File Name: doklad_23_03_2015_P147B7E1H.exe
MD5 Hash Identifier: 6AA3EEAB780CFD8D8BF7CC4C015F8EEB
SHA-1 Hash Identifier: 9EFA278D8118B92A4BCE7235A4CA2ACB0CA1C063
File Size: 46592
File Type: PE32 executable (GUI) Intel 80386, for MS Windows

Platform Version: 3.4.2.32.43041

Down Selector's Analysis:

Engine	GTI File Reputation	Gateway Anti-Malware	Anti-Malware	Custom Yara	Sandbox	Final
Threat Name	---	---	---	---	Malware.Dynamic	
Severity	None	N/A	N/A	None	3	4

Sample is malicious: final severity level 4

Analysis Environment:

- **Microsoft Windows 7 Professional Service Pack 1 (build 7601), 64-bit**
- **Internet Explorer version: 8**
- **Microsoft Office version: 2003**
- **PDF Reader version: 9.0**

File Submitted on: 2015-02-25 10:45:50

Time Taken: 299 seconds

Digital Signature Verified:	unsigned
Publisher:	Not Available
Description:	Not Available
Product Name:	Not Available
Version Info:	Not Available
File version:	Not Available
Strong Name:	Not Available
Original Name:	Not Available
Internal Name:	Not Available
Copyright:	Not Available
Comments:	Not Available

Processes analyzed in this sample:

NAME	*REASON*	*LEVEL*
doklad_23_03_2015_P147B7E1H.exe	loaded by MATD Analyzer	
law.exe	executed by doklad_23_03_2015_P147B7E1H.exe	

Embedded/Dropped content:

MD5	*NAME*
22a4460df6ccc449053324a738f11916	law.exe
53a4a7df2a283d008acceaa358aded80	wujuwy.gif

5d1de1329d254c43d037e013b8fc4929	nnchng.LNK
61624028e9ae32df5e8322f148f58eff	~$nnchng.rtf
682f45112279c69b823061ee8286c8a2	Temp.LNK
fca11178b89b376970a63dafcdc482a7	nnchng.rtf

The attachment file(s) shown above was extracted from the sample file and stored in the dropfiles.zip file

Classification / Threat Score:

Persistence, Installation Boot Survival:	
Hiding, Camouflage, Stealthiness, Detection and Removal Protection:	
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection:	
Spreading:	
Exploiting, Shellcode:	
Networking:	
Data spying, Sniffing, Keylogging, Ebanking Fraud:	

Legend: Sev.0- Sev.1- Sev.2- Sev.3- Sev.4- Sev.5-

Dynamic Analysis:

	Behaved as creating and executing the rtf file from the temp directory		Modified time attribute of the specified file after its creation
	Modified file's time creation attributes		Ran newly created executable file
	Created named mutex object		Contained long sleep
	Executed active content by Windows shell application		Changed the protection attribute of the process

doklad_23_03_2015_P147B7E1H.exe return to top

RUN-TIME DLLS

api-ms-win-core-localregistry-l1-1-0.dll
cabinet.dll
devrtl.dll

FILE OPERATIONS

Files Created

FILE NAME	ACCESS MODE	FILE ATTRIBUTES	MD5
C:\Users\ADMINI~1\AppData\Local\Temp\wujuwy.gif	Write	Normal	
C:\Users\ADMINI~1\AppData\Local\Temp\nnchng.rtf	Read & Write	Normal	
C:\Users\ADMINI~1\AppData\Local\Temp\law.exe	Write	Normal	

Files Opened

FILE NAME	ACCESS MODE	FILE ATTRIBUTES	MD5
C:\Users\ADMINI~1\AppData\Local\Temp\wujuwy.gif	Read	Normal	

Files Deleted

C:\Users\ADMINI~1\AppData\Local\Temp\law.exe

Files Modified

SOURCE FILE	DESTINATION FILE/WRITE	WRITTEN
C:\Users\ADMINI~1\AppData\Local\Temp\wujuwy.gif	1253	1253
C:\Users\ADMINI~1\AppData\Local\Temp\nnchng.rtf	6954	6954
C:\Users\ADMINI~1\AppData\Local\Temp\law.exe	205312	205312

Files Read
C:\Users\ADMINI~1\AppData\Local\Temp\wujuwy.gif
C:\Windows\INF\setupapi.dev.log

