ID: 1407717
Sample Name: a2e-enterprise.26.3.3677.2903.exe
Cookbook: default.jbs
Time: 18:06:47
Date: 12/03/2024
Version: 40.0.0 Tourmaline

Table of Contents

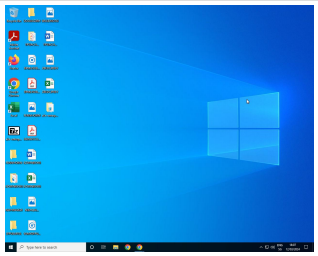
Windows Analysis Report

a2e-enterprise.26.3.3677.2903.exe

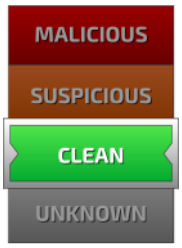
Overview

General Information

Sample name:	a2e-enterprise.26.3.3677.2903.exe
Analysis ID:	1407717
MD5:	29c3418978dd…
SHA1:	08283dd80f959..
SHA256:	22a18e758263…
Infos:	



Detection

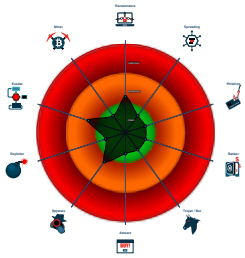


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	40%

Signatures

- Detected potential crypto function
- Drops PE files
- Found dropped PE file which has no…
- Found potential string decryption / a…
- Installs a raw input device (often for…
- PE file contains an invalid checksum
- Sample execution stops while proce…
- Sample file is different than original …
- Tries to load missing DLLs
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Sample has functionality to log and monitor keystrokes, analyze it with the 'Simulates keyboard and window changes' cookbook

Process Tree

- **System is w10x64**
- a2e-enterprise.26.3.3677.2903.exe (PID: 7316 cmdline: C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe MD5: 29C3418978DD57C42C7E9530B3AAC3D6)
  - conhost.exe (PID: 7324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

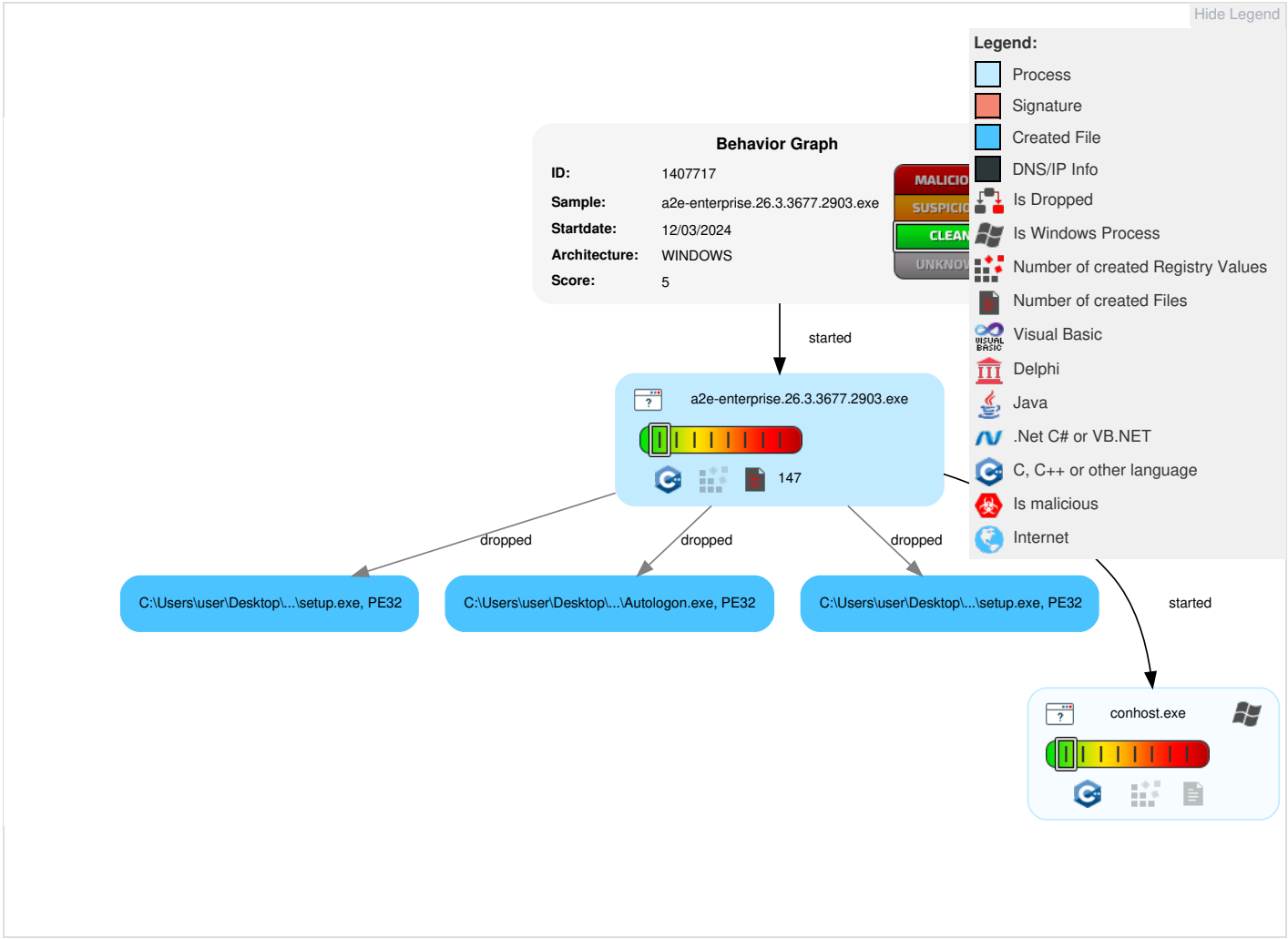
Joe Sandbox Signatures

There are no malicious signatures

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 Process Injection	1 Masquerading	1 1 Input Capture	1 Security Software Discovery	Remote Services	1 1 Input Capture	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Process Injection	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	1 Archive Collected Data	Junk Data	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	1 Deobfuscate/Decode Files or Information	Security Account Manager	2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Steganography	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	2 Obfuscated Files or Information	LSA Secrets	Internet Connection Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact

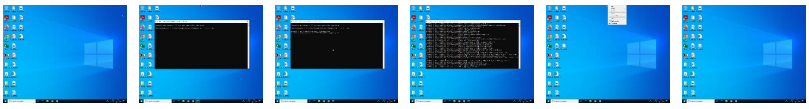
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\setup.exe	0%	ReversingLabs		
C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Autologon.exe	0%	ReversingLabs		
C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Setup Files\setup.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:13556/HosterIdentityHttpLogWriterEndpointInsiderSlabBehaviorProviderLabMachineLangT	0%	Avira URL Cloud	safe	
http://support.diditbetter.com/Secure/Login.aspx?returnurl=/downloads.aspx	0%	Avira URL Cloud	safe	
http://support.diditbetter.com/disable-group-policy.aspx	0%	Avira URL Cloud	safe	
http://www.DidITBetter.com/Solutions/Add2Exchange/Overview.aspARPHELPLINKAdvantage	0%	Avira URL Cloud	safe	
http://www.DidITbetter.com	0%	Avira URL Cloud	safe	
http://www.sysinternals.comopenThe	0%	Avira URL Cloud	safe	
http://https://support.DidItBetter.com/	0%	Avira URL Cloud	safe	
http://https://support.diditbetter.com/downloads.aspx	0%	Avira URL Cloud	safe	
http://support.diditbetter.com/support-request.aspx	0%	Avira URL Cloud	safe	
http://https://support.diditbetter.com/support-request.aspx	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://s3.amazonaws.com/dl.diditbetter.com	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, SQL12x_to_SQL12xSP4.ps1.0.dr, SQL12x_to_SQL22x.ps1.0.dr	false		high
http://https://s3.amazonaws.com/guides.diditbetter.com/Migrating_A2E_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://https://support.DidItBetter.com/	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false	• Avira URL Cloud: safe	unknown
http://support.diditbetter.com/disable-group-policy.aspx	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://s3.amazonaws.com/guides.diditbetter.com/Add2Exchange_Guide.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://https://s3.amazonaws.com/dl.diditbetter.com/	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp	false		high
http://support.diditbetter.com/Secure/Login.aspx?returnurl=/downloads.aspx	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://s3.amazonaws.com/dl.diditbetter.com/A2EDiags-2.3.exe	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://s3.amazonaws.com/guides.diditbetter.com/Private_to_Private_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://https://s3.amazonaws.com/guides.diditbetter.com/Private_to_Public_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://www.DidITbetter.com	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, Add2ExchangeEULA.rtf.0.dr, Add2ExchangeSetup.msi.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://s3.amazonaws.com/guides.diditbetter.com/Migrating_Environments_A2E_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://https://s3.amazonaws.com/guides.diditbetter.com/Template_Creation_RGM_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sysinternals.com	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1814391759.0000000002204000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://s3.amazonaws.com/guides.diditbetter.com/Public_to_Public_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://https://support.diditbetter.com/support-request.aspx	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/ssmsfullsetup	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://www.sysinternals.comopenThe	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1814391759.0000000002204000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://s3.amazonaws.com/guides.diditbetter.com/Public_to_Private_Sync_Scenarios.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://https://support.diditbetter.com/downloads.aspx	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:13556/HosterIdentityHttpLogWriterEndpointInsiderSlabBehaviorProviderLabMachineLangT	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1814391759.0000000002626000.00000004.00000020.00020000.00000000.sdmp, a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1814391759.0000000002204000.00000004.00000020.00020000.00000000.sdmp, setup.exe0.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.DidITBetter.com/Solutions/Add2Exchange/Overview.aspARPHELPLINKAdvantage	Add2ExchangeSetup.msi.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://s3.amazonaws.com/guides.diditbetter.com/GAL_Sync_Scenario.pdf	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp, DiditBetter_Support_Menu.ps1.0.dr	false		high
http://support.diditbetter.com/support-request.aspx	a2e-enterprise.26.3.3677.2903.exe, 00000000.00000003.1805077363.0000000002207000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1407717
Start date and time:	2024-03-12 18:06:47 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 4m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
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:	• HCA enabled • EGA enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	a2e-enterprise.26.3.3677.2903.exe
Detection:	CLEAN
Classification:	clean5.winEXE@2/93@0/0
EGA Information:	• Successful, ratio: 100%
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 • Stop behavior analysis, all processes terminated

Warnings

- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: a2e-enterprise.26.3.3677.2903.exe

Simulations

Behavior and APIs

No simulations

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:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Add2Exchange Enterprise Guide.pdf

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	PDF document, version 1.7
Category:	dropped
Size (bytes):	13802294
Entropy (8bit):	7.381292062112644
Encrypted:	false
SSDEEP:	98304:AVtrmiA6vqtF7gGDpOUU1egv9+SGqjoHm6z3MIBlPB86QnXAe:AVcp6odUUUb+SGwcLBo6Qn7

MD5:	E42B5D240E70A4AE87E23B646B2CE944
SHA1:	6811A7D2FD4B4C5B84BE239C63DF0BC22ADFBC3C
SHA-256:	B2485A101BFBD604737D39FF4A91507292E24784F98CACCCAC48486D32249812
SHA-512:	45B69F7791E1506460560FAEF8768416F59415B231DFFA47CFF690EEA1D5C764DCCF7C5E9F73D57184960876C45D41AF1D2A64C9DD65244F6CF11189BA706512
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	%PDF-1.7.....2 0 obj..[/ICCBased 3 0 R]..endobj..3 0 obj..<<../Filter /FlateDecode ../Length 2596 ../N 3 ..>>..stream..x...wTS....7.P.....khR.H..H..*1..J..."6DTpDQ.. .2(...C..."...Q....D.qp...Id...y.....~k....g.}.....LX....X.....g`.....I..p..B..F...|.I..... ..*.?.....Y"1.P.....\...8=W.%.O..4M.0J."Y.2V.s.,[|..e.9.2.<..s..e...'.9....`.....2.&c.tl.@.o..|N6.(....sSdl-c.(2.-.y..H._.../X.....Z..$...&\S.....M...0.7.#.1..Y..r.f..Y.ym..";.8980m-m.(..]....v.^....D....W~.....e....mi..]..P....`/....u.}q..\|^R..,g+...\K..k)/.....C_\|.R....ax.8.t1C^7n fz.D....p.....u....$../.ED.L L..[.....B.@.....X..!.@~..(*. .{d+..}..G.....}W.L...$..cGD2..Q...Z.4 .E@..@.....A(..q`1.....D .....`'..u..4.6p.t.c.48....`...R0...)...@.....R.t C....X.....C.P...%CBH..@.R.....f.[.(t....C..Qh...z.#0...Z..I..`O8.....28.....p.\..O...X.?.....:..0...FB.x$..!....i@.....H...[..EE1PL.....V.6..Q.P..>.U.(j...MFk.....t,:....FW.....8.... .c.1...L.&.

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Add2ExchangeSetup.msi

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.2, MSI Installer, Create Time/Date: Mon Jun 21 08:00:00 1999, Name of Creating Application: Windows Installer, Security: 1, Code page: 1252, Template: Intel;1033, Number of Pages: 200, Revision Number: {6CC5F0A5-DD20-463B-A745-23226EA64FC9}, Title: Add2Exchange Setup, Subject: Add2Exchange, Author: Advantage International, Comments: A Microsoft Exchange Server synchronization program., Number of Words: 2, Last Saved Time/Date: Mon Mar 11 15:43:44 2024, Last Printed: Mon Mar 11 15:43:44 2024
Category:	dropped
Size (bytes):	30423552
Entropy (8bit):	7.989713441416668
Encrypted:	false
SSDEEP:	786432:AZHbPULLLrq72tsjOH5uQol2vRY+DVN8HKOG:AlPsHrTtsjOH/Hz0H
MD5:	2D8B406D3C360459C99E3A1BC9D1E30E
SHA1:	3288467999C470DC54535A831C47720C299103BE
SHA-256:	F1B7B284704703E02471A645F7295D6678EC87DF998B2C9A90C6B3067CFB590C
SHA-512:	ED6A44B2ED614CE9B2FC698701BAFA8D806B4A3F7158C6AE9F2F2D190A9A0A74FF17F4F0C3A50357323581E339900DAD933F9CFE8CC3D55FC8701EAAAE2E67E5
Malicious:	false
Reputation:	low
Preview:	.....>.....8.....w.....u.....{..... .....Z..... .....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...G.....:...;...<...=...>...?...@...A... B...C...D...Y...F.....H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...[...\...]..._.....^.....`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v. ..w...x...y...z...

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\EULA\Add2Exchange EULA.pdf

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	PDF document, version 1.7, 6 pages
Category:	dropped
Size (bytes):	416578
Entropy (8bit):	**7.9921021749352**
Encrypted:	**true**
SSDEEP:	6144:0DZnpoW8Juj+7PQzBg5vxLX09lgN9h26fswbbEH2XeudeW0uLX:AnNj+bQK5vio9TswUTkeo
MD5:	5717BDB29D1561AE86E08AF6459CAC84
SHA1:	7D74FF33E1A7299CAF9BF2F45D64F15F2F0C336A
SHA-256:	FB6B1D910F9B44416C50E5E31E449835391B9B33FD238AA45C5BCB61465F7373
SHA-512:	995045AC8002438BB0958FBBDB3261B850D4C2AAE7684BE668A94449608573080A079E90458FEDBA5120376C248B913DA1E7141A0591E3E7FECCE4D907C1C203
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	%PDF-1.7..4 0 obj.(Identity).endobj.5 0 obj.(Adobe).endobj.8 0 obj.<</Filter /FlateDecode./Length 77377./Length1 352268./Type /Stream.>>.stream.x..}.`T.....Y 2K..7{..dB2Y....(....$.d..%.\p....}i..j...b@.im...`m+..P...J[.....7.....\|p..=w}..w.s.9.. ..F..u..O..[P<...3.<.Lhn.oY.x..?<...Lh.:....!.....N.~z.8Q...".5O.:}.....@..k.N.1}.;/V.4...:m.. xi.e./..\....4y...k....`.....t.....9.]R.....c.;.....{.....-:...._*....@U....]`.-.7....].ra.....kz.`.._p.....>...-.;.....Az.E.`S8....0.Zt..K..V=....a....]H.%>.:.&.Y:o.9..[...X....^.3.....}.,X1....l. ....^..._...O....k.....-...t.....-..F...'...k..5.....kw...M.s..,.Z.<..j.`..).77}..`.N..v.bm.. .....y9.....@.....2. .....%.ix.R..]P..K..j.....M>.....2..</.I.Rx.....J!KUMrii..(.....h...c... .80~....e.....:?S_....N.,....r....Lz+..s.Px`y.0.....L.=0.{."......9.I./.....V._.....a$A .U.N..7.....?....pT .....b.0.....I..=.....7....

