


Emulated On: Microsoft Windows 7 64 bit, Office 2013, Adobe Acrobat Reader 11.0

1

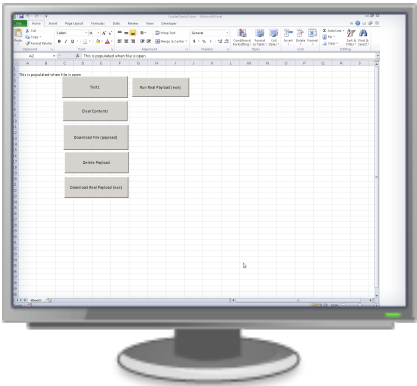


LoaderDemo5.xlsm

 Malicious Activity Detected

Type	 xlsm
File Size	34.5 KB
MD5	b579f62623183ba14592e6021e860284
SHA1	b00c9b2944dc5504e146a0a456e5238a080969a7

[Download malicious file](#)



Emulation Screenshot



55 Suspicious Activities

Attempted Communication to [http://demo.ryanrasmuss.com/download/payload....](http://demo.ryanrasmuss.com/download/payload...)
A command shell or script process was created by an unexpected parent process
Allocates read-write-execute memory (usually to unpack itself)
Captures pdf and office files which drops a file and executes it.

[more](#)



0 Affected Registry Keys

0 Entries Set

0 Entries Deleted



1 Affected Processes

1 Process Created | 0 Processes Terminated | 0 Processes Crashed

C:\Windows\SysWOW64\cmd.exe



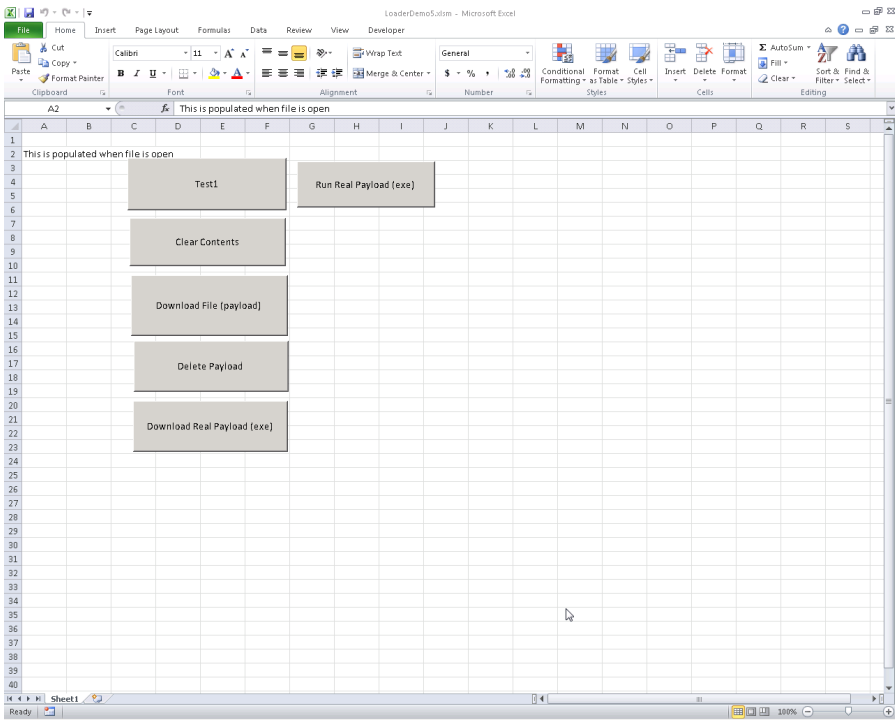
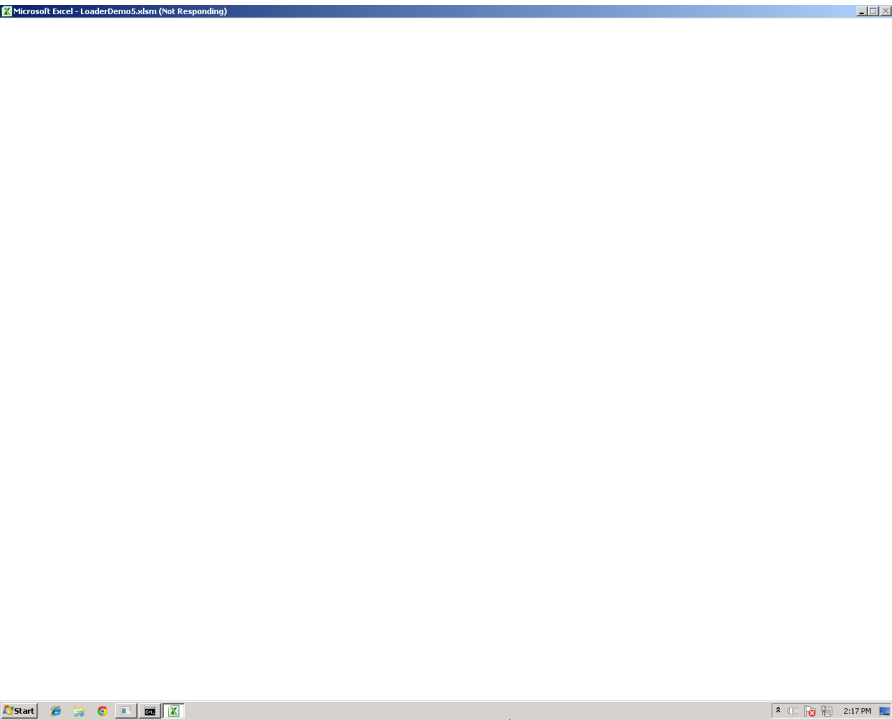
1 Affected Files

