

Emulated On: Microsoft Windows 7 32 bit, Office 2013, Adobe Acrobat Reader 11.0, Adobe Flash Player 12, Java SE 1.7.0

1



Product Enquiry.doc

Malicious Activity Detected

Type doc

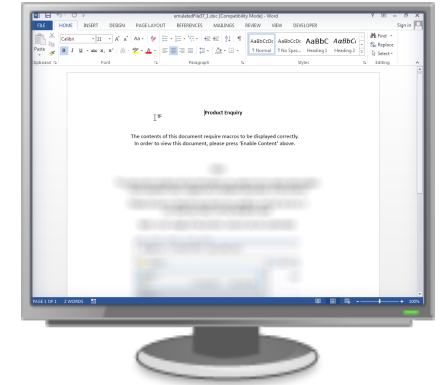
Resource http://62.90.226.156/files/CPU_London/Product...

File Size **164.0 KB**

MD5 **80ddd71913d2373867ee34ecb8e8fff8**

SHA1 **efce8803314438677ac5d83dcaafea9dee30a493**

[Download malicious file](#)



Emulation Screenshot



3 Suspicious Activities

Attempted Communication to <https://themexonline.me/timack/RT456475888y8y..>

CPU-Level Detection Event: Process Loaded Unknown Module

Malware activity observed (HEUR:Trojan-Downloader.Script.Generic)



1 Affected Processes

1 Process Created | 1 Process Terminated | 0 Processes Crashed

C:\Users\admin\AppData\Local\Temp\PRVQG.exe



0 Affected Registry Keys

0 Entries Set | 0 Entries Deleted

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Opt..

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Opt..

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Opt..

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Opt..

[more](#)



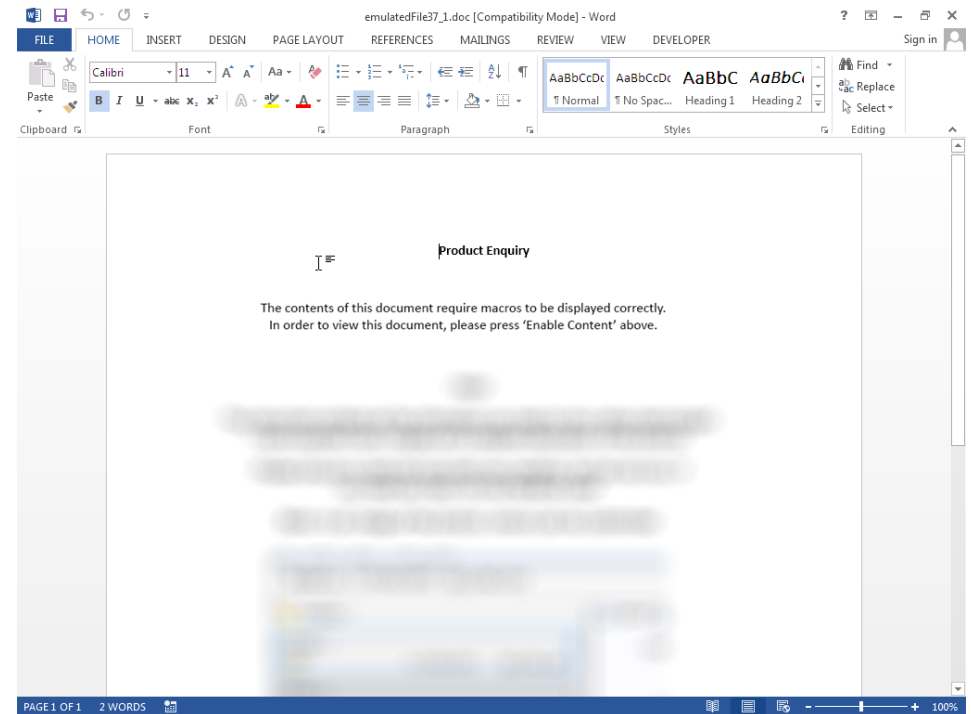
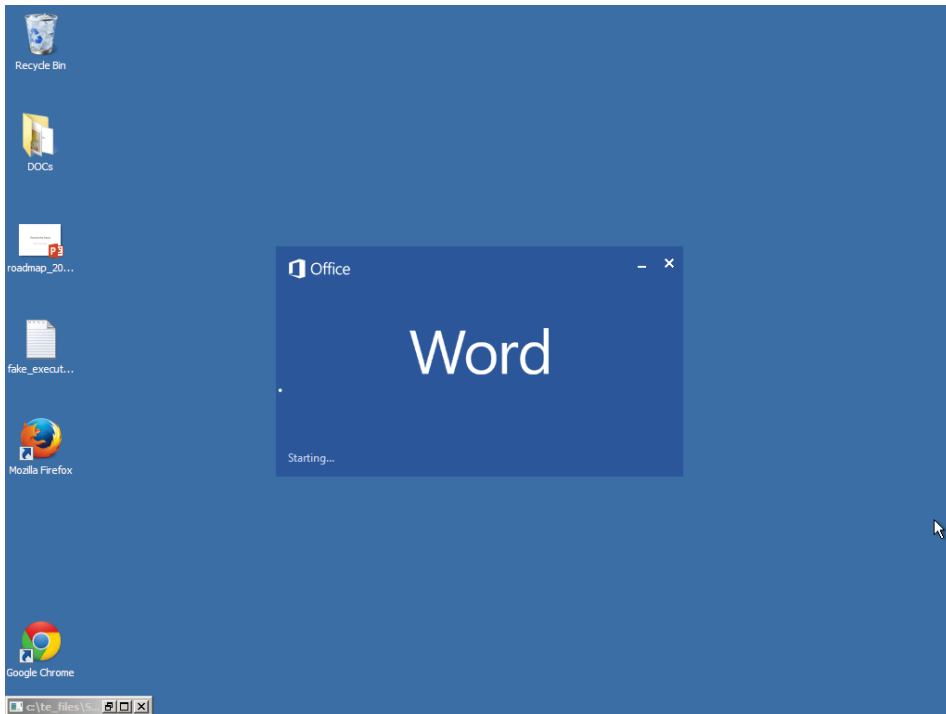
2 Affected Files