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\EULA\Add2Exchange EULA.rtf

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Rich Text Format data, version 1, ANSI, code page 1252, default language ID 1033
Category:	dropped
Size (bytes):	16151
Entropy (8bit):	4.908485763338948
Encrypted:	false

SSDEEP:	384:8EK8+x+DdcyDbv+IvRapPD3+roNVkLNXm64rd2:XK8+x+htbvJwN3+rocP
MD5:	F23F6315632CF0B58C2243A3FA3E4D06
SHA1:	CD32534BAEE9CCB55C1FAF8653FC53DB22291C85
SHA-256:	EA34C9C0CD918EF15FCE8FEED4DF83359BDE1D6E60F6632378970D73D68F36A7
SHA-512:	A5CC08E0CCFE4BD48CDF19D5638B3A34B756DFA8636A12CBD53A78415DCFE6874DFFE99119CDF4D4CF7C05EB041EB461B8E8F48FB84EAF07BAD85FFB4AC97AAB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033\deflangfe1033{\fonttbl{\f0\froman\fprq2\fcharset0 Times New Roman;}{\f1\fswiss\fprq2\fcharset0 Calibri;}}..{\colortbl ;\red0\green0\blue255;}..{*\generator Riched20 10.0.17134}{*\mmathPr\mnaryLim0\mdispDef1\mwrapIndent1440 }\viewkind4\uc1 ..\pard\widctlpar\b\f0\fs22 Add2Exchange End User License Agreement\par..\b0\par....\pard\widctlpar\sa200\sl276\slmult1\f1 This EULA covers both the Retail License and the Original Equipment Manufacturers License. By proceeding, you agree to be bound by one of the following options. [Option #1 is the Retail License and Option #2 is the OEM License]. This is your END-USER LICENSE AGREEMENT ("EULA") FOR DIDITBETTER SOFTWARE(r). IMPORTANT-READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (whether an individual or an entity) and [Option #1 - DIDITBETTER SOFTWARE, a division of Advantage International, Inc. ("DIDITBETTER SOFTWARE")] or [Option #2 - the manufactur

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\First_Time_Installer.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	17385
Entropy (8bit):	4.608607390064206
Encrypted:	false
SSDEEP:	192:y4EBdqrg+gCoTgFPjAJy9oWSWvncm5yJvv8WEj+WonoHEqNgr:CpCocFPSyKWdvXAJcWEtoiEq+r
MD5:	24906D4F36602C1492A74A26C229E000
SHA1:	11A0EA2FDE23EF154F4B2F2E0B37BF4BDB20B390
SHA-256:	E8F85E3101B5613AF06DD998E7E119A9D8F48B2CB0178FD79769EF4CCA73FD0C
SHA-512:	00C6C2F4F94EB11860F061DE5E53A710C93FD13AFDC71D475087AD4C3058E4AB9205E8C3567F420A9D538C80035B29A866002F27DA1BE4AB55206C181BC9FB7
Malicious:	false
Reputation:	low
Preview:	<#.. .SYNOPSIS.. Create Initial Environment for Add2Exchange Install.. Assign Permissions for Add2Exchange.. Install Add2Exchange.. Cleanup.. Luanch Add2Exchange for the first time.... .DESCRIPTION.. Step 1: Account Creation.. Step 2: Upgrade .Net and Powershell if needed.. Step 3: Create zLibrary and Create Shortcuts.. Step 4: Install Outlook and Setup Profile.. Step 5: Mailbox Creation.. Step 6: Create a Mail Profile.. Step 7: Add Permissions (moved to step 11a).. Step 8: Add Public Folder Permissions.. Step 9: Enable AutoLogon.. Step 10: Install Add2Exchange.. Step 11: Add Registry Favs.. Step 11a: Setup Timed Permissions.. Step 12: Cleanup..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurren

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Links\Request Support for DidItBetter.url

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Generic INItialization configuration [InternetShortcut]
Category:	dropped
Size (bytes):	207
Entropy (8bit):	5.155953403004538
Encrypted:	false
SSDEEP:	6:J254vVG/4xtOFVm/lCBL3W3yLPiQAwW3UGIyc1ynE5Vsv:3VW4xtOFVm9C93W3yrCwWghynd
MD5:	A675BC61B22D603FA553D133C3A80530
SHA1:	69C7F69497435AE1C7045FC7646DF7E030A71D60
SHA-256:	703F87D93902B09647F65B0A6C0FAC76AD3D3ECEFCECBA0B487D6BE5FC11CC86
SHA-512:	6B7410E10F34E3675B57A12A0F3986396FFFF60187CE07B8BC2932E463351EEF8C4BF8B0E5E384BEAAEA79CDBA4CBA606C12ECABBC93D0C5FADC40B8A439D6A5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,2..[InternetShortcut]..URL=http://support.diditbetter.com/support-request.aspx..IDList=..IconFile=C:\Windows\system32\SHELL32.dll..IconIndex=160..HotKey=0..

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Outlook_Installer.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2031
Entropy (8bit):	4.9264371266008435
Encrypted:	false
SSDEEP:	48:uLI0WZPDP6MPPOb0PPGsGyk9z1585wQ5zYGLa9zOdg9zzPtvvKn3anIPII:20WIMaMyyk9z1585wQ50GLa9zOdg9zxC

MD5:	9A6C59517107E29E7078D7B96723CB98
SHA1:	3511E00B4372319EF796129621FC62D4AF7A4FA5
SHA-256:	C0553E6FA21203007BCF887EB57BACDC9E01BB3646495200A76C372030164CEF
SHA-512:	C14AA17A084ECA0E3EC106F962AF5271ABCF9AB363CC5D3AC467D29ADF4BFDE1D36CD7AF707897D913C77F660E3B3585527CA8CE15F51EE4930FC210039CECC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<#...NAME.. Outlook Installer..#>....Add-Type -AssemblyName System.Windows.Forms..[System.Windows.Forms.Application]::EnableVisualStyles()....$Outlook365Installer = New-Object system.Windows.Forms.Form..$Outlook365Installer.ClientSize = New-Object System.Drawing.Point(247,169)..$Outlook365Installer.text = "Outlook 365 Install"..$Outlook365Installer.TopMost = $false....$ProRetail = New-Object system.Windows.Forms.Label..$ProRetail.text = "Office 365 Pro Retail"..$ProRetail.AutoSize = $true..$ProRetail.width = 25..$ProRetail.height = 10..$ProRetail.location = New-Object System.Drawing.Point(21,30)..$ProRetail.Font = New-Object System.Drawing.Font('Microsoft Sans Serif',14,[System.Drawing.FontStyle]([System.Drawing.FontStyle]::Bold -bor [System.Drawing.FontStyle]::Underline))....$Pro32 = New-Object system.Windows.Forms.Button

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Office365_Pro_Retailx64_Configuration.xml

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1023
Entropy (8bit):	5.202613438368244
Encrypted:	false
SSDEEP:	24:OkfEslTC6jycWuLcWlfAcWiLcWbFS8httxkB:9fE+e6jyctLcrcjLcqDDtyB
MD5:	BC70B4D7C9C7053F4C30FC1721A67D63
SHA1:	D9E574805F4018C7CC25C2AA97DC56DA3E0B5044
SHA-256:	794E2365F2E580F669BAD988064606F814A1EDDDB7F865C3D291AAF15AE1EF0D
SHA-512:	6AF3A9F2428698FB935894470BF7F0AC8BEAE66936DF3E6B5994A96E62972AD693763892B4FF58CE322E8275C135F4E2FE3A31CBA7A87AC15DA129B0CB24256
Malicious:	false
Preview:	<Configuration ID="0ed28122-0109-4692-886e-6c4b754f4025">.. <Add OfficeClientEdition="64" Channel="Broad" ForceUpgrade="TRUE">.. <Product ID="O365ProPlusRetail">.. <Language ID="MatchOS" />.. <ExcludeApp ID="Access" />.. <ExcludeApp ID="Excel" />.. <ExcludeApp ID="Groove" />.. <ExcludeApp ID="Lync" />.. <ExcludeApp ID="OneDrive" />.. <ExcludeApp ID="OneNote" />.. <ExcludeApp ID="PowerPoint" />.. <ExcludeApp ID="Publisher" />.. <ExcludeApp ID="Word" />.. <ExcludeApp ID="Teams" />.. </Product>.. </Add>.. <Property Name="SharedComputerLicensing" Value="0" />.. <Property Name="PinIconsToTaskbar" Value="TRUE" />.. <Property Name="SCLCacheOverride" Value="0" />.. <Property Name="AUTOACTIVATE" Value="FALSE" />.. <Updates Enabled="TRUE" />.. <AppSettings>.. <User Value="0" Name="runosc" Id="L_TurnOffOutlookSocialConnector" App="outlk16" Type="REG_DWORD" Key="software\microsoft\office\outlook\socialconnector"/>.. </AppSett

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Office365_Pro_Retailx86_Configuration.xml

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1023
Entropy (8bit):	5.2041868894674
Encrypted:	false
SSDEEP:	24:OTfEslTC6jycWuLcWlfAcWiLcWbFS8httxkB:ufE+e6jyctLcrcjLcqDDtyB
MD5:	6C49E64FFF25A2225546976F7A9BE5F6
SHA1:	6CC15D048275904F2E8D7AFC1F7789750FC6365E
SHA-256:	B52A9402BB73233A077BC2437228A26AEEB9C8F53FE3E9147209A09A9D5A833F
SHA-512:	FDCF646EA8D896ACA2EF3AF156D5403D509EAA06580A87854BAA5B2D0353B4483F62EA60F128338020E8039A95A3DC3FC85A45ED4A2539929A0A3B366A0F7B99
Malicious:	false
Preview:	<Configuration ID="0ed28122-0109-4692-886e-6c4b754f4025">.. <Add OfficeClientEdition="32" Channel="Broad" ForceUpgrade="TRUE">.. <Product ID="O365ProPlusRetail">.. <Language ID="MatchOS" />.. <ExcludeApp ID="Access" />.. <ExcludeApp ID="Excel" />.. <ExcludeApp ID="Groove" />.. <ExcludeApp ID="Lync" />.. <ExcludeApp ID="OneDrive" />.. <ExcludeApp ID="OneNote" />.. <ExcludeApp ID="PowerPoint" />.. <ExcludeApp ID="Publisher" />.. <ExcludeApp ID="Word" />.. <ExcludeApp ID="Teams" />.. </Product>.. </Add>.. <Property Name="SharedComputerLicensing" Value="0" />.. <Property Name="PinIconsToTaskbar" Value="TRUE" />.. <Property Name="SCLCacheOverride" Value="0" />.. <Property Name="AUTOACTIVATE" Value="FALSE" />.. <Updates Enabled="TRUE" />.. <AppSettings>.. <User Value="0" Name="runosc" Id="L_TurnOffOutlookSocialConnector" App="outlk16" Type="REG_DWORD" Key="software\microsoft\office\outlook\socialconnector"/>.. </AppSett

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Pro_Retailx64.cmd

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.572765012132931
Encrypted:	false
SSDEEP:	3:Pg4QQ6/QIK6Wde8UMeKJ:PVQQFKWIU2

MD5:	E49E7FD101C66A32558FF27564234222
SHA1:	671A4BBE57BB7C9E872693DFA4CDC967D4329A93
SHA-256:	72507222065118F1D879128E8E98C633AFA6C21275CB9246F5AAC18041A1FDBF
SHA-512:	1A7CE80BE39B2B2CF38B1687A0CD6E9F318C216F6562F1170283835360B8AFE053D72CAD6714F4073927932BFFCD3EDDFCAB09962A6C145BF5F34C1CBD261EB
Malicious:	false
Preview:	setup.exe /configure Office365_Pro_Retailx64_Configuration.xml

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Pro_Retailx86.cmd

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.572765012132931
Encrypted:	false
SSDEEP:	3:Pg4QQ6/QIK6WdoMeKJ:PVQQFKWi2
MD5:	8D16D2E6750AE5217ADBBAC538E6E89E
SHA1:	06126FF482AB5F91E32315DE94ECE2F39533C1BF
SHA-256:	FFB180B7837FAB58A39779694E3025F98A0AE6B747B3A84BCB96BBA59486C5F7
SHA-512:	D17FC93E05CAF4FB938EC1CE9A18793610A2B2381D020227613117031E238B0E6F8A1957EC1000BDD7D2CF2587C3DD1FD4C2CD93010B70686FDF46747BE50B2C
Malicious:	false
Preview:	setup.exe /configure Office365_Pro_Retailx86_Configuration.xml

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\setup.exe

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5169440
Entropy (8bit):	6.649944627880774
Encrypted:	false
SSDEEP:	98304:vqihTvjtEh2N5LQhyddG4THBZoJG3QBMxvble/bsTwY2h3:TpvE8dgq3oJG3QBMxBlW3
MD5:	B374FA0E7E34B9CE9C142FE80E1EFADE
SHA1:	2537F4523B12E9801F2ACB8FE38D5D725A56A61D
SHA-256:	A87105965530799BABBB71A1FD52DBD7CDDEE71C40E2C37576235D156FF02027
SHA-512:	8F5FF73932568006C38B9E1BB8DAABF0DC6E419FC1E6D96159FB1234439B8AB9B283D617540CDC5860538AFFEA89BA0A553F4CCF2B9F1949D9E907BA56C2F74C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....Gc.-...~...~...~..'~...~..%~...~..$~#..~Ig.....~Ig..+..~Ig.....~...~...~ ...~...~fd.....~fd.....~fd.....~fd.....~...~)..~.d.....~.d.....~.d)~...~..A~...~.d.....~Rich...~.....PE..L...r..[.....".....l+..2#.....#.....+...@.....O.....O...@..... .....8b?.....A.....N. ?...`K..<.....:.8.....:.....,@.....+.8....M?.....text....k+.....l+..... ..`.rdata.....+.....p+.....@..@.data.....?..H. ..x?.....@....rsrc.....A.....@.....@..@.reloc...<...`K..>...dJ.....@..B.....

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup.zip

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=store
Category:	dropped
Size (bytes):	2668259
Entropy (8bit):	**7.998881312154931**
Encrypted:	**true**
SSDEEP:	49152:MUbYsgyV5rS/kPE79ObqVIBYZKKXEqYbrjdLiBWn8qfMVqCqJ:MUbYsgyUcgOldZ4ZZLou6qCqJ
MD5:	A00060FA16A451A14EFD4D8431CF4FA0
SHA1:	57EE5FF9CE2DCD217AFC03820FDF2E4A1EFB072B
SHA-256:	5FC1DC21BE4CBC3536079157FD9C75F93EAC09C90DF836432320817E7C720F1A
SHA-512:	4C02E3F18FB1F66BE214811491C7FA11E4570E947DD3C34A18B13A3F24F37B117266E91ACAF0B6A4F11A21A8965918C83CCF8D39AD142290566FBCEFAB8888BA
Malicious:	false

Preview:	PK.....@[W.....Setup/PK.....AiV .-.....<.....Setup/A2E_Auto_Migration.ps1..ks.F.{f....g..Rj..t<u3...6.p.6..C:.j.S...$.....0N_..|...n_.k.}....>...no...K..<.K.....%=. ...^.....kx.....\|".v..7C.g.bR.Y.....R.....%.....h.....y..2.L.O....+..v.+u-.pSr...%....pc...oL..K7..g.R...Sr\|$.f.V.....^...e.c>w.N-2.....d...z,R.=P.....H..fTp...WN..... ~.7.....h|. }x.3e[.q....O.,...;.fOH].*..z.@..X.=.vM..qi.....c.i..7...h..7.F'.}.u$.@MB....5.];.`0.o4..e.g..]sJ(.8a...5[.Cn. 8Pp.A}.....6e.c..#.~...}N.5...wZ....s.....g.....A.c..fdYla...P. O.....k8..\|.h.....ERX8Zz4.$.S~}....%.C..... :.'Z.`.....w4.=..b...C..(.....\K.}E}....|..+k..7..TJ..<~....C.....6..<..+.,f....g..A.dx..G.....;...u..c.S..c.J.x<.38...it*...}.7M...v._.N... .....c.....H..:...j...R.5..2P..x...?v..p..`.e...=ri...U.7..F}....W..`.L-h..O.>...^M+.x..d.C.'K....p...gk6.|..nM...(D..=.....Z.L#.<g.b..c..(#. .K.R..c..Q..5R..e.Ex..

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\A2E_Auto_Migration.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	15579
Entropy (8bit):	4.889068941413246
Encrypted:	false
SSDEEP:	192:URv4EBdSWEG7Dw4XpX4XoXJszFpzVf+/g7sD5FNPZWSDw4XpX4XoXhopz6f+/g7j:URxSWRb5oY+zd+/gI55oYOzC+/gqS
MD5:	93424836BFC74EF4E3291D2AD4190A59
SHA1:	3E9240FD41C8BDD4F969D1676CB4859FA4480F2E
SHA-256:	B9FC8E91F823BC275C8A881B9918609D646546AF25255E9F25E339544A662441
SHA-512:	7E95C9EC2D62D1AD8831BD2160B58C248AECDEF60EF07F7F4322B71A037141C4F784AF50CF80334674B53063098CFC66255E33CBAF9B52057FE1E77BC035D2F A
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Step 1 of 2.. Run Post_A2E_Migration.ps1 after this.. Automatically Migrates Add2Exchange to a new server.... .DESCRIP TION.. Check for current files and locations.. copy reg. files for Add2Exchange and backup.. Backup A2E SQL DB and move to landing zone.. Down load from S3 latest build of Add2Exchange and upgrade prior to move..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_Power

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\A2E_Directory.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	897
Entropy (8bit):	5.143902574568429
Encrypted:	false
SSDEEP:	24:SU0+J2+rcELm7LR6LPk1ophAl6PoHZu2p2MeD3nMhz:A+gYmPROsEDm9eD3E
MD5:	F0881E090546B066243B4E31C5871A4F
SHA1:	20E3AFBA20B081A484E4F6EA00E865394D7DAFC8
SHA-256:	09DC73CEAAC643ED32120FBB7AE81BE75A922C2318A3A55ACED9042CF0350466
SHA-512:	96AA3A128CCF4C7B9735F349A31C240A927D2F44F855BC5C66554A2A466C96028805991BB508EC3DDAE35A5BDF6368FBC4B212AFAAD458041550812FD904067
Malicious:	false
Preview:	<#.. .SYNOPSIS.. A2E Directory shortcut.... .DESCRIPTION.. Open Add2Exchange Directory..... .NOTES.. Version: 3.2023.. Auth or: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Princ ipal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass -Force.....# Script #....$Install = Get-ItemPropertyValue -Path "HKLM:\SO FTWARE\WOW6432Node\OpenDoor Software.\Add2Exchange" -Name "InstallLocation" -ErrorAction SilentlyContinue.. Start-Process $Install....Write-Host "ttyl".. Get-PSSession | Remove-PSSession..Exit....# End Scripting

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\A2E_MMC.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.206402114423433
Encrypted:	false
SSDEEP:	24:zKU0jSJ2+rcELm7LR6LPk1ophAl6PoLZu2p2MeHhpyhz:8+gYmPROsEDO9eHhpK
MD5:	6C6FE5D9C01ED59D63ABC1737A003357
SHA1:	B8FE156802D624D1B1322A211A572C6EC0332E33
SHA-256:	2C9CDDAA12253497C76A7DF48A9E9845FE3D9D3289F2E5844043EDDDA57C6273
SHA-512:	1405622C66DB32383DD8CDEB3409261BD3FD11B8C96BEA0D757B87AEA3EE09E6D98EF39F20303FB8C47A132A2B632A5385A76970AB8E59ADA2D3B79ADCB07 C3A
Malicious:	false

Preview:	<#.. .SYNOPSIS.. A2E MMC shortcut.... .DESCRIPTION.. Open Add2Exchange MMC..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass -Force.....# Script #....$MMC = Get-ItemPropertyValue -Path "HKLM:\SOFTWARE\WOW6432Node\OpenDoor Software.\Add2Exchange" -Name "InstallLocation" -ErrorAction SilentlyContinue..Push-Location $MMC..Start-Process ".\Console\DidItBetter MMC.msc"....Write-Host "ttyl"..Get-PSSession | Remove-PSSession..Exit....# End Scripting

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\A2E_Permissions_Commands.rtf