1 File Created | 1 File Modified | 0 Files Deleted

C:\Users\Administrator\Desktop\payload.bat

Emulation Screen Shots

2



Emulation Screen Shots

3

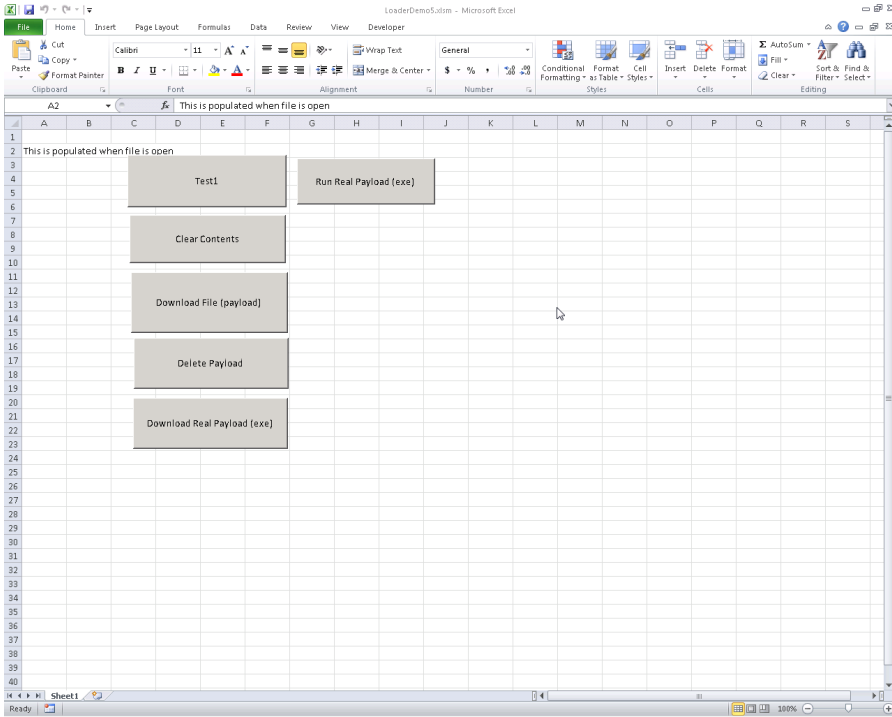
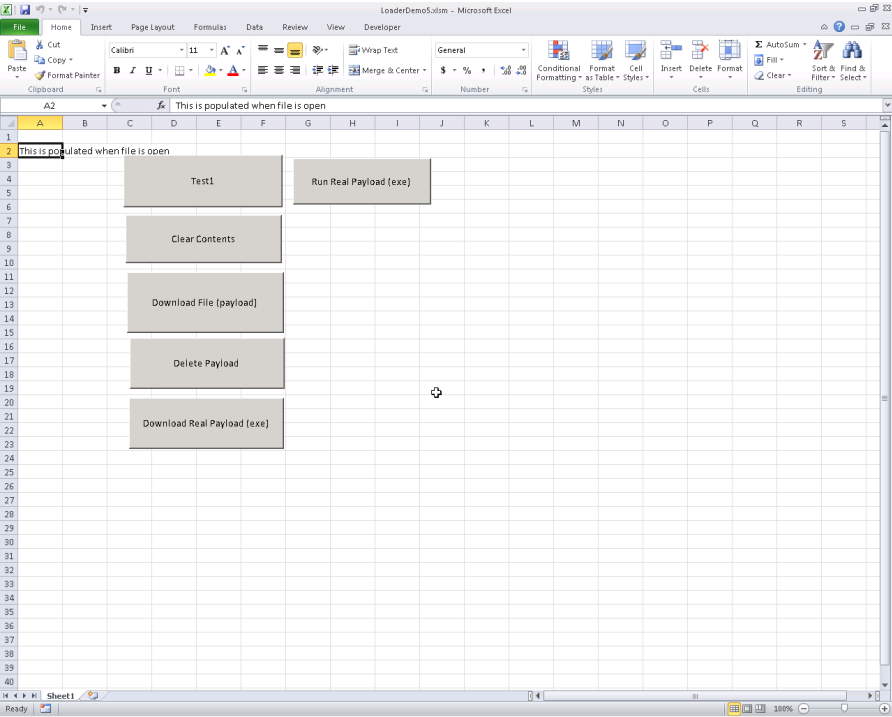