1 File Created | 1 File Modified | 0 Files Deleted

C:\Users\admin\Desktop\fake_executable_execute_flag_file.txt

C:\Windows\System32

Emulation Screen Shots



Emulation Screen Shots

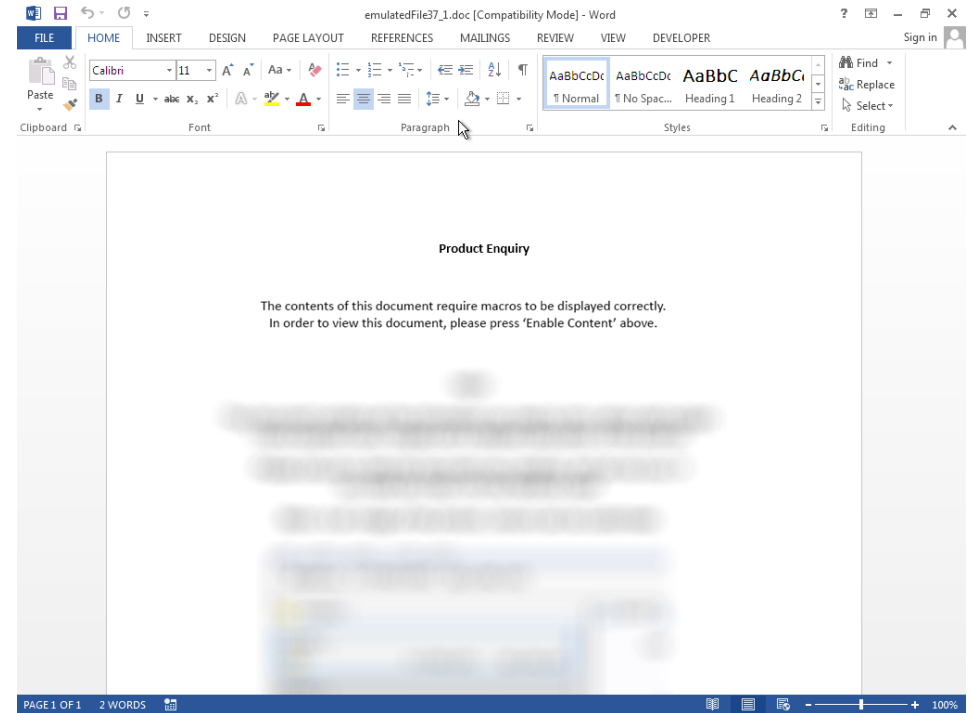
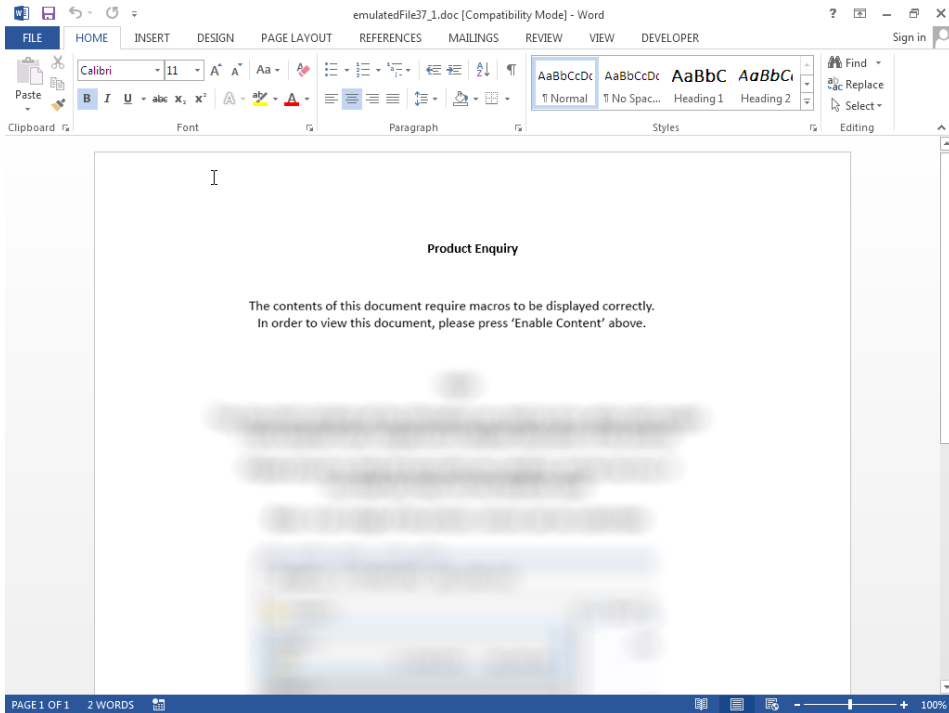