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Rich Text Format data, version 1, ANSI, code page 1252, default language ID 1033
Category:	dropped
Size (bytes):	216321
Entropy (8bit):	4.453510072484783
Encrypted:	false
SSDEEP:	6144:Bruqfz1OZCOkNCRPRs8rHwsREvJGA217MY0sM:hLZOZtpBRmH2V+sM
MD5:	8A81C1400FFC2CD5B1FAAD465C0701EE
SHA1:	D26758B75BB032383464C2F5E5B020DD06FAE7D8
SHA-256:	8CD1F3A5BB0971E36910A7B67E48E2F7C6D310FD088BDA61B498E231AE585F0B
SHA-512:	146A14848BD885D892B38DD264D98D77805273A4F714A355446C0B81DAFBD200B1647E20C1370EC0DDF836B8B4E1F3EF99E5CF3A01477762354BA34F2360193E
Malicious:	false
Preview:	{\rtf1\ansi\ansicpg1252\deff0\nouicompat\deflang1033\deflangfe1033{\fonttbl{\f0\fnil\fcharset0 Calibri;}{\f1\fmodern\fprq1\fcharset0 Consolas;}{\f2\fnil\fcharset0 Arial;}{\f3\fswiss\fprq2\fcharset0 Calibri;}}..{\colortbl ;\red106\green153\blue85;\red212\green212\blue212;\red86\green156\blue214;\red220\green220\blue170;}..{*\generator Riched20 10.0.19041}{*\mmathPr\mnaryLim0\mdispDef1\mwrapIndent1440 }\viewkind4\uc1 ..\pard\widctlpar\f0\fs22\lang9{\pict{*\picprop{\sp{\sn wzDescription}{\sv Image}}{\sp{\sn posv}{\sv 1}}..}\pngblip\picw5349\pich1291\picwgoal3033\pichgoal732 ..89504e470d0a1a0a0000000d494844520000184d000005dd08030000008fbc05e8000000017352..474200aece1ce90000000467414d410000b18f0bfc610500000300504c5445000000ffffffffcef..e7fef7f3fadeceef9560eb7d3cf9d6c2f5be9df2ad85d3e5c7b8d5a6cae0bcdcead2e4efddf4b6..91f09d6cec8547f6faf48cbb6e72ac4d95c179afd09af1a578ed8d547ab157f6c6a9f7ceb683b6..63fbe7daa7cb8fc1dbb19ec684edf5e9ecececb2b2b2c5c5c5d9d9d9f5f5f5cfcfcf6666667979..798c8c8c6f6f6fbcb

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\A2E_SQL_Backup.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	8283
Entropy (8bit):	5.268485089494731
Encrypted:	false
SSDEEP:	96:lPdmPEB3GsP9ELNqjkdsiY7/MyDIC4GmL2MuozftgXWefk7NawVJDQxx/vJvXW1x:b4EBWsPGNqXMyD2LPR6RYNawVpYvBE
MD5:	E289DC757526BB6118CCD8B234483DB7
SHA1:	7185C6F23862169FA3E148935909E28952FA5D08
SHA-256:	C3C92F663B02D0E1E2B2BD46AE8A2983DC6A829EB4E4A8AF09B4D37B589D593C
SHA-512:	F7E76959B0EC843C2EE8C97FBF1D730F779D0BE369C13CCDF83A9D25D9792E02CF06905D2E51AC3CF420B43CBAFAFE80C4F70E4141AC3F6727E866CF529615F
Malicious:	false
Preview:	<#.. .SYNOPSIS.. A2E SQL Backup.... .DESCRIPTION.. Auto backs up the A2E SQL database.. Makes task for auto backup.. default retention is 5 copies..... .NOTES.. Version: 4.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Variables..$Install = Get-ItemPropertyValue -Path "HKLM:\SOFTWARE\WOW6432Node\OpenDoor Software.\Add2Exchange" -Name "InstallLocation" -ErrorAction SilentlyContinue #Current Add2Exchange Installation Path..$CurrentDB = $Install + 'Database\' #Current Database Location..$ServerName = Get-ItemPropertyVal

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\A2E_Setup_Details.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with very long lines (485), with CRLF line terminators
Category:	dropped
Size (bytes):	20181
Entropy (8bit):	5.1450742793043265
Encrypted:	false
SSDEEP:	384:4Xp3AzWqaGaAn6b/bSA40PeFlREGS+FUzgrfFfGroH+mLMYT+RdwKGip4fP28Ewj:yb340SlRjS+6zgLFfeoH3MYCRdbGiKfz
MD5:	8DC459D4B78D918A341B4938B1552F70
SHA1:	595052E1A7BA7A36D8A32AF4CC53AE1B0F85D4EF
SHA-256:	1F27A71C9A9008D49BAF22364336AF763ACB549D260225E387746199A68D6EA8
SHA-512:	EC2DE4DE898083E46C4BE3F32D1FEE0E5032223D4BFF73D9988C51C1DC1C8038E86B4F36184AD4DCBD1EC804020B0CF08D82010DF9FD276E10FA77C826AAEB3
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Powershell script to include Add2Exchange setup details in .txt.... .DESCRIPTION.. Checks registry for A2E setup details and prints to .txt file.. Get licensing info.. Get install paths.. Get local account for Add2Exchange.. Get PS Version.. Get Windows Version.. Get DB Version..... .NOTES.. Version: 1.10.2023.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....# Script #....#Logging..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Support"..if ($(Try { Test-Path $TestPath.trim()

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Add2Outlook_Set_Granular_permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with very long lines (355), with CRLF line terminators
Category:	dropped
Size (bytes):	24006
Entropy (8bit):	4.5977428899880435
Encrypted:	false
SSDEEP:	192:q4EBlX9hOegnbK4pDTfMQ2EX6LyOCXzY4pvfMmc8n6w0STq4pffMcG:EAnbK4pDTfMCuwzY4pvfMQvTq4pffMH
MD5:	9531BBFDE471AF746FDFEEB69964B848
SHA1:	CAE7CAD062B3FE3EF4ED3B78BDE521823C169E99
SHA-256:	229C448416621A50ED51125A1973D019BF3A5FE596584A4CE53E3C6AE1B0A098
SHA-512:	029D7B8703A2A5BF2F1F0B48F5E6F461B3FCD3D3662DBC5DC903E29C201CD565867263FC6576B32730FB11857C3945309DD3550E9AE563C671FD6546CDB6C94
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Add2Outlook Granular permissions.... .DESCRIPTION.. Sets Granualr permissions to users on-premise or office 365..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Support"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "Support Directory Exists...Resuming"..}..Else {.. New-Item -ItemType directory -Path "C:\Program Files (x86)\DidItBetterSoftware\Support"..}....Start-Transcript -Path "C:\Program

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Permissions_Task_Creation.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	41968
Entropy (8bit):	5.243228574520891
Encrypted:	false
SSDEEP:	384:H6tXgbb7+HNlzF2lm8tPj78F2cfBF2lCUBI2F2lzRjRtF2xpF215F2NAF2kFF2G2:m0ADOPpen/Fx0j
MD5:	BB243A354ADBE069FCAF359567A51028
SHA1:	A224B862CEFEEE04408459E81EDC2639DAD3D2E0
SHA-256:	7AED627FC4B85C44148A3AAAEF85B80636D388838AFDE60D62C494E53C8DEA3F
SHA-512:	9FD37D8ACBDC015580B7C2E0A090BDF6C68D52416D5EEA7203EACF9C3F3407A8B0A7A56F072286AEAD99DDB224B79655C77C8F38E00BC7D28698D954D9F7CEA
Malicious:	false
Preview:	#Logging..Start-Transcript -Path ".\A2E_PowerShell_log.txt" -Append....#Pathing....$TestPath = ".\Add2Exchange Creds"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.. ..}..Else {.. .. New-Item -ItemType directory -Path ".\Add2Exchange Creds"..}....#Check for MS Online Module..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2) { Write-Host "You are on the latest Version" } .... Else {.. Write-Host "Upgrading Modules..".. Update-Module -Name ExchangeOnlineManagement -Force.. Write-Host "Success

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\2010-2019_All_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2151
Entropy (8bit):	5.162487348740605
Encrypted:	false
SSDEEP:	48:9YmPROBka5K9X9Lz9k9TEIltstjA4HcYA4Zx:qmPEBVo9X939k9TaMjYY9x
MD5:	3A7D2158C9D2F4FCB32B6E159B0B525E
SHA1:	26955DDF02A0ADA152B45B870A3757EE35DDB157
SHA-256:	8E47D64B5963369453417FFC938997BEF43B15C951C57E52DF190B4BABD95276
SHA-512:	4C0B8E4A3D6832842823CE9D13D864A746CF3876F542A1E5111346C1E21F41481DCA11684CAF0032C7BD8862839486E44B8185903C11DB6E0CE733F10A891DF2
Malicious:	false

Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit.. }.. .. .. #Execution Policy.. .. Set-ExecutionPolicy -ExecutionPolicy Bypass.. [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12.. .. #Variables.. $Exchangename = Get-Content ".\Add2Exchange Creds\Exchange_Server_Name.txt".. $ServiceAccount = Get-Content ".\Add2Exchange Creds\Sync_Account_Name.txt".. $Username = Get-Content ".\Add2Exchange Creds\Exchange_Server_Admin.txt".. $Password = Get-Content ".\Add2Exchange Creds\Exchange_Server_Pass.txt" | convertto-securestring.. .. # Script #.. .. Try {.. .. $Cred = New-Object -typename System.Management.Automation.PSCredential `.. -Argumentlist $Username, $Password.. .. $S

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\2010-2019_Dist_List_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2102
Entropy (8bit):	5.230466173766324
Encrypted:	false
SSDEEP:	48:9YmPROBk6PBN9n9LT9U9TS9jY1tkD7PzNIFMGIA4H9r:qmPEBtPBN9n939U9TS9y8bS2P5r
MD5:	89CF421CCCE150873AA500F3758F8F5A
SHA1:	0B65BA14167491C7764374092CBE1B7013BC5DD0
SHA-256:	FBE3DB3AE3ABACE46DD71EAF8FB1CFE9CDD6E5487B58FD5D94FF1ECA6BF91ECE
SHA-512:	CB948C442328D6A0AD0DF3B9382E2A482DEAE6CD3A613E30411F9C9A3DA172E7F249D0D6DD4DC03E987A400418ECF9D3305C976C305B768F50EEDC3FF34D2DF
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Variables..$Exchangename = Get-Content ".\Add2Exchange Creds\Exchange_Server_Name.txt"..$ServiceAccount = Get-Content ".\Add2Exchange Creds\Sync_Account_Name.txt"..$Username = Get-Content ".\Add2Exchange Creds\Exchange_Server_Admin.txt"..$Password = Get-Content ".\Add2Exchange Creds\Exchange_Server_Pass.txt" \| convertto-securestring..$Groups = Get-Content ".\Add2Exchange Creds\Dist_List_Name.txt"....Try {....$Cred = New-Object -typename System.Management.Automation.PSCredential `.. -Argumentlist $Username

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\2010-2019_Dynamic_Distribution.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3035
Entropy (8bit):	5.145689633354292
Encrypted:	false
SSDEEP:	48:9YmPROBk6PBN9Z9U9TZ9n9x1tkfnAH7lzYtn3BKz1w:qmPEBtPBN9Z9U9TZ9n9n57m6xKz1w
MD5:	1F7EB58896F3866ECF20359778262CC9
SHA1:	93116FF3EDF8528B74641019AEABE9CF53EB528B
SHA-256:	86DC185646EA5CDFEBBB3EAB8A188F3E4A006C07C256777FB18652EAB29564D1
SHA-512:	200C61EBD1C921E461EF6B7129C15A4E094C6C0BBBC235BB199EDA82C99F64EB688C9EF028E76A0233AC476BF851A3B105B782F0B4F6DB4DDC01C0636BE9E659
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Variables..$Exchangename = Get-Content ".\Add2Exchange Creds\Exchange_Server_Name.txt"..$Username = Get-Content ".\Add2Exchange Creds\Exchange_Server_Admin.txt"..$Password = Get-Content ".\Add2Exchange Creds\Exchange_Server_Pass.txt" | convertto-securestring..$DynamicDG1 = Get-Content ".\Add2Exchange Creds\Dynamic_Name.txt"..$StaticDG1 = Get-Content ".\Add2Exchange Creds\Static_Name.txt"....Try{....$Cred = New-Object -typename System.Management.Automation.PSCredential `.. -Argumentlist $Username, $Passwor

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\Office365_All_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2554
Entropy (8bit):	5.173142548372283
Encrypted:	false
SSDEEP:	48:9YmPROBk642pHCZMC/9LT9/9+EY7A4H29:qmPEBtKMC/939/9+ti9
MD5:	454AD4DAF7770AA0475332B7B61F35A8
SHA1:	D9CAF58B50B20B15B6D713DC1C2A87CB0F421CFE
SHA-256:	0B995601F037D76FD2B6B9746AFDCC33A29F8769772A7E26AE8DDA20B79B392A
SHA-512:	D19D3080FD3207716A8AB794DDB103339D50C28AC0BC24FCBBE80BD10E64A27C0282844F6E32B55643AD196912E043A16A3C45EF187C83AB3ED0B1A2CE3F25F
Malicious:	false

Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Check for MS Online Module..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2)

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\Office365_Dist_List_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2772
Entropy (8bit):	5.190597884596586
Encrypted:	false
SSDEEP:	48:9YmPROBk642pHCZMC/9LT9/9+S9jYT7PzNIFMGIA4HyKx:qmPEBtKMC/939/9+S9qbS2PmKx
MD5:	40849438C1AD17F7506ECA0AF810E5A5
SHA1:	622291B78908387DBE154E641D6D22496DA2C946
SHA-256:	9E68CCDA9FA2A971FF15BEA0264A326433C9DAE2AE635E240A790ACE6C7B5F49
SHA-512:	A05BBBE610A0E9317E764782FB375C4140B55CDA1AE0C535B4993A183DE77F74C39BD056853EAE7FA8DE55C33C2E7861F0E58B5C73BA867F52B4F5BD6479393 4
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Check for MS Online Module..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2)

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\Office365_Dynamic_Distribution.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3701
Entropy (8bit):	5.118368046067273
Encrypted:	false
SSDEEP:	48:9YmPROBk642pHCZMCB9/9+V9v9uYWNja7IzYtn8UQprG:qmPEBtKMCB9/9+V9v9ia7m689prG
MD5:	0E3C648CF3C2A950A790C8412752F058
SHA1:	7AD73D971222436E5801E14AF3A43A1E49FE1E9F
SHA-256:	528E4E9F041933014B6CBB1C1405DBBF2CEA0A5225AC56F5090D333595BFEDA7
SHA-512:	E7CE197E2993FA6AABDF8AC4823BD8CAF08312E1AC5D785CF40E28ABB271850444D911678914F4F5DEBD1AF485DCDD642B9037C0127406761ED71ADFBFC414 DE
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Check for MS Online Module..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2)

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\Shell_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with very long lines (355), with CRLF line terminators
Category:	dropped
Size (bytes):	35480
Entropy (8bit):	4.466946069094336
Encrypted:	false
SSDEEP:	192:q4EBXL2hO9keHSowqzeZrTJN7nW9pdYkyO:2nkeHSowqCZ78YkF
MD5:	09F016831A4007FBC4A35EF1C5E88CDA
SHA1:	9AFEC61CECE26BCA466EB0F98EB1D9AD95A83D71
SHA-256:	A1095A2035A2CCD0C20A7DB63A6A473FD1973F481C2C6995A910518320DFEA4F
SHA-512:	0039359F4547CBBEF21ED0584FC16A6FB488CDE30702F4BBF05A354D472033E413111215360F3C0B78884DF4ED7746E35E43836D9BEB41DBAC2EBEB73351DD7 7
Malicious:	false

Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging....$TestPath = ".\Support"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "Support Directory Exists...Resuming"..}..Else {.. New-Item -ItemType directory -Path ".\Support"..}....Start-Transcript -Path ".\Support\A2E_Permission_Results.txt" -Append....# Script #....$Title1 = 'Add2Exchange Enterprise Permissions Menu'....Clear-Host ..Write-Host "================ $Title1 ================"..""..Write-Host "How Are We Logging In?"..""..Write-Host "Press '1' for Office 365"..Write-Host "Press '2' for Exchange 2010" ..Write-Host "Press '3' for Exchange 2013-2019"

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\Stand_Alone_DyanmicDistList_Task.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1182
Entropy (8bit):	5.177298437958451
Encrypted:	false
SSDEEP:	24:9ELm7LR6LPk1ophAI6PoqGba5KNZDaNvmLbPXuq7Whz:9YmPROsEDFdAzuX
MD5:	E7429B9BC39E9217F0FB503DE41E1364
SHA1:	0608BB8B293A11F58EEB8CAA322CAF670CD48EFA
SHA-256:	6C696EF6E3D94FE2712B3063C7A52C6618A0D346C0B22718572FE7DB2A178885
SHA-512:	DB305B546B58D66809CC7F79389CE1D637C1EDDFB490162527C95752A306F2E616CB264B03719A40297773CE1A79D960B453F6EFA6B3C9486648705D351D56B5
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass.....# Script #..# Report Correct File Path of DynamicDistribution List File..Write-Host "Creating Task".. $Repeater = (New-TimeSpan -Minutes 720).. $Duration = ([timeSpan]::maxvalue).. $Trigger = New-JobTrigger -Once -At (Get-Date).AddMinutes(1) -RepetitionInterval $Repeater -RepetitionDuration $Duration.. $Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -WorkingDirectory $Location -Argument '-NoProfile -WindowStyle Hidden -Executionpolicy Bypass -file "ENTER FILE PATH HERE"'.. Register-ScheduledTask -Action $Action -RunLevel Highest -Trigger $Trigger -TaskName "Add2Exchange Permissions" -Descrip

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Permissions_Portable\Scripts\Stand_Alone_Dynamic_Distribution_List.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2376
Entropy (8bit):	5.091813731955432
Encrypted:	false
SSDEEP:	48:9YmPROBkH+yF0TveJjpnAH7IzYtn3BKzi:qmPEBl6KeJjs7m6xKzi
MD5:	CBC1624883A282B70B867D25B380EE1C
SHA1:	519E9B90F6558C1B507A1B71F9706B9400FE1E40
SHA-256:	0470A94170B0407E9C8AF85F2292EA767A424A82686E1991E28F320A2A325809
SHA-512:	16E60FA701564121144AD3217F7F1689C39FB9D368067256C08D4CF0E57CAFEB75B65F2F32FC58AF5119A62D6F1B253B5E18210B4871EAE48CB8E93EA5F0245D
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....# Service Stop #..Get-Service -ComputerName "TYPE COMPUTER NAME HERE" -Name "Add2Exchange Service" | Stop-Service -Verbose -ErrorAction Stop..Start-Sleep -s 30..Get-Service -ComputerName "TYPE COMPUTER NAME HERE" -Name "Add2Exchange Agent" | Stop-Service -Verbose..Start-Sleep -s 10....# Script #..Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;..Set-ADServerSettings -ViewEntireForest $true.. .. #Variables..# Fill Out Dynamic and Statis Distribution Groups Below....$DynamicDG = @("Dynamic DL HERE", "Dynamic DL HERE")..$StaticDG = @("Static DL HERE", "Static DL HERE")....for ($i = 0;