	Table of Contents	4
Malware Residues		5-10
Unexpected Activities By Time		11-17

Malware Residues (1 out of 6)

5

Suspicious Activities

Attempted Communication to <http://demo.ryanrasmuss.com/download/payload.bat>

A command shell or script process was created by an unexpected parent process

Allocates read-write-execute memory (usually to unpack itself)

Captures pdf and office files which drops a file and executes it.

Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available

Checks if process is being debugged by a debugger

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Command line console output was observed

Creates (office) documents on the filesystem

Creates a shortcut to an executable file

Creates a suspicious process

Creates executable files on the filesystem

Creates hidden or system file

Executes embedded malicious script

Generic detection methods (common)

Malicious VBA macros (Shell)

Network communications indicative of a potential document or script payload download was initiated by the process excel.exe

Observe a program that accesses a registry key related to network settings

Observe a program that accesses the CTF registry subkey

Malware Residues (2 out of 6)

6

Suspicious Activities

Observe a program that accesses the Internet Settings registry key

Observe a program that accesses the WinSock registry keys

Observe a program that accesses the WinSock2 parameters registry key

Observe a program that accesses the system services registry subkey

Malware Residues (3 out of 6)

7

Suspicious Activities

- Observe a program that creates registry keys
- Observe a program that disables system error message boxes
- Observe a program that launches the Windows command prompt
- Observe a program that opens its own process
- Observe a program that opens the ControlSet001 subkey
- Observes a program that creates threads in a suspended state
- Observes a program that installs a mouse hook

Malware Residues (4 out of 6)

8

Suspicious Activities

One or more martian processes was created

Resumed a suspended thread in a remote process potentially indicative of process injection

The program accesses a system related registry key

The program attempts to directly detect debuggers

The program changes file attributes

Malware Residues (5 out of 6)

Suspicious Activities

The program directly communicates with system drivers

The program dynamically calls imported functions

The program executes other programs or commands

The program installs a hook to spy on the user

The program installs a potentially dangerous Windows hook

The program loads NTDLL

The program queries a process cookie

The program queries information on its own process

The program queries its own PEB

Malware Residues (6 out of 6)

10

Suspicious Activities

The program sets files as hidden files

The program uses a native API call to load a DLL

Tried to identify the machine name.

Tried to read information about supported languages

Tries to unhook Windows functions monitored by Cuckoo

Uses Windows APIs to generate a cryptographic key

Malware signature matched (Malicious Binary.TC.mnmvbx)

Processes Spawned or Interacted with

C:\Windows\SysWOW64\cmd.exe (Started)

Files Changed

C:\Users\Administrator\Desktop\payload.bat (Created ,Modified)

Unexpected Activities By Time (1 out of 7)

