ID: 344024
Sample Name: COVID-19 Vaccine Provider Questionaire Health First CHC-Providence.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:36:03
Date: 25/01/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2

Analysis Report COVID-19 Vaccine Provider Questionaire Health First CHC-Providence.xlsx 3

- Overview 3
  - General Information 3
  - Detection 3
  - Signatures 3
  - Classification 3
- Startup 3
- Malware Configuration 3
- Yara Overview 3
- Sigma Overview 3
- Signature Overview 3
  - Compliance: 4
- Mitre Att&ck Matrix 4
- Behavior Graph 4
- Screenshots 5
  - Thumbnails 5
- Antivirus, Machine Learning and Genetic Malware Detection 6
  - Initial Sample 6
  - Dropped Files 6
  - Unpacked PE Files 6
  - Domains 6
  - URLs 6
- Domains and IPs 6
  - Contacted Domains 7
  - Contacted IPs 7
- General Information 7
- Simulations 7
  - Behavior and APIs 7
- Joe Sandbox View / Context 8
  - IPs 8
  - Domains 8
  - ASN 8
  - JA3 Fingerprints 8
  - Dropped Files 8
- Created / dropped Files 8
- Static File Info 8
  - General 8
  - File Icon 9
- Network Behavior 9
- Code Manipulations 9
- Statistics 9
- System Behavior 9
  - Analysis Process: EXCEL.EXE PID: 2512 Parent PID: 584 9
    - General 9
    - File Activities 9
      - File Written 9
    - Registry Activities 10
      - Key Created 10
      - Key Value Created 10
- Disassembly 10

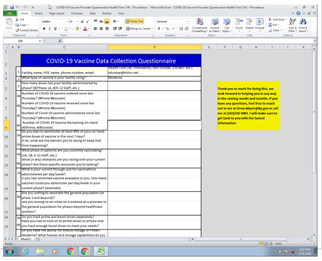
Analysis Report COVID-19 Vaccine Provider Questionair…

Overview

General Information

Sample Name:	COVID-19 Vaccine Provider Questionaire Health First CHC-Providence.xlsx
Analysis ID:	344024
MD5:	da088a6ac0526f5.
SHA1:	ed00c3d987c76c…
SHA256:	2d7a5d5f2e43508.

Most interesting Screenshot:



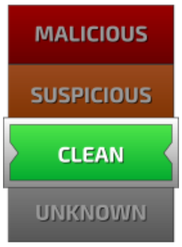
COVID-19 Vaccine Provider Questionaire Health First CHC- Providence - Microsoft Excel - COVID-19 Vaccine Provider Questionaire Health First CHC- Providence

COVID-19 Vaccine Data Collection Questionnaire

1	Facility name, POC name, phone number, email	Health First CHC-Providence, Keri Dunbar, 270-667-7017, kdunbar@hfchc.net
2	What type of vaccine is your facility using?	Moderna
3	How many doses has your facility administered by phase? (#/Phase 1A, #/K-12 Staff, etc.)	
4a	Number of COVID-19 vaccine ordered since last Thursday? (#Prime #Booster)	
4b	Number of COVID-19 vaccine received since last Thursday? (#Prime #Booster)	
4c	Number of Covid-19 vaccine administered since last Thursday? (#Prime #Booster)	
4d	Number of COVID-19 Vaccine Remaining On-Hand (#/Prime, #/Booster)	
5a	Do you plan to administer at least 90% of your on-hand prime doses of vaccine in the next 7 days?	
5b	If no, what are the barriers you're facing to keep that from happening?	
6a	What phase of patients are you currently vaccinating? (1A, 1B, K-12 staff, etc.)	
6b	What (if any) obstacles are you facing with your current phase? Are there specific resources you're lacking?	
7a	What is your current through-put for vaccinations administered per day/week?	
7b	If you had unlimited vaccine available to you, how many vaccines could you administer per day/week in your current phase? (estimate)	
8a	Are you willing to vaccinate the general population (ie phase 2 and beyond)?	
8b	Are you willing to be listed on a website as a provider to the general population for phases beyond healthcare workers?	
9a	Do you track prime and boost doses seperately?	
9b	Have you had to hold on to prime doses to ensure that you have enough boost doses to meet your needs?	
	Do you have the ability for mobile storage of Pfizer? Moderna? What freezer and storage capabilities do you	

Thank you so much for doing this, we look forward to helping you in any way in the coming weeks and months. If you have any questions, feel free to reach out to me at Drew.Myers@ky.gov or call me at (502)310-9083. I will make sure to get back to you with the lastest information.