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Upgrade_Add2Exchange.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	13582
Entropy (8bit):	5.313134466355976
Encrypted:	false
SSDEEP:	384:XUY0O+oYiiMwqhZ6UbLPr9pNjg/vXdAZNBvOrj75bxF5HXgoco8D7zRRCOOyiD+n:z0O+oYiiMwqhZ6UbLPr9pNjg/vXdAZND
MD5:	6BEDF8B55CAB971FF2E23CCC1EA27E7F
SHA1:	627234B6FF79F0780A8B7DAE89B0BDEE54F7526E
SHA-256:	77AD9D0C0B089A83B26AAEFEA3CE8165F0EF1E32B3819AC16B3C4EF9CBCCEE21
SHA-512:	C516BB789C1E8CC52835FFC29C3B25A3BF50E0CE1730BCD2721DE99CD211CB3F976C75928805A5A97A9AED791410C7D05F13ABC5B24D85DDA071B7C5374B13B
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Automatically upgrades Add2Exchange to the newest version.... .DESCRIPTION.. Check and Creates scheduled update for Add2Exhcange.. Checks for outdated license keys and prompts before upgrading.. Downloads from S3.. Upgrades Add2Exchange to latest build.. Sets password for Add2Exchange Service.. Start Add2Exchange Console.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>.. ....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Upgrade_Add2Outlook.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4036
Entropy (8bit):	5.235276683746445
Encrypted:	false
SSDEEP:	48:3WN3qEyse+3iL+gYmPROBkuNQloEMmotXW0muXzag4fvSSRkFWJKMZyqc0IAXzI2:3WPyPCmPEBd+aVnSRRF/ADJHofSLPw
MD5:	4AAA734208D8E215BBAB17D855B7CF97
SHA1:	93840F59A560538EE2DBB7DA884D70FDE2DDAB4B
SHA-256:	B6BF85319892EBDDA5FA5CF47F59531153C463D33A1D74C39D3C704CE2405556
SHA-512:	82357105967198B1494A9483527FB26D9F8110FC20811733C7E3A4FDE6D0D96B0D5688C71F05B5703D42F27D692924C339F15A42376E2CC7CF92C677AAFB1C43
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Automatically upgrades Add2Outlook to the newest version.... .DESCRIPTION.. Check and Creates scheduled update for Add2Outlook.. Checks for outdated license keys and prompts before upgrading.. Downloads from S3.. Upgrades Add2Outlook to latest build.. Sets password for Add2Outlook Service.. Start Add2Outlook interface.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Upgrade_RMM.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6201
Entropy (8bit):	5.186007695712116
Encrypted:	false
SSDEEP:	96:3BcOyaymPEBt0qBfROuEnSjc5SomkY8DP9ku7zF7GNnSnMF/AN6HofYCntdX92rc:C4EBtbf0uSSjlQY8aCa/AEHS
MD5:	2FB639DA7949E56BAA214AE840F13E0B
SHA1:	AC820AE801AB94D6041B5CA11921E53DD31BA232
SHA-256:	2A4E8368A8A7CCAFDE0E226BB499A53A5F265DFBFB48155221C1AD067D7CB072
SHA-512:	F96D6C64D6C99307332835D93B08C8705A32AB74B1FD06E7E24E3856DCD40956ACBFA21FC21D766E0806F2D7DBB8EC161CC52D61621A12290CE51AA9BD9B61B
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Automatically upgrades Recovery and Migration Manager to the newest version.... .DESCRIPTION.. Check and Creates scheduled update for RMM.. Checks for outdated license keys and prompts before upgrading.. Downloads from S3.. Upgrades RMM to latest build.. Start RMM in terface.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>.... if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit.. }....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass ....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....#Test for Upgrad

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Auto_Upgrade_ToolKit.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4164
Entropy (8bit):	5.222446959080407
Encrypted:	false
SSDEEP:	48:3WN3qEyse+3iL+gYmPROBkuNQloEMFtXWaZXzag4fvSSRkFWJkWZyqcKIAXzIy/v:3WPyPCmPEBd+qrnSlLF/AOHofKcOx
MD5:	28E59560B884DA8763573D7B485297E4
SHA1:	05507AC499BF399373C168177ECBC4DD4E60ADD5
SHA-256:	919D7C612EA6790AE25373037E04AE138356135124F83A4A2C9253D3CB42014C
SHA-512:	9677C82C3388628260DAEAA67FB99048AF6B87771BF6E370CA7A73FC705E882452A62AA3C24DA03F2A6B0F829DBCAECACBAC0D04B4B442613324D7A5E9FC6D0C
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Automatically upgrades Add2Outlook to the newest version.... .DESCRIPTION.. Check and Creates scheduled update for Add2Outlook.. Checks for outdated license keys and prompts before upgrading.. Downloads from S3.. Upgrades Add2Outlook to latest build.. Sets password for Add2Outlook Service.. Start Add2Outlook interface.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Autologon.exe

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	138920
Entropy (8bit):	6.351883874026519
Encrypted:	false
SSDEEP:	1536:uMpeguHQeJD3z7NF0Y1g/z1EwyjcOzk954H6STYSs+sRd1cccTMTsWjcdLEs6y2S:Js5HQeh/vgLewZUFYdmJ4s6puehSE+EU
MD5:	607A332709458F781C20AB49940C4B64
SHA1:	923409BE6C1B183C74DA221DD23A42B4B981BA19
SHA-256:	324C64D24818A0BE63A43A8DF678B88DCA4F8959841F91F4875CC6ED0E93F549
SHA-512:	DF90A3E8B041B756DAD139E4036C3D3F512D4348FCA222886E765FA20D1A578271038A798D4D8936447D9767272FC2D27AB0ABE1F021673ED43F3B8DBC730AD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....bc....K...K...K.Q.K...K.Q.K...K.Q.K...K.{.K...K...KF..K.z.K.. .K.Q.K...K...K...K.z.K...KRich...K.....PE..L.....W.....9.....@.....0.....@.....>.....0..... .....@.....text..... ..`.rdata..p.....@..@.data...<1.....@....rsrc.....@..@.rel oc..0.....@..B..... .....

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Bypass_AutoDiscover.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2311
Entropy (8bit):	5.186434811896025
Encrypted:	false
SSDEEP:	48:ZZrFM+gYmPROsEDUX7PpQzs6PkQ8ajPpEIxPphApPp8rgn7:1MCmPEsNrhmR88hEIxhhAphsgn7
MD5:	E4178F8743EFBCF5C913DF3B0C0A67EF
SHA1:	63F9EFBB79FDD3E92DBCB446CD63F41BF0E419E7
SHA-256:	10BEAABFD5D7E3DB3BFF5DEDF25FA115B70603CB4C7B3F984240488D3FE93DEC
SHA-512:	D800D8247F2E8A7B930526A7150857A775CAA68FB358DF2FD3D6490E17DBCAE71C176579D1CC1C31C9AB3EC55E6BDA36774BC6ABAA3E6030142D09CB3169C 05
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Bypass AutoDiscover.... .DESCRIPTION.. When ran, will set registry keys in regedit to bypass current autodiscover and exclude O365 Endpoint..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force ....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #....# Bypass AutoDiscover..Get-ItemProperty -Path "HKCU:Software\Policies\Microsoft\Office\16.0\Outlook\Autodiscover" -Name "ExcludeExplicitO365Endpoint" -ErrorAction SilentlyContinue -E

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\DiditBetter_Support_Menu.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	36279
Entropy (8bit):	5.094410419594323
Encrypted:	false
SSDEEP:	384:iqZEMT2lsd9y18hT2lA5h1OYYPT2lPxD49gccsWT2l1oLq6Al4nlT2lhAKrRWQb5:Dm36PZ+
MD5:	3243E53FE3DC8EBDD8DD2D9C82862EB2
SHA1:	C2FE83D72161EF9A3D8FB01E84B7F2621832E296
SHA-256:	2C3173702001100EDA5538994095561DA59B7023E34EF1F748F2634FA5B39B9B
SHA-512:	5D0E8C8E3C23E75C3139B9CD9DB9B580862A9A92DF4D7EE0C6337DF54C0CEB0B192B5CD6F679A3F0694EA9E5D12A21AF5B1358C0847A4B6F27E57FEF8C20F A3
Malicious:	false

Preview:	<#.. .SYNOPSIS.. DidItBetter Software Support Menu.... .DESCRIPTION.. Menu for all powershell tools used.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....Add-Type -AssemblyName System.Windows.Forms..[System.Windows.Forms.Application]::EnableVisualStyles()....$DidItBetterSupportMenu = New-Object system.Windows.Forms.Form..$DidItBetterSupportMenu.ClientSize = New-Object System.Drawing.Point(542,725)..$DidItBetterSupportMenu.text = "DidItBetter Software Support Menu"..$DidItBetterSupportMenu.TopMost = $false..$DidItBetterSupportMenu.BackColor = [System.Drawing.ColorTranslator]::FromHtml("#ffffff")....$Upgrades = New-Object system.Windows.Forms.Label..$Upgrades.text = "Upgrades"..$Upgrades.AutoSize = $true..$Upgrades.width = 150..$Upgrades.height = 10..$Upgrades.location = New-Object Sys

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Dir_Sync.ps1	
Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	1761
Entropy (8bit):	5.156369223547245
Encrypted:	false
SSDEEP:	48:6X+gYmPROBku5S4uvdGeE/unqH9eD7MFszUHjLH:oCmPEBd5S4ulCunqC7MGojT
MD5:	F15B2367D478E08070CF913EFF9775A4
SHA1:	3B239969D571EC0F29E4C88D7ACF783FDB3EC50F
SHA-256:	9853B16C6DC415B0FE4D19FC9929D987CEEFFDBC65BAD3C5426CDAA4897CD5EC
SHA-512:	C9B94757D0F30B29F27D5F4D0F4C14D3E9A66F2D9CB14F0ECD23D0CB285B61B6B4AD30260573ED3AE71CF8D8B9DFC9922C39E478CD6AF69DF19FFBBFF2E4FE09
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Directory Sync.... .DESCRIPTION.. Forces AD sync with cloud AD..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....# Script #..$wshell = New-Object -ComObject Wscript.Shell.. ..$answer = $wshell.Popup("Caution... You Must Run this on a box with Active Directory. If the box you are running this on does not have Active Directory; Click Cancel and the File will be Automatically copied to your Clipboard. Otherwise, Click OK to Continue.", 0, "WARNING!!", 0x1)..if ($answer -eq 2) {.. $Location = Get-Ite

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Disable_Modern_Authentication.ps1	
Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2643
Entropy (8bit):	5.267360743384632
Encrypted:	false
SSDEEP:	48:HrxMy4+gYmPROhE5UNleEXfEXmtXyBM9wv4DyEwDEuwDymDRn7:54CmPEh9j0mAa9WCyEKEuKy8Rn7
MD5:	DAC366EB2AC0C56F103FCE8F00DFE019
SHA1:	390268DFFE32FE42E167CDC5BD95F2FD1BF63C7C
SHA-256:	AEAE6072BC4BA590E63D789457E46EFCB5FDC1EDC9A5E49C850D834E8ABED797
SHA-512:	BFDCF96F078325CA890CE1CF182196A0ADD12F3BE50558B6B499C52898A5587995F1E46F682913DB25BB48311A70A3B75A5D806CDED12CFE93D6D5AD4AB8B8A
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Disable Modern Authentication.... .DESCRIPTION.. Will disable Modern Authentication for machine that it is run on.. Outlook will then use creds manager on board to connect to exchange..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #....$TestPath = Get-Itemproperty -path "HKCU:\SOFTWARE\Microsoft\Office\16.0\Common\Identity" -Name EnableADAL..$TestPath = Get-Itemproperty -

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Disable_Outlook_Updates.ps1	
Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1490
Entropy (8bit):	5.198020535628352
Encrypted:	false
SSDEEP:	24:oXtLJ2+rcELm7LR6LPk1ophAl6PoPsIN4SHAts+8XToL9bGs+8XToLo/T8GnzJhz:oX2+gYmPROsEDUXr2N8XTawN8XTao/R7
MD5:	4D42BA60AD65211D97ACD062F44E7332
SHA1:	01847AA3E0AF6DB359AD6F1C95D68C20F9C24C11
SHA-256:	21C7370D4D2A23DF0F8C3DF41077AF150497F526B25FAC566C705AAF6DD005B8
SHA-512:	AFF23EB46EE4E323BFE28CA3C15BAE0FB0CB9F7048CB3E56FAA76AC1CA9844FD58CF92046C62E0790F8F2D1403500183A60294176C65A162B1A91D92EF0BBE58
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Disables Outlook Updates.... .DESCRIPTION.. Will disable automatic updates within outlook..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #....Do {.. $confirmation = Read-Host "Would you like to Disable or Enable Outlook Updates [D/E]".. if ($confirmation -eq 'D') {.. Write-Host "Disabling Outlook Updates".. Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Office\C

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Disable_UAC.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1403
Entropy (8bit):	5.267747383282788
Encrypted:	false
SSDEEP:	24:SvD+ilJ2+rcELm7LR6LPk1ophAl6Po/INdWnVV6InVVodkMUSoMnrojRnz:SvD+iq+gYmPROsEDn3qOQokxSoSrox
MD5:	06EF6793B7BB09AC2DCA61E6B9CD8E9F
SHA1:	19389578400B32411CC079DA4BB84433340A0DAF
SHA-256:	7168CE2EE7EDF60478CA33A20070A43EF5825ABF2596CFE14CAB6299B76AC7CA
SHA-512:	7DFBA058341CC28B83D3FF347D2A124E09A3F1852CA65E3712A3F3D932E2F1D08E867CAA4E1DD91C92CA6B0DE9A4C3D7A7818044378FEBE5A8E8A5C27830E81F
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Disable User Access Control.... .DESCRIPTION.. Disables User Access control within the registry.. Reboot is needed if disabled.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Disable UAC..$Val = Get-ItemProperty -Path "HKLM:Software\Microsoft\Windows\Currentversion\Policies\System" -Name "EnableLUA"....if($val.EnableLUA -ne 0)....{..Set-ItemProperty -Path "HKLM:Software\Microsoft

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\EXModule_dotNET_Update.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4479
Entropy (8bit):	5.181862913027437
Encrypted:	false
SSDEEP:	96:qmPEBydtczToZMpYGoYFJoYFJEvsI3GqJSPKegPB:q4EBeATpCytoEl/Yi5
MD5:	690CA58ED8C9BA7684EE98C8AD8CA515
SHA1:	89F8AE137ADFE3B97D67564CDB301FA178D6756E
SHA-256:	3C80256C8C465767B21829577643B47DE98E91A129C562016F18FF2F2E0BF283
SHA-512:	618B34BC22E2AE4FBAF63DB00CF8FBF14FEF173C03CBEC843B0F28258A7CC9AEBE636EA15E1916AEFF734700E037BE57E3DD516A39CC440BDC73474BBE156AF1
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #....#Auto Reboot..$Confirmation = Read-Host "This update may need a reboot. Reboot automatically after successful Install? [Y/N]"..If ($confirmation -eq 'y') { $Reboot = "Auto Reboot Selected" }..If ($confirmation -eq 'n') { $NoReboot = "Please reboot when possible after update" }.....#Create zLibrary..Write-Host "Creating Landing Zone"..$TestPath = "C:\zlibrary\.NET Updates"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "Directory

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Export_ADPhoto.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5871
Entropy (8bit):	4.9788787772328185
Encrypted:	false
SSDEEP:	96:2t3dCmPEBpeYS4o2uDqC7mILsFr/5rhrWWGrhynfxJTSyrhynVZBjqiKqdcT6lSq:ig4EBkAuBCILi1FeY75YDBjsqcTlq
MD5:	73B703ABFEE693CFE74DA332CE4D6306
SHA1:	02BA53EC7F923158E3D0F72010E69AF9A983665C
SHA-256:	921FCEFFB82CA49BD1BB8B546C375FC43A701DE8976DB41655ED8807050B8B0B
SHA-512:	AA0813187360F0DBC3FF48303A286A4CCE5A82083B26F344B2FBC70C48FCB7A30BAB8C51C4E16470BCABF344F91E8CBA1F02ED1968F201AE4C237AD70B81E37C
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Export Avtice Directory Photos.... .DESCRIPTION.. Exports user photos from AD or Azure.. PLaces them in .jpg format and attaches an email to the photo.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsP rincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Support Directory..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\AD_Photos"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "Support Directory Exists...Resuming"..}..Else {.. New-Item -ItemType directory -Path "C:\Program Files (x86)\DidItBetterSoftw

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Export_License_and_Profile1.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	999
Entropy (8bit):	5.26714723254083
Encrypted:	false
SSDEEP:	24:SFLuFOJ2+rcELm7LR6LPk1ophAl6PHPek2p8DHk2phqKhz:N+gYmPROsEDveSHH
MD5:	67BCE29BD16BD783041BE4C485263227
SHA1:	F6B6570F9C474666ABEA3E36FB66CF5446A3AF7C
SHA-256:	A6DCFAB242B14EEB55F98F0055AB46856BDAED46FEC060719E91177082039C93
SHA-512:	11C347577D7C297A6951F4BA19BCC8416A06B528EBD0D66A125C0851CD58488E04F1505A191291A4BD4D792321DD88C9B2AED3177DB6DF3FBCD78C6DFC49FE E5
Malicious:	false
Preview:	<#.. .SYNOPSIS.. A2E Export license and Profile 1 data.... .DESCRIPTION.. Exports A2E reg files license and profile 1 data.. places files in zlib rary.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principa l.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}..#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....REG EXPORT "HKLM\ SOFTWARE\WOW6432Node\OpenDoor Software.\Add2Exchange\LicenseRegistryInfo" C:\zlibrary\License_Info.Reg..REG EXPORT "HKLM\SOFTWARE\WOW6432Nod e\OpenDoor Software.\Add2Exchange\Profile 1" C:\zlibrary\Profile_1.Reg....Write-Host "Done"..Write-Host "ttyl"..Get-PSSession | Remove-PSSession..Exit....# End Scripting