Table of Contents

4

[Malware Residues](#)

[5-6](#)

[Unexpected Activities By Time](#)

[7](#)

Malware Residues (1 out of 2)

5

Suspicious Activities

Attempted Communication to <https://themexoneonline.me/timack/RT456475888y8y98yhvh657467hvkfFYUFKHMVVHVCHCVMVCE7ti7t4irgsejgxdgdhdf1E448F.exe>

CPU-Level Detection Event: Process Loaded Unknown Module

Malware activity observed (HEUR:Trojan-Downloader.Script.Generic)

Processes Spawned or Interacted with

C:\Users\admin\AppData\Local\Temp\PRVQG.exe (Terminated ,Started)

Files Changed

C:\Users\admin\Desktop\fake_executable_execute_flag_file.txt (Created ,Modified)

C:\Windows\System32

Registry Keys Modified

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\KERNELBASE.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\UseFilter

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\kernel32.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\msvcrt.dll

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DIINXOptions\ntdll.dll

Malware Residues (2 out of 2)

6

Registry Keys Modified

HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers

HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled

HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions

HKLM\SYSTEM\ControlSet001\Control\Session Manager

HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode

HKLM\SYSTEM\ControlSet001\Control\hivelist

HKLM\SYSTEM\ControlSet001\Control\hivelist\Registry\User\S-1-5-21-292738990-2461527479-3432112557-1000_Classes

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers

Unexpected Activities By Time

7

Elapsed Time	Type	Action
00:00:10	HTTP Request	GET Request for https://themexoneonline.me/timack/RT456475888y8y98yhvh657467hvkfFYUFKHMVVHVCHCVVMVCE7ti7t4irgsejgxrddhdtf1E448F.exe
00:00:10	Process Creation	C:\Program Files\Microsoft Office\Office15\WINWORD.EXE Created C:\Users\admin\AppData\Local\Temp\PRVQG.exe
00:00:12	Process Termination	C:\Program Files\Microsoft Office\Office15\WINWORD.EXE Terminated C:\Users\admin\AppData\Local\Temp\PRVQG.exe
00:00:12	File Create	C:\Users\admin\AppData\Local\Temp\PRVQG.exe Created C:\Users\admin\Desktop\fake_executable_execute_flag_file.txt
00:00:12	File Write	C:\Users\admin\AppData\Local\Temp\PRVQG.exe Wrote To C:\Users\admin\Desktop\fake_executable_execute_flag_file.txt
00:00:23	Suspicious Activity	CPU-Level Detection Event: Process Loaded Unknown Module
	Suspicious Activity	Malware activity observed (HEUR:Trojan-Downloader.Script.Generic)