Other
Retrieved the full path for the module
Obtained the path of the Windows system directory
Retrieved the path of the directory designated for temporary files
Obtained the short path form of a path
Obtained a set of FAT file system attributes for a file or directory
Set the date and time of a file or directory

REGISTRY OPERATIONS

Registry Read	
C:\Users\ADMINI~1\AppData\Local\Temp\wujuwy.gif	SystemSetupInProgress

PROCESS OPERATIONS

Process Opened	
PROCESS NAME/ADDRESS	*PID/PROCESS NAME*
	C:\USERS\ADMINI~1\APPDATA\LOCAL\TEMP\NNCHNG.RTF
	C:\USERS\ADMINI~1\APPDATA\LOCAL\TEMP\LAW.EXE

Process killed
Ended itself and all of its threads

Other
Changed the protection attribute of process address: 0x400000, new attribute: ReadWrite
Changed the protection attribute of process address: 0x400000, new attribute: ReadOnly
Changed the protection attribute of process address: 0x401000, new attribute: ReadWrite
Changed the protection attribute of process address: 0x401000, new attribute: Execute_ReadWrite
Changed the protection attribute of process address: 0x403000, new attribute: ReadWrite
Changed the protection attribute of process address: 0x403000, new attribute: ReadOnly
Changed the protection attribute of process address: 0x401054, new attribute: ReadWrite
Changed the protection attribute of process address: 0x401054, new attribute: Execute_ReadWrite

OTHER OPERATIONS

Signal Objects
MUTEX-OBJECT NAME
Created/opened an event object
mcvioesa

Others
Expanded environment-variable strings and replace them with the values defined for the current use
Generate a pseudo-random number

law.exe return to top

FILE OPERATIONS

Files Read
list

Memory Mapped Files
Created a file that can be used for memory mapping

Other
Retrieved the full path for the module
Searched a directory for the name: list

PROCESS OPERATIONS

Thread Created
25ca404

Other
Enabled an application to supersede the top-level exception handler
Searched for a top-level window with string: class
Searched for a top-level window with string: note
Changed the protection attribute of process address: 0x400000, new attribute: Execute_ReadWrite
Changed the protection attribute of process address: 0x401000, new attribute: Execute_ReadWrite
Changed the protection attribute of process address: 0x402000, new attribute: Execute_ReadWrite
Changed the protection attribute of process address: 0x403000, new attribute: Execute_ReadWrite
Changed the protection attribute of process address: 0x404000, new attribute: Execute_ReadWrite
Changed the protection attribute of process address: 0x400000, new attribute: ReadOnly

OTHER OPERATIONS

Others
Obtained the current system date and time in in Coordinated Universal Time (UTC) format

GTI URL Reputation return to top

CONNECTED SITES

SEVERITY	REPUTATION	CATEGORY NAME	RISK GROUP	FUNCTIONAL GROUP	PORT	URL
	Minimal	---	---	---	53	78.46.34.27

Network Simulator return to top

NETWORK ACTIVITY

TIME OFFSET	ACTIVITY
0.000	DNS QUERY: EXCLUSIVENUTRIENTS.COM. : IP=78.46.34.27
2.358	OUTGOING TCP CONNECTION TO IP: 78.46.34.27 PORT: 80 (HTTP)