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\First_Time_Installer.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	17385
Entropy (8bit):	4.608607390064206
Encrypted:	false
SSDEEP:	192:y4EBdqrg+gCoTgFPjAJy9oWSWvncm5yJvv8WEj+WonoHEqNgr:CpCocFPSyKWdvXAJcWEtoiEq+r
MD5:	24906D4F36602C1492A74A26C229E000
SHA1:	11A0EA2FDE23EF154F4B2F2E0B37BF4BDB20B390
SHA-256:	E8F85E3101B5613AF06DD998E7E119A9D8F48B2CB0178FD79769EF4CCA73FD0C
SHA-512:	00C6C2F4F94EB11860F061DE5E53A710C93FD13AFDC71D475087AD4C3058E4AB9205E8C3567F420A9D538C80035B29A866002F27DA1BE4AB55206C181BC9FB7
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Create Initial Environment for Add2Exchange Install.. Assign Permissions for Add2Exchange.. Install Add2Exchange.. Cle anup.. Luanch Add2Exchange for the first time.... .DESCRIPTION.. Step 1: Account Creation.. Step 2: Upgrade .Net and Powershell if needed.. Step 3: Create zLibrary and Create Shortcuts.. Step 4: Install Outlook and Setup Profile.. Step 5: Mailbox Creation.. Step 6: Create a Mail Profile.. Step 7: Add Permissions (moved to step 11a).. Step 8: Add Public Folder Permissions.. Step 9: Enable AutoLogon.. Step 10: Install Add2Exchange.. Step 11: Add Registry Favs.. Step 11a: Setup Timed Permissions.. Step 12: Cleanup..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurren

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\GP_Results.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1559
Entropy (8bit):	5.174877386170697
Encrypted:	false
SSDEEP:	24:YhvEJ2+rcELm7LR6Lifk1oxhAlOHoPWIN/kvjstXBGXjdmPZGkvsv/S+jyGnzJKS:YNL+gYmPROBkuNp4jstXcsDsHVjPn9
MD5:	D8F3B0F174893BFD6855097BCF188C38
SHA1:	5D3CC8271B4E8F192368369E8F8D1A6C651AA9E7
SHA-256:	891FB63F37784A2D77653278198C3B1CEEC2F923BE32A1FBFE38D3284E29ED26
SHA-512:	0AA9A49F4084A5084CB6075592EF46F2039F8C4D467B680E7990FD08455F3CE0985C7A1066928445530143446 2BAF91AC5D6E97DC563CD70D599DEE328893318
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Group Policy Results.... .DESCRIPTION.. Finds and diplays current group policies on current user and machine.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent( )).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyI nvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Group Policy Results..$TestPath = "C:\zlibrary"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "zLibrary Directory Exists...Resuming"..}..Else {.. New-Item -ItemType directory -Path "C:\zli

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Get_Diags.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2063
Entropy (8bit):	5.320900192955916
Encrypted:	false
SSDEEP:	48:goN+gYmPROBkuNQtXhRvzfh305LK1019skCZ:9NCmPEBdmdmZi05m
MD5:	2F9F4E1534713C5F75B2D1569B4980C8
SHA1:	D317F95060E851D36DE749BD0C3EA164331FACE9
SHA-256:	D294B5769B0DFE14ED596287FD3676D7FD8F034DFC3D9844AE8D6AD9F25DF870
SHA-512:	EE43595AC38D5C2CA5BEBB6C35720ABB1ECDC8BABDF50E04CF0B9987315E8F03F14DF6D6818A93DD3045E490162393003E5FC60C450382A1D924C75B73393C F
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Get A2E Diags.... .DESCRIPTION.. Downloads and extracts A2E Diags from Amazon S3.... .NOTES.. Version: 3 .2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInR ole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocatio n.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....#Create zLibrary\A2E Diags Directory....Write-Host "Creating Landing Zone"..$TestPath = "C:\zlibrary\A2E Diags"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "A2E Diags Directory Exists...Resuming"..}..Else {.. New-Ite

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Legacy_PowerShell.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4326
Entropy (8bit):	5.300027941259094
Encrypted:	false
SSDEEP:	96:YhPCmPEBdHHYXTYp8rgcr9wSEW4v2ZQwSES8ZwSEVc:R4EBdYXsirvJZ+Z8tr
MD5:	38AC352720450197714B1C8A9A32ACE3
SHA1:	D3C6469DC5B28659DEFA3B7DCA680B78463C1135
SHA-256:	E52FFA8E1FD828987EE62B2975DBD7900EB138EBE95FA03F6BD66B0A07269FB3
SHA-512:	86168DA8760E7663D3001DE186E68BE041566FE786275A62BB96A32D49C67DA02C9D7E8EB19B4BF58E1DF61CF0BA2AA2FDE1379517E62597F545E1C55C7FC71 7
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Powershell script to check and update .net and .... .DESCRIPTION.. Will update Powershell to 5.1 if .net is below version 4.5.. Get Windows Version.. Get .net version..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Pri ncipal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an ele vated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -Ex ecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Check if .Net 4.5 or above is installed..$release = (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full\' -Name Release -Err

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\MSExchangeDelegation.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with very long lines (321), with CRLF line terminators
Category:	dropped
Size (bytes):	3485
Entropy (8bit):	5.146501540480007
Encrypted:	false
SSDEEP:	48:G54+gYmPROBkx9JltXiJJ5lJTS4uvdGeE/unqH9eD7rdBNR/S7ERp5rZjPnv:G54CmPEBuMW4S4ulCunqC7rDN3JZjPnv
MD5:	C3B6051BFF57D81301759DFF51EDE1C5
SHA1:	C65685554BA7717D9980D46FBE9A52B4FEE60F90
SHA-256:	202D5AA879A1511C7F8EB926B6A5AD98DBF9D13443CD54C9D8414C142DFE9B09
SHA-512:	44C445F99A30389BF63B1C3FCC90256AE10DE4277B074EA208952AF0F414770B7744C5D47423C5697FE294D2F16019D53CE1D1D0D4A55D2F6D8908DA0B4119C
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Microsoft Exchange Delegation.... .DESCRIPTION.. Finds old data in msexchangedelegate attribute field for users in a specific OU.. Must run this on AD.. Removes the msexchangedelegate list link from the user.... .NOTES.. Version: 3.2023.. Author: DidItBetter Softwa re.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Admi nistrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.. .. ..#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass.. ..#Support Directory..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Support"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.. .. Write-Host "Support Directory Exists...Resuming"..}..Else {.. New-I

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\OSC_Disable.bat

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2735
Entropy (8bit):	5.422414574821863
Encrypted:	false
SSDEEP:	48:qeo1e9eoxe9ZW9eIxZW9edZW5eIxZW5edXW9eIxXW9edXW5eoxXW5eaz4zF0Bnzu:qREdEZW99ZW9kZW59ZW5kXW99XW9kXWV
MD5:	59FDCC52E51AC335C4D24CD27A0FD8BC
SHA1:	019DDC5FD0193C995CA930959E4A8F8BB38C03AC
SHA-256:	3B123AA11B50E117A4FBA11ED03922121F64ED5C8D64DA30F0AEACEC78F0C820
SHA-512:	DCC1B89D0AA1419BF85EE71ABC415878D23F3BA33D5ACBFD522B2E47702112F5090D1E191C714E8635D7DBE5667B172AF0E8C88FC99D845DB6CFB614EE21B4 B9
Malicious:	false
Preview:	reg query HKLM\SOFTWARE\Wow6432Node\Microsoft\Office\Outlook\Addins\OscAddin.Connect....if %ERRORLEVEL% EQU 0 (..reg add HKLM\SOFTWARE\Wow64 32Node\Microsoft\Office\Outlook\Addins\OscAddin.Connect /t REG_DWORD /v LoadBehavior /d 0 /f..)....reg query HKLM\SOFTWARE\Microsoft\Office\Outlook\Ad dins\OscAddin.Connect....if %ERRORLEVEL% EQU 0 (..reg add HKLM\SOFTWARE\Microsoft\Office\Outlook\Addins\OscAddin.Connect /t REG_DWORD /v Loa dBehavior /d 0 /f..)....reg query HKLM\SOFTWARE\Microsoft\Office\15.0\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Office\Outlook\AddIns \OscAddin.Connect....if %ERRORLEVEL% EQU 0 (..reg add HKLM\SOFTWARE\Microsoft\Office\15.0\ClickToRun\REGISTRY\MACHINE\Software\Wow6432Node\M icrosoft\Office\Outlook\AddIns\OscAddin.Connect /t REG_DWORD /v LoadBehavior /d 0 /f..)....reg query HKLM\SOFTWARE\Microsoft\Office\15.0\ClickToRun\RE GISTRY\MACHINE\Software\Microsoft\Office\Outlook\AddIns\OscAddin.Connect....if %ERRORLEVEL% EQU 0 (..reg add HKLM\SOFTWARE\Microso

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Office_Updater.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	980
Entropy (8bit):	5.145816531057854
Encrypted:	false
SSDEEP:	24:GoqapJ2+rcELm7LR6LPk1ophAl6PofINPy+27hz:GoqJ+gYmPROsEDNr2h
MD5:	F7AFFC19CB6DD094845898341D7F08B7
SHA1:	57BF666D2BC57314E4B1CDAFB859E02FD87ABFAD
SHA-256:	8DA1870CAC7721E842024BE4653DEA71D8799F7DFB1BD598DCCFD4E639F7F1BF
SHA-512:	D45539CFD91BF560F6CA0CC55AE7064BFF55849EB265914287DA0E80D6AE7ABB1639AF907978A7A11E045A6EDF9CCCC8E49C3083FC900525479FC319AE6C02 D5
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Microsoft Office Manual updater.... .DESCRIPTION.. Will start the process for Outlook to search for new updates.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurre nt()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyIn vocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Logging..Start-Transcript -Path " C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #..Set-Location "C:\Program Files\Common Files\Microsoft Shared\C lickToRun".....\OfficeC2RClient.exe /update user.....Write-Host "ttyl"..Get-PSSession | Remove-PSSession..Exit....# End Scripting

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Outlook_Installer.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2265
Entropy (8bit):	4.869041116921122
Encrypted:	false
SSDEEP:	48:fLn2wmL+a0WZPDP6MPPOb0PPGsGyk9z1585wQ5zYGLa9zOdg9zzPtvvKn3anlPlI:Sdr0WIMaMyyk9z1585wQ50GLa9zOdg9M
MD5:	D44914C6A4C7369D3C627CD4E10BD2D1
SHA1:	7C216AF33F406E83EE06FCC19084A8667AE47DED
SHA-256:	6320EA3B5D06B458781D3EA9411C9E80BBFE6352A3C9D714A371333883D1032A
SHA-512:	5D29A3E880AC2862D7051D6A5F45CAED339C783B1A797459BFAE0E1A6AFC43236B7181471AE81C0BC4C703DC51F2147C6813B2BC30D913E85F2BCC5AD34608 B
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Outlook Installer Menu.... .DESCRIPTION.. Choose between Outlook 32bit or 64bit.. This is just a menu for choice.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....Add-Type -AssemblyName System.Windows.Forms..[System.Windows.Forms.Application]::EnableVisualStyles()....$Outlook365Installer = New-Object system.Windows.Forms.Form..$Outlook365Installer.ClientSize = New-Object System.Drawing.Point(247,169)..$Outlook365Installer.text = "Outlook 365 Install"..$Outlook365Installer.TopMost = $false....$ProRetail = New-Object system.Windows.Forms.Label..$ProRetail.text = "Office 365 Pro Retail"..$ProRetail.AutoSize = $true..$ProRetail.width = 25..$ProRetail.height = 10..$ProRetail.location = New-Object System.Drawing.Point(21,30)..$ProRetail.Font = New-

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Outlook_Profile_Set.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	20832
Entropy (8bit):	5.392154078265476
Encrypted:	false
SSDEEP:	384:K4Dno5fW6yyfe8sPbkZb/CzHtlf+qm/Vru1Fw4Ck8CjI8r:NDno57CzHtlf+il8r
MD5:	880A9575A59B6D1B592248FAC5EE0571
SHA1:	4807DD3AF489E41FAB399745F0B57722FDBE5DE5
SHA-256:	84205172A09054014BB37A59CC32A75D21C941CDBE6D570424AA9544A6BBC670
SHA-512:	6165CBFFADF62A44D1F8007E9F7DF4CF707DEA3A4997BAEE8FA89421990EED67075F70274415B7CACAE1CBA474BB68DC6CDFBB091A44C2617B32E0DAB53FABA9
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Outlook Profile Setup.... .DESCRIPTION.. Setup Outlook profile for Add2Exchange.. Setup GAL Options.. Setup Send/Recieve.. Disables COM Addins.. Sets Options.. Disables Outlook Popups.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #....#Check Outlook Version..$Version = Get-ItemProperty "Registry::HKEY_CLASSES_ROOT\Outlook.Application\CurV

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Outlook_Tools_Menu.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	5780
Entropy (8bit):	5.151421010601781
Encrypted:	false
SSDEEP:	96:ir0WeMjI/wz9zqL29zI+9zruY9z3lB9z77u9zPdt9zuk9ze6cqW:NyE/wz9m29M+9fuY95B9H7u9zdt9Ck9U
MD5:	140B1F8CA61563B37C91750045ECBF87
SHA1:	28354FA245E5310B8C74F240EEF115B9C41D44E6
SHA-256:	3E7B62BD9BBE9222449438EDBAC7198C5BAF01E77D32E19FDABAC645293AA10A
SHA-512:	C06F1D8F0D6B769FDFA5E43572DD82F0B4D7D99CC87D64D0D7042D58BC9192DF9B3F3DAB1F0470A0C89EF2046BDBA62A71476F7F0B7331B54E2B7A23996269B
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Outlook Tools Menu.... .DESCRIPTION.. Simple Menu to show tools that link to powershell files.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....Add-Type -AssemblyName System.Windows.Forms..[System.Windows.Forms.Application]::EnableVisualStyles()....$OutlookTools_Menu = New-Object system.Windows.Forms.Form..$OutlookTools_Menu.ClientSize = New-Object System.Drawing.Point(247,344)..$OutlookTools_Menu.text = "Outlook Tools"..$OutlookTools_Menu.TopMost = $false..$OutlookTools_Menu.BackColor = [System.Drawing.ColorTranslator]::FromHtml("#ffffff")....$Rearm_Office = New-Object system.Windows.Forms.Label..$Rearm_Office.text = "rearm Office"..$Rearm_Office.AutoSize = $true..$Rearm_Office.width = 150..$Rearm_Office.height = 10..$Rearm_Office.location = New-Object System.Drawing.Poi

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\PermissionsOnPremOr0365Combined.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with very long lines (355), with CRLF line terminators
Category:	dropped
Size (bytes):	37412
Entropy (8bit):	4.4377513076022455
Encrypted:	false
SSDEEP:	192:lK4EBuL1h59kJvwqzukl6zZrTJccUV6D9pFO:lLrkJvwq3mur
MD5:	7E4D25A72B3C66B9434B31C57E06F287
SHA1:	80A029D83FF84BDB3239FEC19ED6D7276582098C
SHA-256:	3A95B367EAAFB21B83C53F3BF8BC252180315FB419B155A5AB9C50003C1A6309
SHA-512:	2CD4600CEC2DFEDBADE22C26151FEB6178E6EA0BA7042CFBC488B452F718F28AF5A674412C6241D581E7ADC7D173A8337375FC240A3950C9605FDEB0120E7FB7
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Permissions for on Premise or Office365.... .DESCRIPTION.. Updates PS EXO modules.. Choice of on premise Exchange 2010-2019 server or Office 365.. Sets permissions for individual users, dist. lists.. Can remove permissions.. Remove or add permissions to public folders.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Support"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "S

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Permissions_Task_Creation.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	43490
Entropy (8bit):	5.249776444593379
Encrypted:	false
SSDEEP:	384:e6tXgbb7+HNlzF2lm8tPj78F2cfBF2lCUBI2F2lzRjRtF2xpF215F2NAF2kFF2Gl:N0ADYsXQZxfnaL
MD5:	84A7CA382672E2CC2AC294809F5DD084
SHA1:	C8B5AEB08A1C2244429D9D1C2FDCA193D721C458
SHA-256:	F5CB96173BFF7C6DC81C01CC6416E9D384A6ECEC64ABEDAA95E1BD023DAE3038
SHA-512:	44F1AB6E1174273F473547E72608F26C50F99558106F1A6257054F0265105FE35F44D4A06029D713B537D242085642C50EF35C2B12B3E0521EC53482ACD72A96
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Permissions task creator.... .DESCRIPTION.. Updates EXO PS modules.. Saves and bit locks passwords and usernames for a uto log in to exchange or office 365.. sets additional tasks for permissions to auto run using credentials provided.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append.. ..#Pathing....$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.. ..}..Else {.. .. New-Item -ItemType directory -Path "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds"..}....#Check for MS Online Module..Write-Host "Checking for Exhange Online Module"..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....IF (Get-Module -ListAvailable -

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Post_A2E_Migration.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	8346
Entropy (8bit):	4.744374547827754
Encrypted:	false
SSDEEP:	192:8sY4EBfPE0BYmSABMdKJX4hBdmSATMFKJXQu:8hPjBDSABMmohBsSATM+V
MD5:	75631EEEF162F81CA161A59E63693945
SHA1:	37B8587D9228B52CC88F6234E533B771C7CE78CA
SHA-256:	0F84D9670388289E3DED4D3500656D20DA4E976CA8831B3CE8E1C95D0AD58A86
SHA-512:	0E70B72914F3AA591EB7389750DCDF29F80E1ED295C199FFF12BB1C2F1188DD90A11DEA621C79375966DBC00D6541C632E5AAFABABC0CDD59C03F2F6EB107 11
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Step 2 of 2.. Finishes Migration of Add2Exchange to a new server.... .DESCRIPTION.. Check for current files and locations.. copy reg. files for Add2Exchange and backup.. Runs First_Time_Installer.ps1 once all files are copied over..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #..Do {.... $Title1 = 'Add2Exchange Post Migration Wizard'.... Clear

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Public _Folder_to_Address_Book.vbs

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	268
Entropy (8bit):	5.030279585044127
Encrypted:	false
SSDEEP:	3:TQ9h+rOtcN+m87REKOLEBYMQsNjD/vzTKOtUDATrBAHiLIEQuUIE7UybfrQuFYL8:kgScNPcRjOcjrKuuAT7JUcEDLXs
MD5:	A7171DD633A4B2F800DF6102D7E93DC0
SHA1:	0969D0388FBE550FFB679E331B2217C37BBC1D00
SHA-256:	E93783BCF685866CDD02275E987EA5F2266FCDF50465578D132F2549A85BD634
SHA-512:	EC366E1722818C997A4B9E867ECADC076241FC98C1AB456C2CCCE86195D4E3AB21CF5156E7D05B5A735AF9E37A22326B4C1BB44799A415474D9A633AA90E13 E
Malicious:	false
Preview:	Option Explicit....Dim objOL, objNS, objFolder..Set objOL = CreateObject("Outlook.application")..Set objNS = objOL.GetNamespace("MAPI").....Set objFolder = objNS.GetDefaultFolder(18).Folders("Contacts").Folders("Firm Contacts").. objFolder.ShowAsOutlookAB = True..