11

Elapsed Time	Type	Action
00:00:24	HTTP Request	GET Request for http://demo.ryanrasmuss.com/download/payload.bat
00:00:24	Process Creation	C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE Created C:\Windows\SysWOW64\cmd.exe
00:00:27	File Create	C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE Created C:\Users\Administrator\Desktop\payload.bat
00:00:27	File Write	C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE Wrote To C:\Users\Administrator\Desktop\payload.bat
00:02:23	Suspicious Activity	Captures pdf and office files which drops a file and executes it.
00:02:23	Suspicious Activity	A command shell or script process was created by an unexpected parent process
00:02:23	Suspicious Activity	Network communications indicative of a potential document or script payload download was initiated by the process excel.exe
00:02:23	Suspicious Activity	One or more martian processes was created
00:02:23	Suspicious Activity	Resumed a suspended thread in a remote process potentially indicative of process injection
00:02:23	Suspicious Activity	Tries to unhook Windows functions monitored by Cuckoo
00:02:23	Suspicious Activity	Executes embedded malicious script
00:02:23	Suspicious Activity	Malicious VBA macros (Shell)
00:02:23	Suspicious Activity	Tried to identifie the machine name.
00:02:23	Suspicious Activity	Tried to reads information about supported languages
00:02:23	Suspicious Activity	Observes a program that creates threads in a suspended state
00:02:23	Suspicious Activity	The program attempts to directly detect debuggers
00:02:23	Suspicious Activity	The program uses a native API call to load a DLL

Unexpected Activities By Time (2 out of 7)

12

Elapsed Time	Type	Action
00:02:23	Suspicious Activity	The program deliberately waits for a long period
00:02:23	Suspicious Activity	The program sets files as hidden files
00:02:23	Suspicious Activity	Observes a program that installs a mouse hook
00:02:23	Suspicious Activity	The program executes other programs or commands
00:02:23	Suspicious Activity	Generic detection methods (common)
00:02:23	Suspicious Activity	The program installs a hook to spy on the user
00:02:23	Suspicious Activity	Observe a program that accesses a registry key related to network settings

Unexpected Activities By Time (3 out of 7)

13

Elapsed Time	Type	Action
00:02:23	Suspicious Activity	The program installs a potentially dangerous Windows hook
00:02:23	Suspicious Activity	Allocates read-write-execute memory (usually to unpack itself)
00:02:23	Suspicious Activity	Creates (office) documents on the filesystem
00:02:23	Suspicious Activity	Creates executable files on the filesystem
00:02:23	Suspicious Activity	Creates hidden or system file
00:02:23	Suspicious Activity	Creates a shortcut to an executable file
00:02:23	Suspicious Activity	Creates a suspicious process
00:02:23	Suspicious Activity	Observe a program that creates registry keys

Unexpected Activities By Time (4 out of 7)

14

Elapsed Time	Type	Action
00:02:23	Suspicious Activity	The program queries its own PEB
00:02:23	Suspicious Activity	The program dynamically calls imported functions
00:02:23	Suspicious Activity	The program loads NTDLL
00:02:23	Suspicious Activity	Observe a program that accesses the WinSock registry keys
00:02:23	Suspicious Activity	The program directly communicates with system drivers
00:02:23	Suspicious Activity	Observe a program that opens its own process
00:02:23	Suspicious Activity	The program queries a process cookie
00:02:23	Suspicious Activity	The program queries the execute flags for a process
00:02:23	Suspicious Activity	The program queries information on its own process

Unexpected Activities By Time (5 out of 7)

15

Elapsed Time	Type	Action
00:02:23	Suspicious Activity	Observe a program that accesses the WinSock2 parameters registry key
00:02:23	Suspicious Activity	Observe a program that opens the ControlSet001 subkey
00:02:23	Suspicious Activity	Observe a program that accesses the CTF registry subkey
00:02:23	Suspicious Activity	Observe a program that disables system error message boxes
00:02:23	Suspicious Activity	The program accesses a system related registry key
00:02:23	Suspicious Activity	The program changes file attributes
00:02:23	Suspicious Activity	Checks if process is being debugged by a debugger
00:02:23	Suspicious Activity	Command line console output was observed

Unexpected Activities By Time (6 out of 7)

16

Elapsed Time	Type	Action
00:02:23	Suspicious Activity	Uses Windows APIs to generate a cryptographic key
00:02:23	Suspicious Activity	Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)
00:02:23	Suspicious Activity	Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
00:02:23	Suspicious Activity	Observe a program that creates a new process
00:02:23	Suspicious Activity	Observe a program that accesses the Internet Settings registry key
00:02:23	Suspicious Activity	Observes a program that registers to auto-run on system startup
00:02:23	Suspicious Activity	Observe a program that accesses the system services registry subkey

Unexpected Activities By Time (7 out of 7)

Elapsed Time	Type	Action
00:02:23	Suspicious Activity	Observe a program that launches the Windows command prompt
	Suspicious Activity	Malware signature matched (Malicious Binary.TC.mnmvbx)