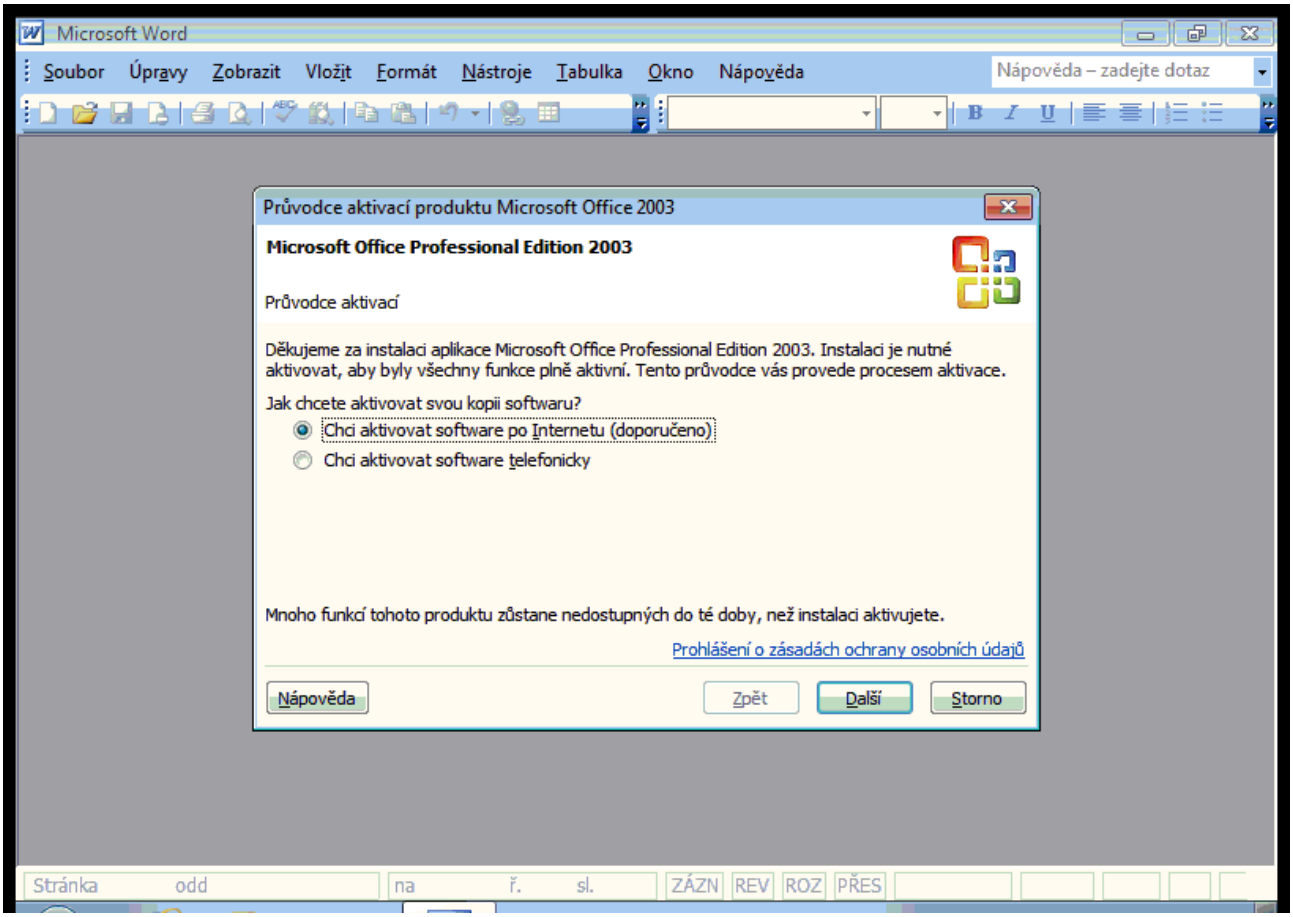
Screenshots:

Note: a pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample

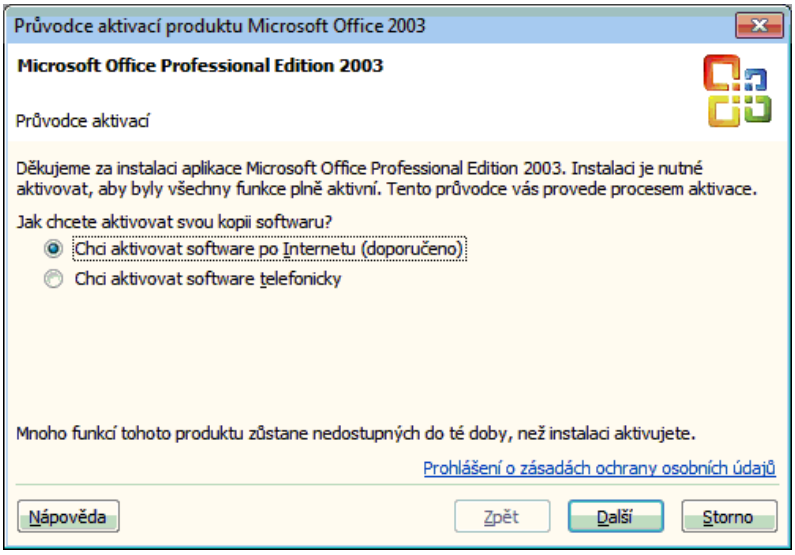
doklad_23_03_2015_P147B7E1H.exe return to top

SCREENSHOTS

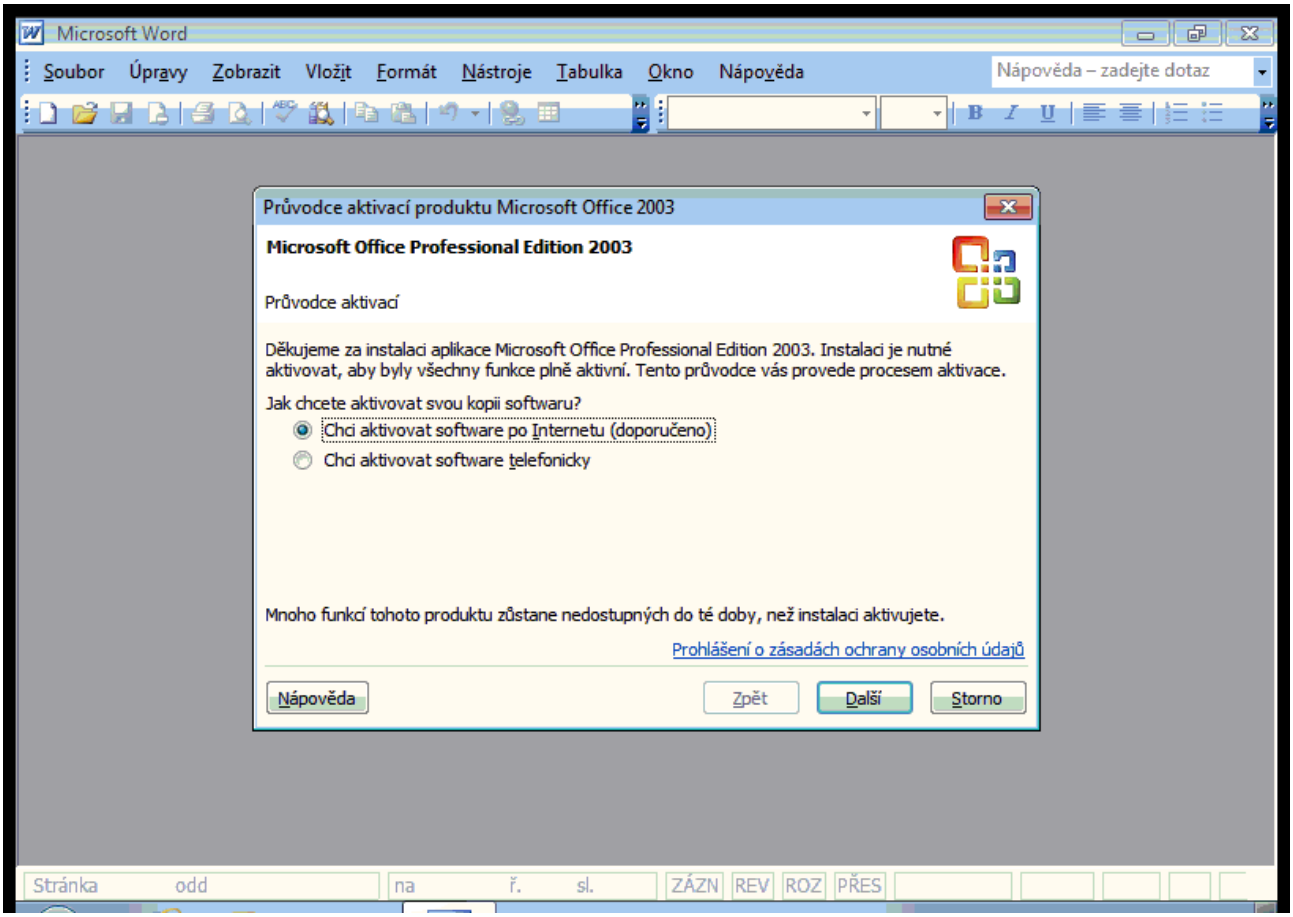
34C2F1.JPG



34951E.JPG



323053.JPG



353D4E.JPG