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\REARM_Office.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1386
Entropy (8bit):	5.304265312379865
Encrypted:	false
SSDEEP:	24:f8NLJ2+rcELm7LR6LPk1ophAl6PoP6+8P5o1FDO+p+utP5o14DlzChz:f8G+gYmPROsEDUP8P5wDsoP5wBz6
MD5:	D3AF23D1D7084FC8BE912E016D51B4FF
SHA1:	D1B3DC03B0419669FD8BAA02D1343875693DD253
SHA-256:	0B2157D302BCAE924480D48254111A363EAB87933881A105FCB300B528041E25
SHA-512:	6D0E5BC6229FAC783E14147D13FC5A4266C6E38F59B2C83A42EBCE385F4551E991ED00CF9E00C6ACA1EB9B925C8BEA20022E011BDA5BDEAB2AB9DD417C21C B4D
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Outlook ReARM.... .DESCRIPTION.. Restarts Outlook trial mode.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}" -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force.....# Script #....#Detect Bitness..$64Bits = Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Office\16.0\Outlook" -Name "Bitness" | Select-Object Bitness -ExpandProperty Bitness -ErrorAction SilentlyContinue....If ($64Bits -eq 'x64'){.. Set-Location "C:\Program Files\Microsoft Office\Office16".....\OSPPREARM.EXE....cscript .\ospp.vbs /dstatus....Pause..}....$32Bits = Get-ItemProperty -Path "HKL

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Registry_Favorites.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with very long lines (342), with CRLF line terminators
Category:	dropped
Size (bytes):	4433
Entropy (8bit):	5.260436401478338
Encrypted:	false
SSDEEP:	48:P+gYmPROBzBr2gjUkIxUYEwoU+YUf8UIDU8kUvIkUb/UzIp0sUBIMUcVIXW9ev6r:PCmPEBUhbC7kqNf8tQtbc8cCl7XW90jw
MD5:	AF59015B32AE299D4428243674C54706
SHA1:	6B2A86DD040D579348F32F4FCC349729514491A5
SHA-256:	FFF79D64EDF0F517CCC529A88E21D3A3974BE82E9B209EDDAC0B1048943414BC
SHA-512:	FA9511E5C7C11B0A470BDD46791984F8C37A07A696A5F486FED7E2A48982A5FDD48615601B36B22515B7BE6B89E250B57AA6DD2E9B38E0D7A5AC9C2CBBE725 D6
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Powershell script to add Registry favorites.... .DESCRIPTION.. Adds Reg. Favs to Registry shortcuts..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.... Start-Process powershell.exe "-File", ('"{0}" -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append....# Registry Favorites..Start-Process Regedit....Write-Host "Creating Registry Favorites"..New-ItemProperty -Path "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Applets\Regedit\Favorites" -Name "Session Manager" -Type string -Value "

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Reset_A2E_Password.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	1776
Entropy (8bit):	5.178124013506394
Encrypted:	false
SSDEEP:	24:kDbM731MpW/J2+rcELm7LR6Lifk1oxhAlOHoPhd1sEVTIs08mCDdK6CDfsZdxV2j:R3u7+gYmPROBkuzX0gCA7Bz7MH
MD5:	6D9B75BDE724C06B10B6A2BF461859C9
SHA1:	9AC9C9CD2F844E174CBF56A6D3C66B34E911C5E5
SHA-256:	D85A2F7527A2126274FB31CBD8CE40BEF76F652EB7C3307A1DB62B2F3A896253
SHA-512:	6720554B12444558F91C07DAD836FE38AE203710A29FCE8F42851ADE40AC67838EBFAD5605CC4A1A69675F0043A514F75265DC2C6C4DFAF687CE8212DA7435E
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Add2Exchange password Reset.... .DESCRIPTION.. Clears out the password field in A2E reg... Asks for new password and updates the Add2Exchange service with new password..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}" -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass.....# Script #..Write-Host "Reseting the Servive Account Password" -ForegroundColor Red..$Password = Read-Host "What is the New Service Account Password?"..$SVC = Get-WmiObject win32_service -Filter "Name='Add2Exchange Service'"..$SVC.StopService();..$Result = $SVC.Change($Null, $Nul

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Firewall_Rules.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6339
Entropy (8bit):	4.59062346175513
Encrypted:	false
SSDEEP:	96:P8CmPEBdMt4IEYcrjJ+YALRqHALzPAFRqHAFZPn7:74EBdnIEYcrjUBR7zWR1B7
MD5:	5D15CC681D31E58EB755EDF96DAB987F
SHA1:	045A9EE48903AC50B494A0716A8751BAA0942F4F
SHA-256:	298CE83535B8F62B324ACF467722EB89E114AB09687883FCA5B27CF08E57A627
SHA-512:	C8B699E226F3D50C53ECDCC48EE4F3F8CA3B39F1B5226957B61237FE8BBE3C690B90B3F607E462ED571A689582258F42AA4F0C6DAFFBA82FA114723B3D80F473
Malicious:	false
Preview:	<#.. .SYNOPSIS.. SQL Firewall Rules.... .DESCRIPTION.. Deploys rule changes in Firewall for SQL to properly work.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyC ommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..Start-Transcript -Path "C:\Program Files (x 86)\DidItBetterSoftware\Support\A2E_PowerShell_log.txt" -Append.....# Script #..Do {.. $Title1 = 'Firewall Rules for Remote Add2Exchange SQL'.... Clear-Host .. Write-Host "================ $Title1 ================".. "".. Write-Host "Please Pick Were to Apply Firewall Rules".. "".. Write

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQL12x_to_SQL12xSP4.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	6945
Entropy (8bit):	5.221084649519329
Encrypted:	false
SSDEEP:	192:9HhM4EDNMCCmdjMVpDlSczf3cTxEa6gF1Xhx:92MXmhgpDMilEaX
MD5:	0B20B6F052DFDB6E1C3A69AF0030ACB8
SHA1:	0F1461CF9E7616F04A0F94C054C895A1850F6CF6
SHA-256:	543708058ADB5F3AC204995B2EC266AA39766FE8DEA0CB3A893673A2139DEB3B
SHA-512:	DEC7B4DF7877786C6B5724380EB1571695974D79A563C7A413DA03643FFB6A16657415ED785AFA806B0A29CE0F12A0913449A59CEDEFE0401E5BC084FA46CD7
Malicious:	false
Preview:	<#.. .SYNOPSIS..PowerShell Script to Upgrade SQL Server Express 2012 to 2012 SP4....Ensure you run PowerShell as Administrator....Ensure to adjust paths and instance names as per your environment.....1. Backup Databases..Implement backup logic as per your environment & requirement.....2. Verify SQL Server 2012 is installe d..Verify manually or add script logic as per your requirement.....3. Install SQL Server 2012 Express SP4.... .DESCRIPTION.. Will upgrade SQL Express 2012 to SQL Express 2012 SP4.... .NOTES.. Version: 1.3.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Se curity.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. #Relaunch as an elevated process:.. Start-Pro cess powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.. ..#Execution Policy..Set-ExecutionPolicy -Executi

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQL12x_to_SQL22x.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	13337
Entropy (8bit):	5.2561277625098555
Encrypted:	false
SSDEEP:	192:+1IBq4EDNQdTMVpDQSczW3ZT/HuHpy+tSLdcSJ3aWGpXrjBZo2ClUoI76v:+1QxgpDli0td5+VRZpClUJ76v
MD5:	AD4A1E79C7603CBCCBDC37A9109C498C
SHA1:	4332F28C590CED2B9B9EA66CF8EE78D28E494E53
SHA-256:	BA17D1CFF354EF35C11C62D9DAEBCD5357D2E51EEA89EFEFAC29ED912E6D6813
SHA-512:	D726DF4DCC2C71F799A9129B0BCA45FFF75455DC9CB0A409D0CD09ECF8BCF49796AD45AF6E2C768A90B6486C82ECB25E10D096FF65F0AB81EE999A003E86A45
Malicious:	false
Preview:	<#.. .SYNOPSIS..PowerShell Script to Upgrade SQL Server Express 2012 SP4 to 2022....Ensure you run PowerShell as Administrator....Ensure to adjust paths and instance names as per your environment.....1. Backup Databases..Implement backup logic as per your environment & requirement.....2. Verify SQL Server 2008 SP4 is installed..Verify manually or add script logic as per your requirement.....3. Install SQL Express 2022.... .DESCRIPTION.. Will upgrade SQL Express 2012 SP4+ to SQL Express 2022.... .NOTES.. Version: 1.3.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security .Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. #Relaunch as an elevated process:.. Start-Process p owershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.. ..#Execution Policy..Set-ExecutionPolicy -ExecutionPoli

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQL17x_to_SQL22x.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators

Category:	dropped
Size (bytes):	6918
Entropy (8bit):	5.206034581692453
Encrypted:	false
SSDEEP:	192:EAtc0q4EDNYC6djMVpDiSczf3XT/pgFyNc0q:EAi3h6hgpDbijql
MD5:	F1C85E7B65D147DD29AE2AE410AEC21A
SHA1:	4CA83E0864F3AE91B15987896AC741DA42D28472
SHA-256:	D5E8B1EC255797D5797F36F9B6B81E37D912E2D5E911428EC88CC055764463C0
SHA-512:	6633BD676977EFD456D5363194EE6B4251B33AC86A12FFD24D440242C8C869DB9569D2F5000A09A22BD4828E06CAC4D39A7B641D85B97D472C9DAC36F57D55E
Malicious:	false
Preview:	<#.. .SYNOPSIS..PowerShell Script to Upgrade SQL Server Express 2017+ to 2022....Ensure you run PowerShell as Administrator....Ensure to adjust paths and instance names as per your environment.....1. Backup Databases..Implement backup logic as per your environment & requirement.....2. Verify SQL Server 2017+ is installed..Verify manually or add script logic as per your requirement.....3. Install SQL Server 2022 Express.... .DESCRIPTION.. Will upgrade SQL Express 2017+ to SQL Express 2022.... .NOTES.. Version: 1.3.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. #Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.. ..#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQL8x_to_SQL12x.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	6880
Entropy (8bit):	5.246944638572133
Encrypted:	false
SSDEEP:	192:pHTM4EDdskCPdjMVpDQSczf3cTxEa6gFiXTo:pIsNPhgpDliIEav
MD5:	EBA62744DFE66991433BAF7FC0BAEBF5
SHA1:	137385A79E897DF5C0D0FC6AEFEDDDB8CC4385D7
SHA-256:	9AD9453564BABC5EB58CB18243E094C5CB8BA753009724393517185E1AFDE7BB
SHA-512:	54CAEC1376B3CDEF75CF75B22CF924DCA1EA663BB6203DB85EA6D15916D79E85C0421765C614D2161686384498DA9DB2885C57C0E6D099DA6E2D8C76E168DC
Malicious:	false
Preview:	<#.. .SYNOPSIS..PowerShell Script to Upgrade SQL Server Express 2008 SP4 to 2012 SP4....Ensure you run PowerShell as Administrator....Ensure to adjust paths and instance names as per your environment.....1. Backup Databases..Implement backup logic as per your environment & requirement.....2. Verify SQL Server 2008 SP4 is installed..Verify manually or add script logic as per your requirement.....3. Install SQL Server 2012 Express SP4.... .DESCRIPTION.. Will upgrade SQL Express 2008 SP4 to SQL Express 2012 SP4.... .NOTES.. Version: 1.3.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. #Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQL8x_to_SQL8xSP4.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	6869
Entropy (8bit):	5.271716332455319
Encrypted:	false
SSDEEP:	192:SmCd4EDd9yCGdjMVpD5SczW3bTR79IgFJXC/:StBGhgpDAiT
MD5:	1A8612F6E5EF271B6308386FAFCAC2FC
SHA1:	C12001B6714417A25E9D33CBB5E0E3E28FC0C8AB
SHA-256:	A02286A6251AA589C3A01D14DAD72E6A973C5CE3247775ACBDF0A0002702202C
SHA-512:	1F933E8BB7A0DC707820275A3A00DFBF065CF4583A0D20D5978100D5CDD3F1FC64FC844F822CF441C32BDD912667FBF545534BBBEB18BF66F30420D473E29F7
Malicious:	false
Preview:	<#.. .SYNOPSIS..PowerShell Script to Upgrade SQL Server Express 2008 to 2008 SP4....Ensure you run PowerShell as Administrator....Ensure to adjust paths and instance names as per your environment.....1. Backup Databases..Implement backup logic as per your environment & requirement.....2. Verify SQL Server 2008 is installed..Verify manually or add script logic as per your requirement.....3. Install SQL Server 2008 Express SP4.... .DESCRIPTION.. Will upgrade SQL Express 2008 to SQL Express 2008 SP4.... .NOTES.. Version: 1.3.. Author: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. #Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPo

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQLExpress_Main_2022_Upgrade.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	10147
Entropy (8bit):	5.151791839049951

Encrypted:	false
SSDEEP:	192:5icEOrSM54EBd7MCpNOvO07BBkNOh50LspMzxaSa9/Oz0/Xu/yc0/W5/G3p:wnYDNmnH5qPoyU
MD5:	1ADD9F6985014CB6D580776FB1ED7184
SHA1:	6037CE1867FDAECD5AB96619330C7056B81A667E
SHA-256:	F396B1B7C0812275DC5A3F9F46881FFB8D1BA9A9AC356AFCDC9571E8F1911D61
SHA-512:	87E8B62FBD2E2B30DE4A7E069C2EF79A26E4DECC08F2479B1978F1446BF471B94BF5879FE977DCFD18DC2B662F9C7624CDCB67587A8A7E2D4B49EDBD757405 62
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Backup and Store A2E DB.. Find SQL Express Version and upgrade accordingly.. Upgrades SQL Express 8x to SQL Express 2022.. Note* SQL 2008 must be at least SP4 to update to SQL Express 2012.. Note* SQL Express 2012 SP4 last version for x86. Must export and import DB into fresh SQL Express 2022.... .DESCRIPTION.. .... .NOTES.. Version: 1.1.. Author: DidItBetter Software.... #>.....if (-NOT ([Securi ty.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....#Logging..Start-Transcript -Path

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\SQL_Upgrade_Files\SQL_Management_Studio_Quiet_Install.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3008
Entropy (8bit):	5.120422215233596
Encrypted:	false
SSDEEP:	48:4WM+YmPROBkuXjXzag4fvSf8/kyb0X/x3EpWoDLgmtQ7+7lt0c/EqzCwZu4M:7MlmPEBdznf8cyb0GtLgwQ7+7liPt
MD5:	D1BC3C992B5D78090C375480B7BE9D3B
SHA1:	7FE5F2FBC111E6B863326F74D24438169CA680EC
SHA-256:	53E87C98740D6CF268B641B55133958EA6A729DCEB04E71FAB13710B3861D4F0
SHA-512:	325BD84478EE91C5C39A1A92469853DC6084B42CAF079766B0130866653507456DD01CA48F7CCBC9D3CFFF5938B1800463B3EA78123D557FD3FCCB149E314CD
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Downloads and Silently Installs SQL Managament Studio 19x.... .DESCRIPTION.. .... .NOTES.. Version: 1.1.. Aut hor: DidItBetter Software.... #>.....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Pr incipal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Logging..Start-Transcript -Path "C:\Program Files (x86)\DidItBette rSoftware\Support\A2E_PowerShell_log.txt" -Append....# Script #....#Test for HTTPS Access..Write-Host "Testing for HTTPS Connectivity"....try {.. $wresponse = Invoke-WebRequest -Uri https://s3.amazonaws.com/dl.diditbetter.com -UseBasicParsing.. if ($wresponse.StatusCode -eq 200) {.. Write-Output

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Scheduled_Update_Add2Exchange.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	6631
Entropy (8bit):	5.235810758535446
Encrypted:	false
SSDEEP:	96:aUKXYYmPEBhJ77gEmYBF/A54HofObcV7755JG9ZZ07xz0aDQrQ:hY4EBhJzf/A6HHAt0rQ
MD5:	AFB9AADF777A7A19E1AE27D5FD22514F
SHA1:	0C1A6A7F0E6D22BC7A635C266868682D7DDEEF1A
SHA-256:	DD988CFD11109E1E7875D41607916EC30B73F4DDDF310515BD15E762A36058D8
SHA-512:	45C3B59D82600DFA5FC3A970C4EB88850AA38D40C05930D8F3ABF8E000AB4384A34BD2B6F26ABB0ECDDE45A982A9F109E49235CD874FA33BA41495A0287864 C
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Scheduled Task to automatically upgrade Add2Exchange to the newest version.... .DESCRIPTION.. Downloads from S3.. Upgr ades Add2Exchange to latest build.. Sets password for Add2Exchange Service.. Starts Add2Exchange Service after succesfull install.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... To run this as a scheduled task open CMD prompt and type in: schtasks /run /tn "Scheduled Update Add2Exchange" .. Note* the task must be already created before running this in CMD.. #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.Win dowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Office365_Pro_Retailx64_Configuration.xml

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1023
Entropy (8bit):	5.202613438368244
Encrypted:	false
SSDEEP:	24:OkfEslTC6jycWuLcWlfAcWiLcWbFS8httxkB:9fE+e6jyctLcrcjLcqDDtyB

MD5:	BC70B4D7C9C7053F4C30FC1721A67D63
SHA1:	D9E574805F4018C7CC25C2AA97DC56DA3E0B5044
SHA-256:	794E2365F2E580F669BAD988064606F814A1EDDDB7F865C3D291AAF15AE1EF0D
SHA-512:	6AF3A9F2428698FB935894470BF7F0AC8BEAE66936DF3E6B5994A96E62972AD693763892B4FF58CE322E8275C135F4E2FE3A31CBA7A87AC15DA129B0CB24256
Malicious:	false
Preview:	<Configuration ID="0ed28122-0109-4692-886e-6c4b754f4025">.. <Add OfficeClientEdition="64" Channel="Broad" ForceUpgrade="TRUE">.. <Product ID="O365 ProPlusRetail">.. <Language ID="MatchOS" />.. <ExcludeApp ID="Access" />.. <ExcludeApp ID="Excel" />.. <ExcludeApp ID="Groove" />.. <Ex cludeApp ID="Lync" />.. <ExcludeApp ID="OneDrive" />.. <ExcludeApp ID="OneNote" />.. <ExcludeApp ID="PowerPoint" />.. <ExcludeApp ID="Publisher" />.. <ExcludeApp ID="Word" />.. <ExcludeApp ID="Teams" />.. </Product>.. </Add>.. <Property Name="SharedComputerLicensing" Value="0" />.. <Property N ame="PinIconsToTaskbar" Value="TRUE" />.. <Property Name="SCLCacheOverride" Value="0" />.. <Property Name="AUTOACTIVATE" Value="FALSE" />.. <Updates Enabled="TRUE" />.. <AppSettings>.. <User Value="0" Name="runosc" Id="L_TurnOffOutlookSocialConnector" App="outlk16" Type="REG_DWORD" Key="softw are\microsoft\office\outlook\socialconnector" />.. </AppSett

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Office365_Pro_Retailx86_Configuration.xml

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1023
Entropy (8bit):	5.2041868894674
Encrypted:	false
SSDEEP:	24:OTfEsITC6jycWuLcWIfAcWiLcWbFS8httxkB:ufE+e6jyctLcrcjLcqDDtyB
MD5:	6C49E64FFF25A2225546976F7A9BE5F6
SHA1:	6CC15D048275904F2E8D7AFC1F7789750FC6365E
SHA-256:	B52A9402BB73233A077BC2437228A26AEEB9C8F53FE3E9147209A09A9D5A833F
SHA-512:	FDCF646EA8D896ACA2EF3AF156D5403D509EAA06580A87854BAA5B2D0353B4483F62EA60F128338020E8039A95A3DC3FC85A45ED4A2539929A0A3B366A0F7B9 9
Malicious:	false
Preview:	<Configuration ID="0ed28122-0109-4692-886e-6c4b754f4025">.. <Add OfficeClientEdition="32" Channel="Broad" ForceUpgrade="TRUE">.. <Product ID="O365 ProPlusRetail">.. <Language ID="MatchOS" />.. <ExcludeApp ID="Access" />.. <ExcludeApp ID="Excel" />.. <ExcludeApp ID="Groove" />.. <Ex cludeApp ID="Lync" />.. <ExcludeApp ID="OneDrive" />.. <ExcludeApp ID="OneNote" />.. <ExcludeApp ID="PowerPoint" />.. <ExcludeApp ID="Publisher" />.. <ExcludeApp ID="Word" />.. <ExcludeApp ID="Teams" />.. </Product>.. </Add>.. <Property Name="SharedComputerLicensing" Value="0" />.. <Property N ame="PinIconsToTaskbar" Value="TRUE" />.. <Property Name="SCLCacheOverride" Value="0" />.. <Property Name="AUTOACTIVATE" Value="FALSE" />.. <Updates Enabled="TRUE" />.. <AppSettings>.. <User Value="0" Name="runosc" Id="L_TurnOffOutlookSocialConnector" App="outlk16" Type="REG_DWORD" Key="softw are\microsoft\office\outlook\socialconnector" />.. </AppSett

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Pro_Retailx64.cmd

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.572765012132931
Encrypted:	false
SSDEEP:	3:Pg4QQ6/QIK6Wde8UMeKJ:PVQQFKWIU2
MD5:	E49E7FD101C66A32558FF27564234222
SHA1:	671A4BBE57BB7C9E872693DFA4CDC967D4329A93
SHA-256:	72507222065118F1D879128E8E98C633AFA6C21275CB9246F5AAC18041A1FDBF
SHA-512:	1A7CE80BE39B2B2CF38B1687A0CD6E9F318C216F6562F1170283835360B8AFE053D72CAD6714F4073927932BFFCD3EDDFCAB09962A6C145BF5F34C1CBD261E B
Malicious:	false
Preview:	setup.exe /configure Office365_Pro_Retailx64_Configuration.xml

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Pro_Retailx86.cmd

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.572765012132931
Encrypted:	false
SSDEEP:	3:Pg4QQ6/QIK6WdoMeKJ:PVQQFKWi2
MD5:	8D16D2E6750AE5217ADBBAC538E6E89E
SHA1:	06126FF482AB5F91E32315DE94ECE2F39533C1BF
SHA-256:	FFB180B7837FAB58A39779694E3025F98A0AE6B747B3A84BCB96BBA59486C5F7

SHA-512:	D17FC93E05CAF4FB938EC1CE9A18793610A2B2381D020227613117031E238B0E6F8A1957EC1000BDD7D2CF2587C3DD1FD4C2CD93010B70686FDF46747BE50B2C
Malicious:	false
Preview:	setup.exe /configure Office365_Pro_Retailx86_Configuration.xml

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Setup Files\setup.exe

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5169440
Entropy (8bit):	6.649944627880774
Encrypted:	false
SSDEEP:	98304:vqihTvjtEh2N5LQhyddG4THBZoJG3QBMxvble/bsTwY2h3:TpvE8dgq3oJG3QBMxBlW3
MD5:	B374FA0E7E34B9CE9C142FE80E1EFADE
SHA1:	2537F4523B12E9801F2ACB8FE38D5D725A56A61D
SHA-256:	A87105965530799BABBB71A1FD52DBD7CDDEE71C40E2C37576235D156FF02027
SHA-512:	8F5FF73932568006C38B9E1BB8DAABF0DC6E419FC1E6D96159FB1234439B8AB9B283D617540CDC5860538AFFEA89BA0A553F4CCF2B9F1949D9E907BA56C2F74C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....0.....!..L.!This program cannot be run in DOS mode....$.....Gc.-...~...~...~..'~...~..%~...~..$~#..~lg.....~lg..+..~lg.....~...~...~...~...~fd.....~fd.....~fd.....~fd.....~...~)..~.d.....~.d.....~.d)~...~..A~...~.d.....~Rich...~.....PE..L...r..[.....".....l+..2#.....#.....+...@.....O.....O...@.....8b?.....A.....N. ?...`K..<....:.8.....:.....@.....+.8....M?.....text....k+.....l+..... ..`.rdata.....+.....p+.....@..@.data.....?..H...x?.....@....rsrc.....A.....@.....@..@.reloc...<...`K..>...dJ.....@..B.....

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Shell_Into_Exchange.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	7051
Entropy (8bit):	4.675718132414485
Encrypted:	false
SSDEEP:	96:iCmPEBdzcsNZg5MVzQWgM4cRpPOY6WIQK84cRpfOY6Wi:54EBdQshqkl6fUV65
MD5:	4ABCE57C7D70986A012F11683C23D47F
SHA1:	4B7CD4E02EDBE9D04A489196A0465A228A5DD39D
SHA-256:	5507006FEDCC5410CAB7C9DC33C0B52E6E919697DD46EEC2F3733E3803887CFD
SHA-512:	A879AA334B113E7A6A64F1A936871C15E79D32DA37EEA257D867F38C762E5263E8124F6C4FE3AE219BEB8719C2BBB7C78C69740E7D648F195D864A07359FCBB6
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Shell into Exchange.... .DESCRIPTION.. Allows for login to Exchange or Office 365 with ability to enter commands manually..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}" -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Support"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "Support Directory Exists...Resuming"..}..Else {.. New-Item -ItemType directory -Path "C:\Program Files (x86)\DidItBetterSoftware\Support"..}....Start-Transcript -Path "C:\Pr

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Shell_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with very long lines (355), with CRLF line terminators
Category:	dropped
Size (bytes):	36559
Entropy (8bit):	4.503630667237573
Encrypted:	false
SSDEEP:	192:zo4EBdHRhO9keHSowqzSZrTJN7nd9pdYkyO:ElkeHSowqGZ7PYkF
MD5:	BF7B956A983D4C2B772F143AC437F401
SHA1:	BB5902AAF9844CC9C0786884F8B35D052BE13B4A
SHA-256:	51250044F351B81A1A8E38C1EFD47DCB99312DAAAAE15F1A2CA856E0D0E42E73
SHA-512:	4E980628CDA60EC0F91CD4C78B1C8D1D651FBBCD29702A205721B26BBE45B43342BE932DD37C5B2D498ECFD73E511A7EA982C3CBB326A629D64F34A725DA4D7
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Shell Permissions.... .DESCRIPTION.. Automatically logs into the desired on premise exchange or Office 365 and applies permissions.. uses bit-locked creds from timed permission setup..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass....#Logging..$TestPath = "C:\Program Files (x86)\DidItBetterSoftware\Support"..if ($(Try { Test-Path $TestPath.trim() } Catch { $false })) {.... Write-Host "Support Directory Exists...Resuming"..}..Else {.. New-Item -ItemType directory -Path "C:\Program Files (x

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\2010-2019_All_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2313
Entropy (8bit):	5.206475437016567
Encrypted:	false
SSDEEP:	48:9YmPROBkaheuGuLiuZuTEIltsEjA4HcYA4Zx:qmPEBV7JpoTaJjYY9x
MD5:	A119485189BCC14AC82C12ADCA54E81E
SHA1:	5CFE9A212D000E8F367B83B1F39474B99F89CD55
SHA-256:	25CA6D42AEE88E873C065741F37959D148A07A41CCC8B393ACB05C7B9F3729CB
SHA-512:	C6FAB52DDC71FAF46D9F260ADA73C5D22E2880068E3319F07106838A86EC2484AF42BEE4383C5708F1A37181D89D4EFF082EB8D158999DEC6BB08E8F9269246
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit.. }.. .. .. #Execution Policy.. .. Set-ExecutionPolicy -ExecutionPolicy Bypass.. [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12.... #Variables.. .. $Exchangename = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Name.txt".. $ServiceAccount = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Sync_Account_Name.txt".. $Username = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Admin.txt".. $Password = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Pass.txt" | convertto-securestring.

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\2010-2019_Dist_List_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2309
Entropy (8bit):	5.27046054524564
Encrypted:	false
SSDEEP:	48:9YmPROBk6PYUuWuLCuJuTnujY1tkD7PzNIFMGIA4H9r:qmPEBtPYX5p4Tuy8bS2P5r
MD5:	65AEF2EBB5A702F05BDDB39426D22E9E
SHA1:	A40DB715731183703E8E0D9B8D883D039E64D1C0
SHA-256:	A57544B50D040A836A9AFA3334EC7820AD4A11CE3B1E22563BD68183296B1802
SHA-512:	FF41E94E3DD9E40D731F2EB19D2CB978D2AA2564841F42D3E272981EDCE0CC061697FD55D49BAA3E9D6E5B11200DFEE9DC4246089FAD05C577C49D86C6E1E33
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Variables....$Exchangename = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Name.txt"..$ServiceAccount = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Sync_Account_Name.txt"..$Username = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Admin.txt"..$Password = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Pass.txt" \| convertto-securestring..$Groups = G

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\2010-2019_Dynamic_Distribution.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3242
Entropy (8bit):	5.184235576844559
Encrypted:	false
SSDEEP:	48:9YmPROBk6PYUuguJuTguWux1tkfnAH7lzYtn3BKz1w:qmPEBtPYXD4TD5n57m6xKz1w
MD5:	399F572DA4C7F58117067DD1D70AB422
SHA1:	03CC2AFDF3AF84E147F0E0A934B094D32FB0460E
SHA-256:	BB60CC3AB32A798ABAD83A52224C2A665B43FD0B389B5FEF8FD146BB8ECFC281
SHA-512:	90576BDD350BEF61E341B50FC59CE81C1C298C97CDA65E1CCD160044B976A848681E82C3CF7C89C15F4DE86DAFD8BA583253328E135EF2B65C7A7D853E0170A
Malicious:	false

Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Variables....$Exchangename = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Exchange_Server_Name.txt"..$Username = Get-Content "C:\Program Files (x86)\DidI tBetterSoftware\Add2Exchange Creds\Exchange_Server_Admin.txt"..$Password = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\ Exchange_Server_Pass.txt" | convertto-securestring..$DynamicDG1 = Get-Content "C:\Program Files (x86)\DidItBetterSoftware\Add2Exchange Creds\Dynamic_N ame.txt"..$StaticDG1 = Get-Con

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\Office365_All_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2681
Entropy (8bit):	5.206204413905134
Encrypted:	false
SSDEEP:	48:9YmPROBk642pHCZMTruLCuuu+EY7A4H29:qmPEBtKMTipx+ti9
MD5:	4CEE73D454FF52AD206F6779B8C1B1C2
SHA1:	2AFF775DEBB685870CB1027DFB629709134C78AD
SHA-256:	CFFE62C1DD72BB82A9B1FF47092FD096B2A5DF219778CDA5D9D0B61B86E72E6B
SHA-512:	00727409C9A4EA398854BAA6398D04C404E40B8B69AB940DAC26789F708F2D0223C27A55FF53FC372B5B1D7DB57BB6967647B8CD7DECD97C4C66BB02418CB4 D
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Check for MS Online Mod ule..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2)

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\Office365_Dist_List_Permissions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2936
Entropy (8bit):	5.226696749733595
Encrypted:	false
SSDEEP:	48:9YmPROBk642pHCZMCruLCuuu+nujYs7PzNIFMGIA4HyKx:qmPEBtKMCipx+u9bS2PmKx
MD5:	29DCE03F380B4119D910F6916C83E553
SHA1:	C094CFF3C3D9B460F44F7CF61CA78C8D1F84122D
SHA-256:	3B92B4559CBB46C25330E2D1272C1946928A896B0FEC503A2C2624C7E35509F7
SHA-512:	C14CB1A123CAC0DBB3306A193C5BADAD07E088565383111F1265FC9AA8B5E0BD5A1B94942FF8F7C4C5A9D44E3C250BFFD681AAEF70A5465690A8C8002455F6 9F
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Check for MS Online Mod ule..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2)

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\Office365_Dynamic_Distribution.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3867
Entropy (8bit):	5.150671684787593
Encrypted:	false
SSDEEP:	48:9YmPROBk642pHCZMCpuuu+8ueuuYWNja7IzYtn8UQprG:qmPEBtKMCYx+fBia7m689prG
MD5:	9DB45E661D4F1819D5C2119BA8EBE6F7
SHA1:	43F8E5466B03431EE886981A1A6D15AC4CBF09C4
SHA-256:	91B84050C3505A65F63C4084DE97CEB183BB2131C5ECE05E1FD5B2C9385A5271
SHA-512:	6A8968A8B70BCD6DA01BDD495D2BE1A7F4F2B2620CA216EB123E524F862641860711D3A048029853BF8609C2ED2A96F9586938A184E3E0BF3D8D2C32D976B93
Malicious:	false

Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}.....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass..[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12....# Script #....#Check for MS Online Module..Write-Host "Checking for Exhange Online Module"....IF (Get-Module -ListAvailable -Name ExchangeOnlineManagement) {.. Write-Host "Exchange Online Module Exists".... $InstalledEXOv2 = ((Get-Module -Name ExchangeOnlineManagement -ListAvailable).Version | Sort-Object -Descending | Select-Object -First 1).ToString().... $LatestEXOv2 = (Find-Module -Name ExchangeOnlineManagement).Version.ToString().... [PSCustomObject]@{.. Match = If ($InstalledEXOv2 -eq $LatestEXOv2)

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\Stand_Alone_DyanmicDistList_Task.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1182
Entropy (8bit):	5.177298437958451
Encrypted:	false
SSDEEP:	24:9ELm7LR6LPk1ophAI6PoqGba5KNZDaNvmLbPXuq7Whz:9YmPROsEDFdAzuX
MD5:	E7429B9BC39E9217F0FB503DE41E1364
SHA1:	0608BB8B293A11F58EEB8CAA322CAF670CD48EFA
SHA-256:	6C696EF6E3D94FE2712B3063C7A52C6618A0D346C0B22718572FE7DB2A178885
SHA-512:	DB305B546B58D66809CC7F79389CE1D637C1EDDFB490162527C95752A306F2E616CB264B03719A40297773CE1A79D960B453F6EFA6B3C9486648705D351D56B5
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass.....# Script #..# Report Correct File Path of DynamicDistribution List File..Write-Host "Creating Task".. $Repeater = (New-TimeSpan -Minutes 720).. $Duration = ([timeSpan]::maxvalue).. $Trigger = New-JobTrigger -Once -At (Get-Date).AddMinutes(1) -RepetitionInterval $Repeater -RepetitionDuration $Duration.. $Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -WorkingDirectory $Location -Argument '-NoProfile -WindowStyle Hidden -Executionpolicy Bypass -file "ENTER FILE PATH HERE"'.. Register-ScheduledTask -Action $Action -RunLevel Highest -Trigger $Trigger -TaskName "Add2Exchange Permissions" -Descrip

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed Permissions\Stand_Alone_Dynamic_Distribution_List.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2376
Entropy (8bit):	5.091813731955432
Encrypted:	false
SSDEEP:	48:9YmPROBkH+yF0TveJjpnAH7IzYtn3BKzi:qmPEBl6KeJjs7m6xKzi
MD5:	CBC1624883A282B70B867D25B380EE1C
SHA1:	519E9B90F6558C1B507A1B71F9706B9400FE1E40
SHA-256:	0470A94170B0407E9C8AF85F2292EA767A424A82686E1991E28F320A2A325809
SHA-512:	16E60FA701564121144AD3217F7F1689C39FB9D368067256C08D4CF0E57CAFEB75B65F2F32FC58AF5119A62D6F1B253B5E18210B4871EAE48CB8E93EA5F0245D
Malicious:	false
Preview:	if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass....# Service Stop #..Get-Service -ComputerName "TYPE COMPUTER NAME HERE" -Name "Add2Exchange Service" | Stop-Service -Verbose -ErrorAction Stop..Start-Sleep -s 30..Get-Service -ComputerName "TYPE COMPUTER NAME HERE" -Name "Add2Exchange Agent" | Stop-Service -Verbose..Start-Sleep -s 10....# Script #..Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn;..Set-ADServerSettings -ViewEntireForest $true.. .. #Variables..# Fill Out Dynamic and Statis Distribution Groups Below....$DynamicDG = @("Dynamic DL HERE", "Dynamic DL HERE")..$StaticDG = @("Static DL HERE", "Static DL HERE")....for ($i = 0;

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Timed_A2E_SQL_Backup.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Non-ISO extended-ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4303
Entropy (8bit):	5.198975556588784
Encrypted:	false
SSDEEP:	48:o+gYmPROBkuU69eKr3IHvD5AMgihSKD6dgmdW7CXdWCnvlCVg7SCjSpcMQJtI6oT:oCmPEBdUGwvsiL7FC4GmL2MuozKtG
MD5:	3AAAC6808F523B20E401258345F64C9B
SHA1:	D69BE6F4135500FC2E9312F3F5091FDA06CDB046
SHA-256:	E54C2AB3CA3FAD2491C022C763744D6F82998734F616801F049B21266029BE1D
SHA-512:	0DD462BD8D984B6BACC6635611D128D4AE024D689E5278266B640CEA1204749DED2124CC6589D110637907A2726F20720DE283786C25D746D0C733E29F5D79F
Malicious:	false

Preview:	<#.. .SYNOPSIS.. Timed A2E SQL Backup.... .DESCRIPTION.. This is a part of a scheduled task to run and backup A2E SQl DB every 3 days.. 5 version retention by default.... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Variables..$Install = Get-ItemPropertyValue -Path "HKLM:\SOFTWARE\WOW6432Node\OpenDoor Software.\Add2Exchange" -Name "InstallLocation" -ErrorAct ion SilentlyContinue #Current Add2Exchange Installation Path..$CurrentDB = $Install + 'Database\' #Current Database Location..$BackupDirs = Get-Conten

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\Windows_Defender_Exclusions.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ISO-8859 text, with CRLF line terminators
Category:	dropped
Size (bytes):	2815
Entropy (8bit):	5.2554300122995485
Encrypted:	false
SSDEEP:	48:wli8k8z+N+8Y8zK+gYmPROhE5N/ZVgo9ei2COW818zW1NR8t8zf/xcXWH9enxoSa:halKCmPEhgVJAhfYxoSroz
MD5:	65BAF2C4AECB3C31BD9F5D991FB5F666
SHA1:	7AAC1911A4A0E2235AD4BAC1F8D03DDFC863F4C5
SHA-256:	65DB9ADCFD894401F42E618FCD973498F2D86563BF7B12687A9AFCC0B3BF65E4
SHA-512:	6139BAC47DEA096CD4E6F8AAEFF5A77ABBEE42D1BFE71E1E646534C295262EC96119AF971132920B45731ACC240B42418244380A82C783E0767F2D7CD0D24B(3
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Windows Defender Exclusions.... .DESCRIPTION.. Excludes the below from windows defender live scanning.. "Program Files (x86)\OpenDoor Software.".. "Program Files (x86)\Microsoft SQL Server".. "Program Files\Microsoft SQL Server".. "Program Files (x86)\DidItBetterSoft ware".. "zLibrary".. "Program Files (x86)\Microsoft Office".. "C:\Users\zadd2exchange\AppData".... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.Window sBuiltInRole]::Administrator)) {.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File", ('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. e xit..}....#Execution Policy....Set-ExecutionPolicy -ExecutionPolicy Bypass -Force....#Logging..Start-Transcript -Path "C:\Program

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Setup\shell.ps1

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	786
Entropy (8bit):	5.003777918597954
Encrypted:	false
SSDEEP:	24:V5U4J2+rcELm7LR6LPk1ophAl6PoPhjJyFhNxT:7E+gYmPROsEDUJs5
MD5:	0C3D59CF2897ACE0354138628A349F9A
SHA1:	D3CD0F829B6C162C77C68FFC137E89392E573410
SHA-256:	E81BF291B9B93BDD31AAB066D2E4078C3C2D9EC8A5BFC802DD910C59F47361DD
SHA-512:	498A6702F9CFF747AB1986CB1CB5AB61D11979DDF8C2892FA2C07645FFD883A0048C7DC132C0B22964734495769258 3B292D1E47DDD82658B0FED116AF53219(
Malicious:	false
Preview:	<#.. .SYNOPSIS.. Shell.... .DESCRIPTION.. Simple open another PS session to shell into Exchange of Office365.. Calls another powershell file "Shell into Exchange"..... .NOTES.. Version: 3.2023.. Author: DidItBetter Software.... #>....if (-NOT ([Security.Principal.WindowsPrincipal] [Se curity.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator))..{.. # Relaunch as an elevated process:.. Start-Process powershell.exe "-File",('"{0}"' -f $MyInvocation.MyCommand.Path) -Verb RunAs.. exit..}....#Execution Policy..Set-ExecutionPolicy -ExecutionPolicy Bypass.....# Script #..Powershell.exe -noexit ".\Shell_Into_Exchange.ps1" -noprofile....# End Scripting..

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Tools\Logging\gollevel.xtx

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:xJ8n:xun
MD5:	FB5B87D7E7127C6CCBB0D47B99C98629
SHA1:	D0E38F05930EF0AC54BF5A2C555B5013BF7B8145
SHA-256:	120C7DC65B2424AAC3D64B06D0F28C1CFB41553A0294C99DFCBC6B750428430B
SHA-512:	9F39FAEAC437F3A6FC7E32818209CE19E0441B389C6028FDD706B64417EE8EFCF36963A08A1B6764680E762A40716C6E833EE8FBE97F33D07CD6BA68AD164C3 9
Malicious:	false
Preview:	Level:9

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Tools\Mapi\ExchangeMapiCdo.MSI	
Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 5.2, MSI Installer, Code page: 1252, Title: Installation Database, Subject: Messaging API and Collaboration Data Objects 1.2.1 v6.5.8320.0, Author: Microsoft, Keywords: Installer, Template: Intel;1033, Revision Number: {EB06CAF7-FF9E-4e70-B2DC-20D0B3E4A188}, Create Time/Date: Mon Apr 29 10:13:53 2013, Last Saved Time/Date: Mon Apr 29 10:13:53 2013, Number of Pages: 200, Number of Words: 2, Name of Creating Application: Windows Installer XML (candle/light), Security: 1
Category:	dropped
Size (bytes):	3569152
Entropy (8bit):	6.968260863030964
Encrypted:	false
SSDEEP:	49152:Ozi7eSMsESiOtGc5DUNmj6lpDrfb0YZUafrtxjkkwuh+GQGY:tllEllGcyNy6lpDrfQYZ7Bxj1wpGQ
MD5:	1C0E9FD7CB73D8E40802FA2F535B2D96
SHA1:	F109F0E751D0B358C9D5DEE1322738609E07EA2E
SHA-256:	40480D120D9A4349716471B75015FFC08313B541A8E303E326F2A2809EA98731
SHA-512:	EEEEC835D3B29C0E7A5147A2D57A289584DF81070DE90569A0DA6A508EE7CB739CDA5737BB394B6370A0B990440A663B1FD0CCA973F52213FD00445CDB3843 2
Malicious:	false
Preview:	.....>.....7.....=.....i...j.../...0...1...2...3...4...5...6...7...8...9..... ....+..... ...!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?. ..@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s... t...u...v...w...x...y...z...

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Tools\OutlookTools\Autodiscover\365autodiscoverOutlook13.reg	
Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Windows Registry text (Win2K or above)
Category:	dropped
Size (bytes):	673
Entropy (8bit):	5.200084512777063
Encrypted:	false
SSDEEP:	12:jBJ0SK0Z83rQbDIYLRfRRfJ/bjr83rQrKfAsGKMAsk8dAskKPysAskKObsAsOKPK:jBJtZ8bQbDv7P78bQrKf1S1ki1kKf1kT
MD5:	6650B0C072434405DF42D91C81A1573C
SHA1:	D5EF1E3A4408F8FBDC0A514C1F411627FCEA1F98
SHA-256:	D5157FAE52FF0A7CF3D0BFC204EA1674AA117267241B95F1FF90A87F2DA2F612
SHA-512:	83241CAEDB38CC1BCB1DC5FE37984F92E879C8FFACC458DC95947462CE216789F756642CBA99B622289800A45AA8CE3F022ED36E9663EE26CA8B5F31F00096 8
Malicious:	false
Preview:	Windows Registry Editor Version 5.00....[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\AutoDiscover].."ExcludeScpLookup"=dword:00000000.."E xcludeHttpsAutodiscoverDomain"=dword:00000001.."ExcludeHttpsRootDomain"=dword:00000001.."ExcludeSrvLookup"=dword:00000000.."ExcludeHttpRedirect"=dword :00000000.."ExcludeSrvRecord"=dword:00000000....[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\AutoDiscover\RedirectServers].."autodiscover- s.outlook.com"=hex(0):.."autodiscover.hotmail.com"=hex(0):.."autodiscover-s.partner.outlook.cn"=hex(0):.."autodiscover-s.outlook.de"=hex(0):.."autodiscover-s.office365.u s"=hex(0):.."autodiscover.THEIR_DOMAIN.com"=hex(0):..

C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903\Tools\OutlookTools\Autodiscover\365autodiscoverOutlook16.reg	
Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	Windows Registry text (Win2K or above)
Category:	dropped
Size (bytes):	673
Entropy (8bit):	5.201934605641604
Encrypted:	false
SSDEEP:	12:jBJ0SK0Z8PbDIYLRfRRfJ/bjr8PrKfAsGKMAsk8dAskKPysAskKObsAsOKPAv:jBJtZ8PbDv7P78PrKf1S1ki1kKf1kKY1
MD5:	98DD72DEF80AB5D47318F76A726EAFBF
SHA1:	A596F1DC0D4060B90872ABD75C5AA587B55469D6
SHA-256:	224D9957C0368840C9677FAB790B7978AD85F8CBE1F4C344853D4ABB2E19FC8E
SHA-512:	F95D02AF1CD45FC4E6365C290412CD4BBA9B03A44905D33659CFB7B1D34262946DF6589617581D69F78E39BDB9B989017FF3E22E41DB212359DEF138FA937792
Malicious:	false
Preview:	Windows Registry Editor Version 5.00....[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\AutoDiscover].."ExcludeScpLookup"=dword:00000000.."E xcludeHttpsAutodiscoverDomain"=dword:00000001.."ExcludeHttpsRootDomain"=dword:00000001.."ExcludeSrvLookup"=dword:00000000.."ExcludeHttpRedirect"=dword :00000000.."ExcludeSrvRecord"=dword:00000000....[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\AutoDiscover\RedirectServers].."autodiscover- s.outlook.com"=hex(0):.."autodiscover.hotmail.com"=hex(0):.."autodiscover-s.partner.outlook.cn"=hex(0):.."autodiscover-s.outlook.de"=hex(0):.."autodiscover-s.office365.u s"=hex(0):.."autodiscover.THEIR_DOMAIN.com"=hex(0):..

\Device\ConDrv

Process:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	9011
Entropy (8bit):	5.090114603797306
Encrypted:	false
SSDEEP:	96:e5JV1qFpLMKTjVEQqoheUe68AX313tBA73pAC6kvDDM:edQqoheFOIbQ
MD5:	D2AE156D41D73955EF95375E429E5B8A
SHA1:	42DF0552AE25A3C214CDB14B2E26DAF136CB2820
SHA-256:	BE67C2179BF4F732A1F1DDC529F0DEC5BA18728804EDB6EDF889EC5CAB402168
SHA-512:	81AD918486F87C1C42FE54D1CB48A9F34E1F6F3232B6A03BA6AC673C97AE365617135D24BAC5BC02E1151BAC636A171B311633851E3357F02C0E21986913CAE
Malicious:	false
Preview:	..7-Zip SFX 4.65 Copyright (c) 1999-2009 Igor Pavlov 2009-02-03....Processing archive: C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe....Extracting a2e-enterprise.26.3.3677.2903\Setup.zip..Extracting a2e-enterprise.26.3.3677.2903\Add2ExchangeSetup.msi..Extracting a2e-enterprise.26.3.3677.2903\Tools\Mapi\ExchangeMapiCdo.MSI..Extracting a2e-enterprise.26.3.3677.2903\Setup\OSC_Disable.bat..Extracting a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Pro_Retailx64.cmd..Extracting a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Pro_Retailx64.cmd..Extracting a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Pro_Retailx86.cmd..Extracting a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Pro_Retailx86.cmd..Extracting a2e-enterprise.26.3.3677.2903\O365Outlook32\Setup Files\Office365_Pro_Retailx64_Configuration.xml..Extracting a2e-enterprise.26.3.3677.2903\Setup\Setup Files\Office365_Pro_Retailx64_Configuration.xml..Extracting a2e-enterprise.26.3.3677.2903\O365Ou

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.999918044877228
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	a2e-enterprise.26.3.3677.2903.exe
File size:	42'987'850 bytes
MD5:	29c3418978dd57c42c7e9530b3aac3d6
SHA1:	08283dd80f9597fffd5abc3977b21894e9ad962b
SHA256:	22a18e7582631d3d2efae7d691fc20421c7a9693103b6f21a190f664c686b94b
SHA512:	e8ffc68971e23bf040155fec5dc0101730fb729365208a202a101e27c289c55016b8e94ef7eaceb820182372fedd68484165b8e491587cf4b5c5a0ed127fb9b3
SSDEEP:	786432:v/NH38u8rB8LSc8EPX+0m8EKQLFD/uDoWIqIKxMTxv9+vCqJuI:JMwPXjFQZGDo/qFAxVw9b
TLSH:	7B973304B0A08677F1022970B3695BE456BFEAD4AC3A3937761267BA1DB7D0D8633DC1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A..~/F.~/F.~/F.a$F.~/F^b!F.~/F.a%F.~/F.a+F.~/FSvpF.~/F.~.F_~/F^vrF.~/F.X$F.~/F.,.F.~/F..RF.~/F.X%F.~/F.x)F.~/FRich.~/F.....

File Icon

Icon Hash:	b8868baba9aba2d8

Static PE Info

General

Entrypoint:	0x419d2c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x4987F062 [Tue Feb 3 07:21:06 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:	be41dda43b3125c88e27c41d5512c51f

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0041DC68h
push 00419D26h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 20h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
and dword ptr [ebp-04h], 00000000h
push 00000001h
call dword ptr [0041D0DCh]
pop ecx
or dword ptr [00427704h], FFFFFFFFh
or dword ptr [00427708h], FFFFFFFFh
call dword ptr [0041D0E0h]
mov ecx, dword ptr [004256FCh]
mov dword ptr [eax], ecx
call dword ptr [0041D0E4h]
mov ecx, dword ptr [004256F8h]
mov dword ptr [eax], ecx
mov eax, dword ptr [0041D0E8h]
mov eax, dword ptr [eax]
mov dword ptr [00427700h], eax
call 00007FDCB47E441Ah
cmp dword ptr [004233D0h], 00000000h
jne 00007FDCB47E434Eh
push 00419E6Ch
call dword ptr [0041D0ECh]
pop ecx
call 00007FDCB47E43EBh
push 00422050h
push 0042204Ch
call 00007FDCB47E43D6h
mov eax, dword ptr [004256F4h]
mov dword ptr [ebp-28h], eax
lea eax, dword ptr [ebp-28h]
push eax
push dword ptr [004256F0h]
lea eax, dword ptr [ebp-20h]
push eax
lea eax, dword ptr [ebp-2Ch]
push eax
lea eax, dword ptr [ebp-1Ch]
push eax
call dword ptr [0041D0F4h]
push 00422048h
push 00422000h

Instruction
call 00007FDCB47E43A3h

Rich Headers

Programming Language:	• [C++] VS98 (6.0) SP6 build 8804 • [C] VS2008 build 21022 • [ASM] VS2005 build 50727 • [C] VS98 (6.0) SP6 build 8804 • [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	0x21600	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x28000	0x818	.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	0x1d000	0x180	.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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1b102	0x1b200	d4c5d76b946ca36ab9bd5aab6cc41d87	False	0.5753078197004609	data	6.570310815454297	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x4db4	0x4e00	c6b21ccaf0d9ef15381630f9c2f032a4	False	0.30193309294871795	data	4.0571847265275185	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x22000	0x570c	0x1400	e1801865b67dbd9655621941066a71b9	False	0.5072265625	data	4.868264558733701	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x28000	0x818	0xa00	8a01387edd37bf9a125c14f9a1d77f1e	False	0.248828125	data	2.249846752391889	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_ICON	0x283e0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States	0.16532258064516128
RT_ICON	0x286c8	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	United States	0.32094594594594594
RT_GROUP_ICON	0x287f0	0x22	data	English	United States	1.0
RT_VERSION	0x28120	0x2c0	data	English	United States	0.4985795454545454547

Imports

DLL	Import
USER32.dll	CharUpperW, CharNextA, CharUpperA
OLEAUT32.dll	VariantClear, SysFreeString, SysAllocString
MSVCRT.dll	_controlfp, __set_app_type, __p__fmode, __p__commode, _adjust_fdiv, __setusermatherr, _initterm, __getmainargs, __p___initenv, exit, _XcptFilter, _exit, _onexit, __dllonexit, ?terminate@@YAXXZ, ??1type_info@@UAE@XZ, _except_handler3, _beginthreadex, memset, memcpy, fputc, fputs, fflush, fgetc, fclose, _iob, free, malloc, memmove, _purecall, memcmp, _CxxThrowException, __CxxFrameHandler

DLL	Import
KERNEL32.dll	FormatMessageW, InitializeCriticalSection, ResetEvent, SetEvent, CreateEventA, WaitForSingleObject, VirtualFree, VirtualAlloc, DeleteCriticalSection, WaitForMultipleObjects, EnterCriticalSection, LeaveCriticalSection, GetStdHandle, FileTimeToSystemTime, SetEndOfFile, WriteFile, ReadFile, SetFilePointer, GetFileSize, CreateFileA, FindFirstFileW, FindFirstFileA, FindClose, GetFullPathNameW, GetFullPathNameA, lstrlenA, DeleteFileW, GetCommandLineW, SetFileApisToOEM, SetConsoleCtrlHandler, FileTimeToLocalFileTime, GetVersionExA, MultiByteToWideChar, WideCharToMultiByte, GetLastError, AreFileApisANSI, GetModuleFileNameA, GetModuleFileNameW, LocalFree, FormatMessageA, CloseHandle, SetFileTime, CreateFileW, SetLastError, SetFileAttributesA, RemoveDirectoryA, MoveFileA, SetFileAttributesW, RemoveDirectoryW, MoveFileW, CreateDirectoryA, CreateDirectoryW, DeleteFileA

Possible Origin

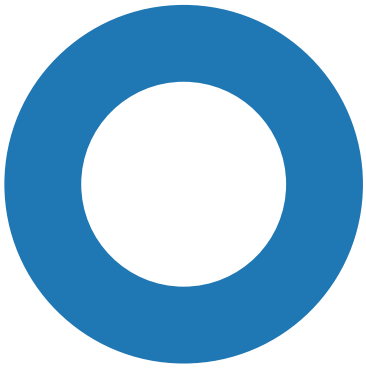
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

a2e-enterprise.26.3.3677.2903.exe
conhost.exe

System Behavior

Analysis Process: a2e-enterprise.26.3.3677.2903.exe PID: 7316, Parent PID: 2580

General

Target ID:	0
Start time:	18:07:45
Start date:	12/03/2024
Path:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\a2e-enterprise.26.3.3677.2903.exe
Imagebase:	0x400000
File size:	42'987'850 bytes

MD5 hash:	29C3418978DD57C42C7E9530B3AAC3D6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: **7324**, Parent PID: **7316**

General

Target ID:	1
Start time:	18:07:45
Start date:	12/03/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly