9.1.ver0x0000000 \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Local \\	no	no	yes	no	no	no	no
C: \Windows \Globalization \Sorting \sortdefault.nls \	no	no	yes	no	no	no	no
C: \Windows \System32 \\	no	no	yes	no	yes	no	no
C: \ProgramData \Microsoft \Windows \WER \ReportArchive \	no	no	yes	no	no	no	no
C: \Windows \	no	no	yes	no	no	no	no
C: \Windows \System32 \tzres.dll \	no	no	yes	no	no	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \WER \ReportArchive \	no	no	yes	no	yes	no	no
C: \Windows \System32 \shlpexts.exe:Zone.Identifier \	no	no	no	yes	no	no	no

C: \Windows \\	no	no	no	no	yes	no	no
C: \Users \cuckoo \AppData \Roaming \	no	no	no	no	yes	no	no
C: \Windows \System32 \propsys.dll \	no	no	no	no	yes	no	no
C: \Windows \explorer.exe \	no	no	no	no	yes	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \WER \ERC \responsestatecache.xml \	no	no	no	no	yes	no	no
C: \Users \cuckoo \AppData \Local \Temp \32 \	no	no	no	no	yes	no	no
C: \Users \cuckoo \AppData \Local \Microsoft \Windows \WER \ERC \queuepester.txt \	no	no	no	no	yes	no	no
C: \Users \cuckoo \AppData \Roaming \Microsoft \Windows \Themes \slideshow.ini \	no	no	no	no	no	yes	no

0.7 Registry Activity

This section outlines all the interactions processes made with the registry. This allows analysts to see activity with the same registry spread across multiple processes. Entries in red were accessed by a process in the process tree started by the sample. These should be investigated further for changes.

Registry	opened	read	written
HKEY_CLASSES_ROOT \.tiff \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.wb2 \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.jfif \	yes	no	no
HKEY_CLASSES_ROOT \.secstore \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.exp \	yes	no	no
HKEY_CLASSES_ROOT \.vdx \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.obj \	yes	no	no
HKEY_CLASSES_ROOT \.IVF \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.vor \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.dwfx \OpenWithProgids \	yes	no	no
HKEY_CLASSES_ROOT \.sst \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.ps1xml \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.contact \OpenWithProgids \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.vcf \	yes	no	no
HKEY_CLASSES_ROOT \.avi \	yes	no	no
HKEY_CLASSES_ROOT \.AAC \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.bat \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.bau \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.p7r \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.bas \	yes	no	no
HKEY_CLASSES_ROOT \.group \	yes	no	no

HKEY_CLASSES_ROOT \.wsc \	yes	no	no
HKEY_CLASSES_ROOT \.vssscc \	yes	no	no
HKEY_CLASSES_ROOT \.ai \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.3gp2 \OpenWithProgids \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.mapimail \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.asx \OpenWithProgids \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.jpe \OpenWithProgids \	yes	no	no
HKEY_CLASSES_ROOT \.wsz \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.webp \	yes	no	no
HKEY_CLASSES_ROOT \.scd \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.p7b \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.mp4v \OpenWithProgids \	yes	no	no
HKEY_CLASSES_ROOT \.au \	yes	no	no
HKEY_CLASSES_ROOT \Directory \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.mydocs \	yes	no	no
HKEY_CLASSES_ROOT \.pct \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.p7m \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.appref-ms \	yes	no	no
HKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion \Action Center \Providers \EventLog \DAB69A6A-4D2A-4D44-94BF-E0091898C881 \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.au \OpenWithProgids \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \1 \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \2 \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \3 \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \4 \	yes	no	no
HKEY_CLASSES_ROOT \.vst \	yes	no	no
HKEY_CLASSES_ROOT \.resmoncfg \	yes	no	no
HKEY_CLASSES_ROOT \.xls \	yes	no	no
HKEY_CLASSES_ROOT \.m3u \	yes	no	no
HKEY_CLASSES_ROOT \.mlc \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.stl \	yes	no	no
HKEY_CLASSES_ROOT \.js \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \.py \OpenWithProgids \	yes	no	no
HKEY_CLASSES_ROOT \.slupkg-ms \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.aif \	yes	no	no
HKEY_CLASSES_ROOT \.msstyles \	yes	no	no
HKEY_CLASSES_ROOT \.std \	yes	no	no
HKEY_CLASSES_ROOT \.potx \	yes	no	no
HKEY_CLASSES_ROOT \SystemFileAssociations \.stw \	yes	no	no
HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \0 \	yes	no	no
HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \1 \	yes	no	no

HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \2 \	yes	no	no
HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \3 \	yes	no	no
HKEY_LOCAL_MACHINE \Software \Policies \Microsoft \Windows \CurrentVersion \Internet Settings \Zones \4 \	yes	no	no
HKEY_CLASSES_ROOT \.gmmp \	yes	no	no
HKEY_CLASSES_ROOT \.evt \	yes	no	no
HKEY_CLASSES_ROOT \.H1S \	yes	no	no
HKEY_CURRENT_USER \Software \Microsoft \Windows \CurrentVersion \Explorer \FileExts \	yes	no	no

0.8 Network Activity

This section outlines the network connections cuckoo observed during sample execution. These include tcp and udp connections, dns queries, dns servers, and websites visited. These should be investigated on a case-by-case basis.

This is a list of IP addresses which a process tried to connect that cuckoo determined was 'dead'. This means it is either no longer valid, or could not be reached. Having entries here is very often an inidicator of malware.

10.10.10.101
10.10.10.17
70.184.125.132
46.4.100.178
174.110.151.45
24.119.116.230
74.195.13.150
12.182.146.226
197.249.165.27
104.220.152.118
23.239.2.11

These are the IPs of DNS servers that were used for making DNS queries. These are not suspicious outright, but should still be noted.

10.10.10.17

This section is a list of domains Cuckoo observed connections being made to. These likely need to be investigated, but do so carefully as they may be malicous.

clients2.google.com
teredo.ipv6.microsoft.com
www.msftncsi.com

The following IPs made UDP connections with the Cuckoo VM. They are not suspicious outright, but should be used as a point of further investigation.

10.10.10.17
10.10.10.255
224.0.0.252
239.255.255.250

The following IPs made TCP connections with the Cuckoo VM. They are not suspicious outright, but should be used as a point of further investigation.