Detection

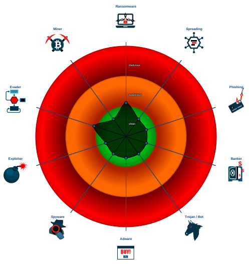


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2512 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● Compliance
● System Summary
● Hooking and other Techniques for Hiding and Protection

Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

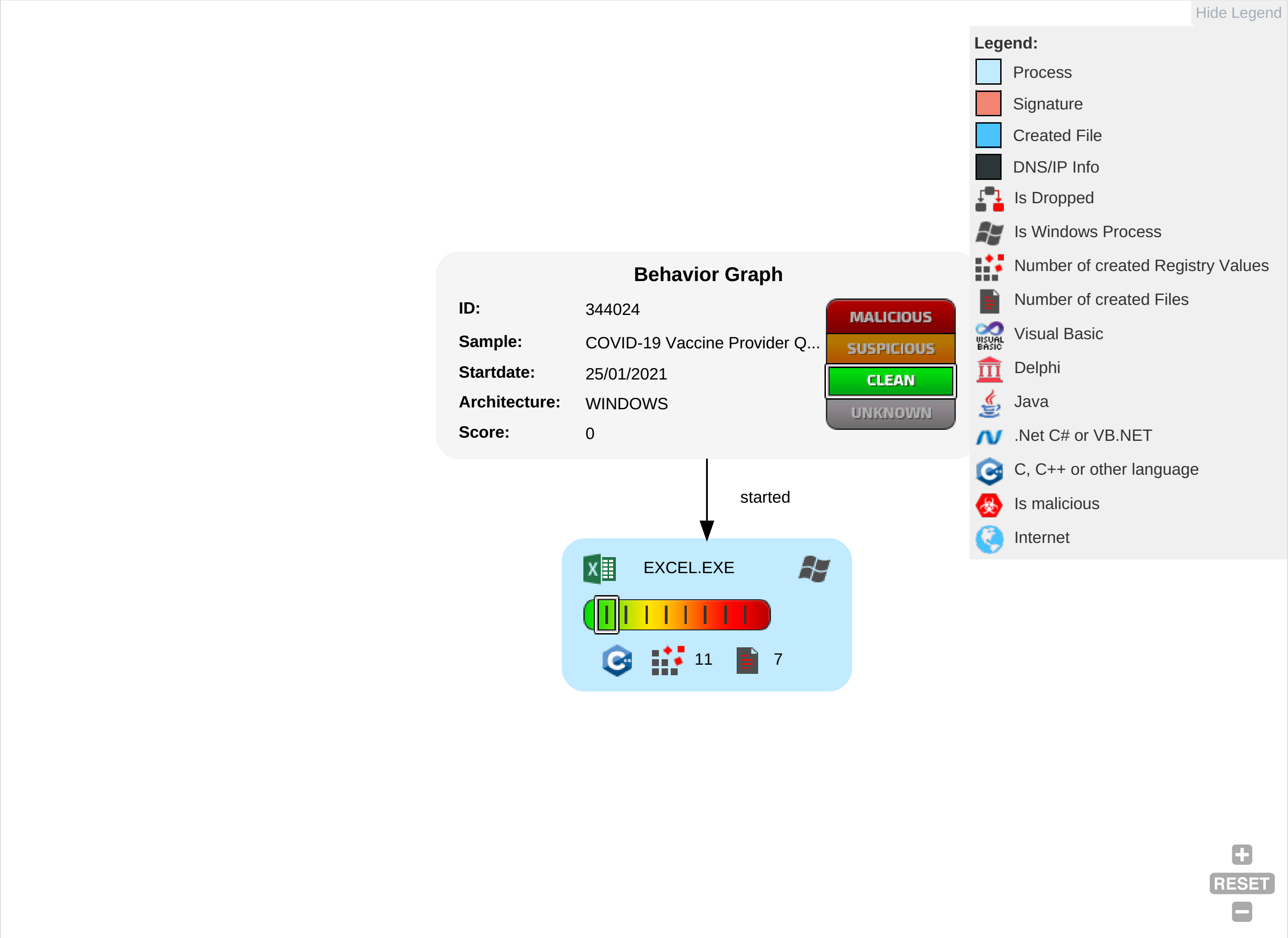
Compliance:

Uses new MSVCR Dlls

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Behavior Graph



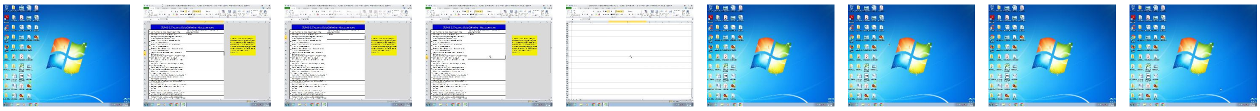
Behavior Graph

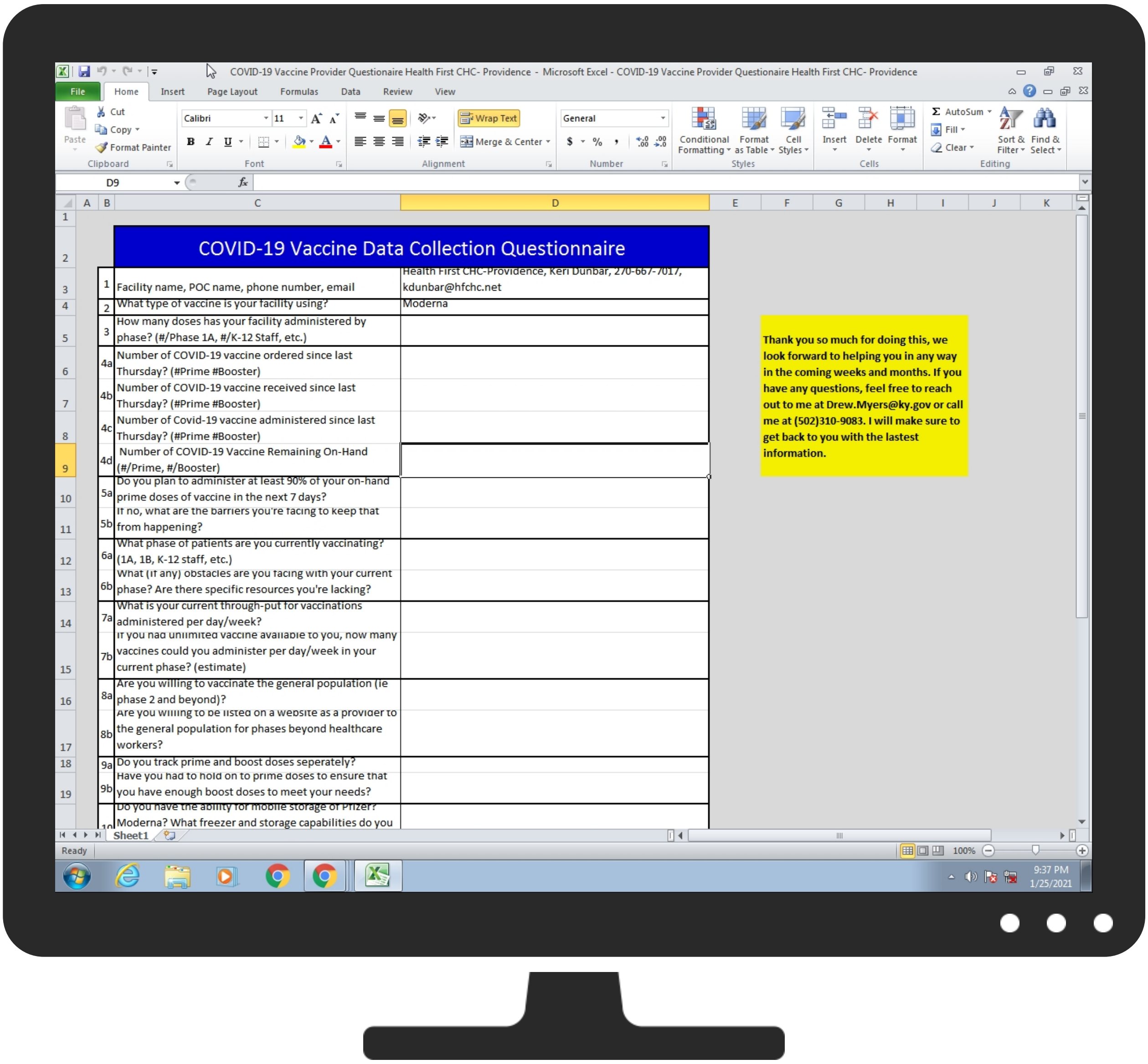
ID:	344024
Sample:	COVID-19 Vaccine Provider Q...
Startdate:	25/01/2021
Architecture:	WINDOWS
Score:	0

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





COVID-19 Vaccine Provider Questionaire Health First CHC- Providence - Microsoft Excel - COVID-19 Vaccine Provider Questionaire Health First CHC- Providence

COVID-19 Vaccine Data Collection Questionnaire

1	Facility name, POC name, phone number, email	Health First CHC-Providence, Keri Dunbar, 270-667-7017, kdunbar@hfchc.net
2	What type of vaccine is your facility using?	Moderna
3	How many doses has your facility administered by phase? (#/Phase 1A, #/K-12 Staff, etc.)	
4a	Number of COVID-19 vaccine ordered since last Thursday? (#Prime #Booster)	
4b	Number of COVID-19 vaccine received since last Thursday? (#Prime #Booster)	
4c	Number of Covid-19 vaccine administered since last Thursday? (#Prime #Booster)	
4d	Number of COVID-19 Vaccine Remaining On-Hand (#/Prime, #/Booster)	
5a	Do you plan to administer at least 90% of your on-hand prime doses of vaccine in the next 7 days?	
5b	If no, what are the barriers you're facing to keep that from happening?	
6a	What phase of patients are you currently vaccinating? (1A, 1B, K-12 staff, etc.)	
6b	What (if any) obstacles are you facing with your current phase? Are there specific resources you're lacking?	
7a	What is your current through-put for vaccinations administered per day/week?	
7b	If you had unlimited vaccine available to you, how many vaccines could you administer per day/week in your current phase? (estimate)	
8a	Are you willing to vaccinate the general population (ie phase 2 and beyond)?	
8b	Are you willing to be listed on a website as a provider to the general population for phases beyond healthcare workers?	
9a	Do you track prime and boost doses seperately?	
9b	Have you had to hold on to prime doses to ensure that you have enough boost doses to meet your needs?	
10	Do you have the ability for mobile storage of Pfizer? Moderna? What freezer and storage capabilities do you	

Thank you so much for doing this, we look forward to helping you in any way in the coming weeks and months. If you have any questions, feel free to reach out to me at Drew.Myers@ky.gov or call me at (502)310-9083. I will make sure to get back to you with the lastest information.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344024
Start date:	25.01.2021
Start time:	21:36:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID-19 Vaccine Provider Questionaire Health First CHC- Providence.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	2
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winXLSX@1/1@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/344024/sample/COVID-19 Vaccine Provider Questionaire Health First CHC- Providence.xlsx

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\Desktop\~$COVID-19 Vaccine Provider Questionaire Health First CHC- Providence.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . .

Static File Info

General	
File type:	Microsoft Excel 2007+
Entropy (8bit):	7.241265507017585
TrID:	• Excel Microsoft Office Open XML Format document (40004/1) 83.33% • ZIP compressed archive (8000/1) 16.67%
File name:	COVID-19 Vaccine Provider Questionaire Health First CHC- Providence.xlsx
File size:	14085
MD5:	da088a6ac0526f528932271fc37d58ff
SHA1:	ed00c3d987c76ca406e42d915190250e528e99e1
SHA256:	2d7a5d5f2e435088ea7a90e399e6b40693bf04dd82aa17 572a7421f6f9f5dd7
SHA512:	3330f3f07826b89aa3c0bee2bba301d5417158e9bccb910 50b093e2a01836752f8ba1d98a53a706dfedeb1bdde99d 6c06a3d0034ae016a6e44abd90d7e7ffc6
SSDEEP:	384:KH3k5m0ubJPBc8fzjC4UiB+WCUP/MOova:Kq8f64 Us7PUW

General	
File Content Preview:	PK..........!.A7..n...........[Content_Types].xml ...(............... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXCEL.EXE PID: 2512 Parent PID: 584

General

Start time:	21:36:45
Start date:	25/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13feb0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$COVID-19 Vaccine Provider Questionaire Health First CHC- Providence.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	1400FF526	WriteFile
C:\Users\user\Desktop\~$COVID-19 Vaccine Provider Questionaire Health First CHC- Providence.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00	..A.l.b.u.s.	success or wait	1	1400FF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	s|6	binary	73 7C 36 00 D0 09 00 00 02 00 00 00 00 00 00 00 26 01 00 00 01 00 00 00 92 00 00 00 88 00 00 00 63 00 6F 00 76 00 69 00 64 00 2D 00 31 00 39 00 20 00 76 00 61 00 63 00 63 00 69 00 6E 00 65 00 20 00 70 00 72 00 6F 00 76 00 69 00 64 00 65 00 72 00 20 00 71 00 75 00 65 00 73 00 74 00 69 00 6F 00 6E 00 61 00 69 00 72 00 65 00 20 00 68 00 65 00 61 00 6C 00 74 00 68 00 20 00 66 00 69 00 72 00 73 00 74 00 20 00 63 00 68 00 63 00 2D 00 20 00 70 00 72 00 6F 00 76 00 69 00 64 00 65 00 6E 00 63 00 65 00 2E 00 78 00 6C 00 73 00 78 00 00 00 63 00 6F 00 76 00 69 00 64 00 2D 00 31 00 39 00 20 00 76 00 61 00 63 00 63 00 69 00 6E 00 65 00 20 00 70 00 72 00 6F 00 76 00 69 00 64 00 65 00 72 00 20 00 71 00 75 00 65 00 73 00 74 00 69 00 6F 00 6E 00 61 00 69 00 72 00 65 00 20 00 68 00 65 00 61 00 6C 00 74 00 68 00 20 00 66 00 69 00 72 00 73 00 74 00 20 00 63 00 68 00 63 00 2D 00 20 00 70 00 72 00 6F 00 76 00 69 00 64 00 65 00 6E 00 63 00 65 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly