ID: 877008
Sample Name: Fwd_ Money-Back Fund Recovery Avtal.msg
Cookbook: default.jbs
Time: 14:15:38
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

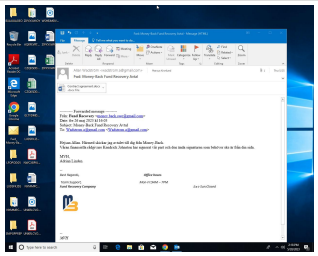
Windows Analysis Report

Fwd_ Money-Back Fund Recovery Avtal.msg

Overview

General Information

Sample Name:	Fwd_ Money-Back Fund Recovery Avtal.msg
Analysis ID:	877008
MD5:	7e6f449c9ca36..
SHA1:	b9f06ca54a6fe…
SHA256:	b611ba8a9097…
Infos:	



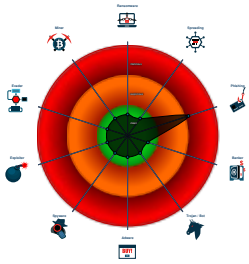
Detection

Score:	21
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- LLM found phishing text in email (M…
- Creates or modifies windows services
- Deletes files inside the Windows fol…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- OUTLOOK.EXE (PID: 4108 cmdline: C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE" /f "C:\Users\user\Desktop\Fwd_ Money-Back Fund Recovery Avtal.msg MD5: 7DD935BA9B57D9D7EFF63C67653E70B5)
- **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

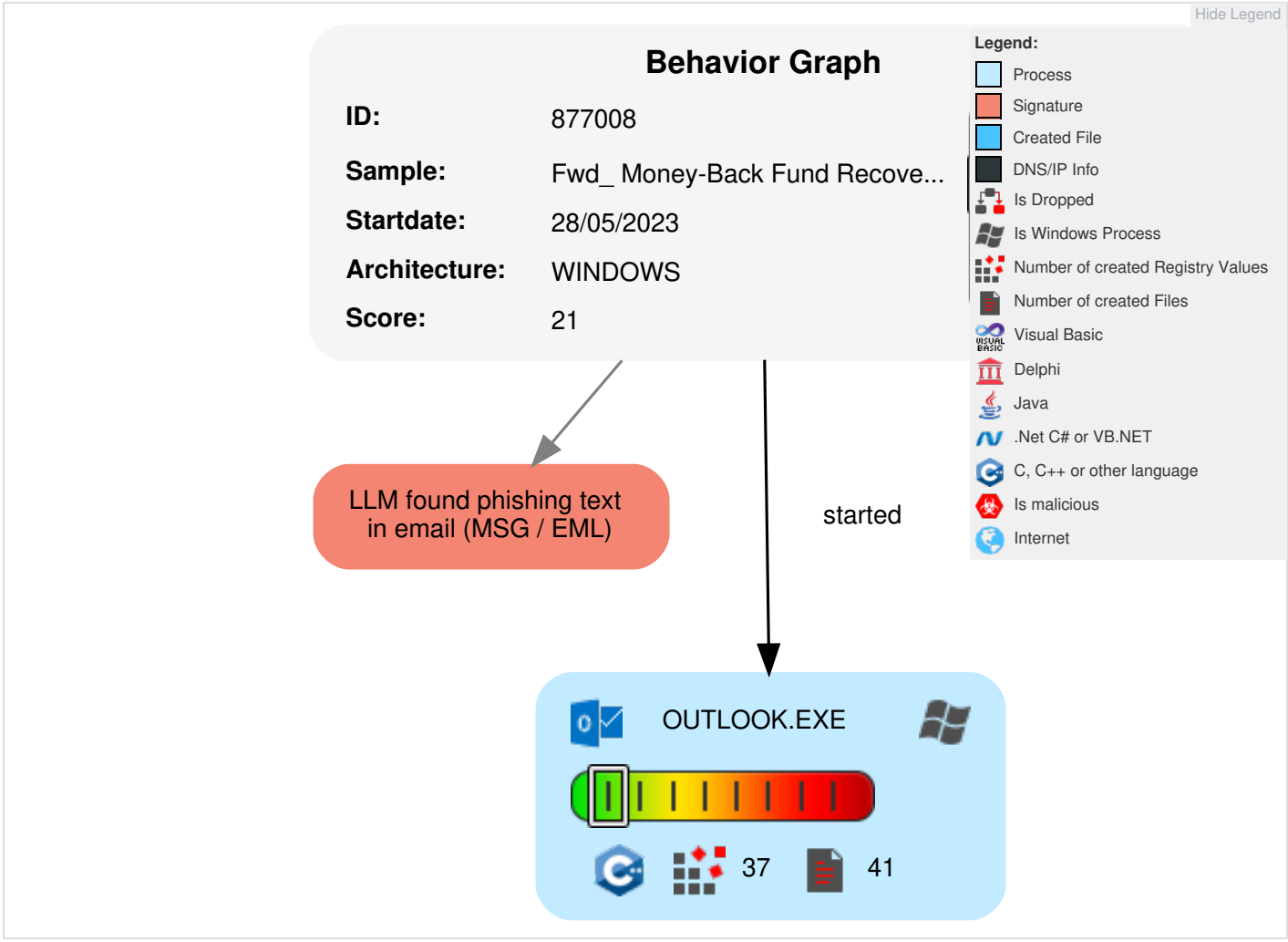
Phishing

LLM found phishing text in email (MSG / EML)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 Windows Service	1 Windows Service	1 1 Masquerading	OS Credential Dumping	2 File and Directory Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File Deletion	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

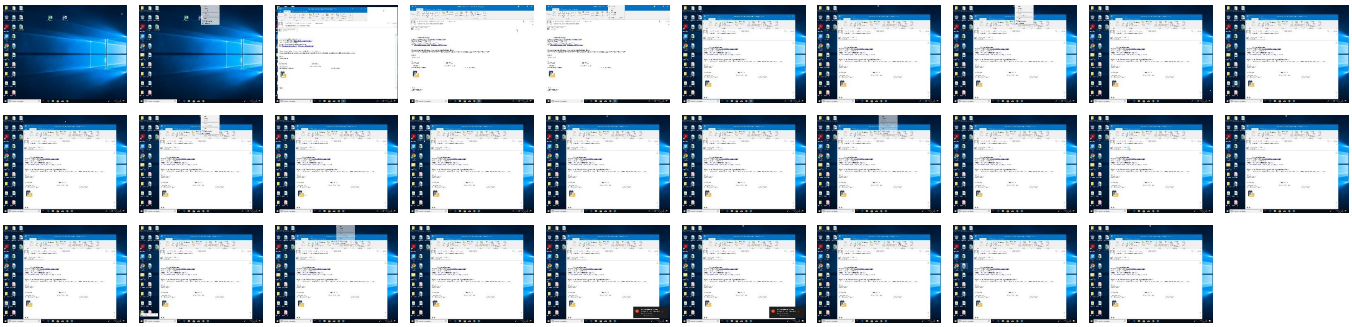
Behavior Graph

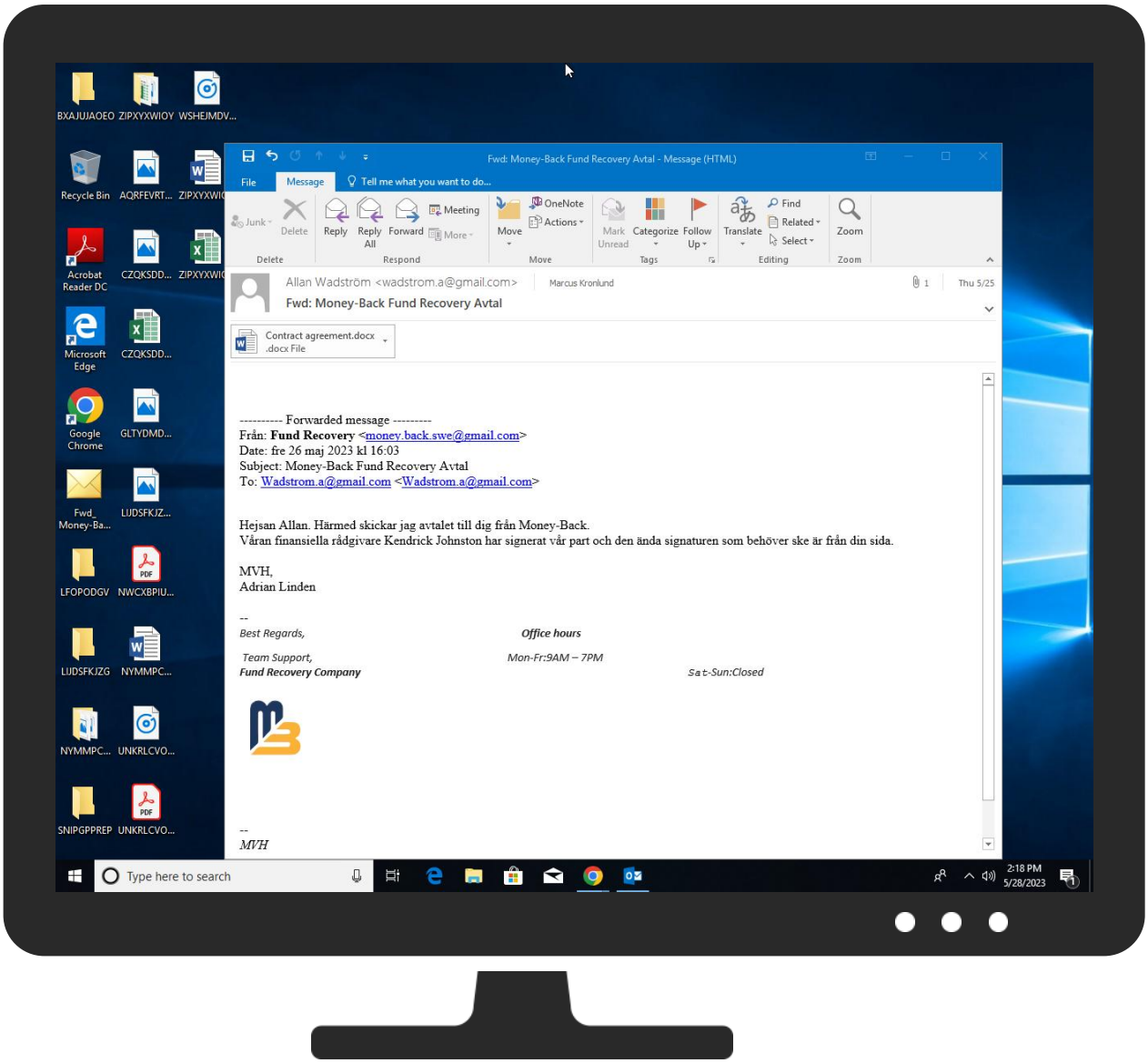


Screenshots

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

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://api.scheduler.	0%	URL Reputation	safe	
http://https://my.microsoftpersonalcontent.com	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://d.docs.live.net	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://make.powerautomate.com	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://login.windows.local	0%	URL Reputation	safe	
http://https://login.windows.local	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://api.officescripts.microsoftusercontent.com/api	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://api.diagnosticssdf.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://login.microsoftonline.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://shell.suite.office.com:1443	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://autodiscover-s.outlook.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://cdn.entity.	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://powerlift.acompli.net	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://lookup.onenote.com/lookup/geolocation/v1	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://cortana.ai	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.aadrm.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://www.yammer.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.microsoftstream.com/api/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://cr.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://graph.ppe.windows.net	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.scheduler.	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://my.microsoftpersonalcontent.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://messaging.engagement.office.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://web.microsoftstream.com/video/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://graph.windows.net	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://dataservice.o365filtering.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://d.docs.live.net	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://ncus.contentsync.	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://weather.service.msn.com/data.aspx	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://apis.live.net/v5.0/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://messaging.lifecycle.office.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://pushchannel.1drv.ms	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://management.azure.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://outlook.office365.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://wus2.contentsync.	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://make.powerautomate.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.office.net	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://entitlement.diagnostics.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://outlook.office.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://login.windows.local	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office365.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://webshell.suite.office.com	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://schema.org	Fwd_ Money-Back Fund Recovery Avtal.msg	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=OneDrive	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://substrate.office.com/search/api/v1/SearchHistory	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://management.azure.com/	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://messaging.lifecycle.office.com/getcustommessage16	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://api.officescripts.microsoftusercontent.com/api	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/c2r/v1.0/InteractiveInstallation	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://login.windows.net/common/oauth2/authorize	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false		high
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	48B20F25-693B-4953-AE33-6DC7E35E4C09.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877008
Start date and time:	2023-05-28 14:15:38 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Fwd_ Money-Back Fund Recovery Avtal.msg
Detection:	SUS
Classification:	sus21.phis.winMSG@1/13@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .msg

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 20.231.69.218, 20.234.90.154
- Excluded domains from analysis (whitelisted): prod-w.nexus.live.com.akadns.net, config.officeapps.live.com, prod.configsvc1.live.com.akadns.net, nexus.officeapps.live.com, officeclient.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryAttributesFile calls found.

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\AppData\Local\Microsoft\FORMS\FRMCACHE.DAT

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	231348
Entropy (8bit):	4.387220539959205
Encrypted:	false
SSDEEP:	1536:PYLdgsvLhmPgsxNcAz79ysQqt2ATqoQ9rcm0FvPy09PV/b9yH38uCu51:4dgEmPgWmiGu2EqoQ9rt0Fva01V/UXv1
MD5:	774D3E2CD564BE266505ABD2AD40DA81
SHA1:	B55246CB45B183C2CE1C1C85176E0FB6F19A9F11
SHA-256:	D67A09ADF86F2450076B2FFB9032A59DBA5C9EBB34ED76CDF49029DDABE1095C
SHA-512:	66F4105483B6899750756744298FEA6B3BDF7284E6817DCA42225087E277CBA418A00083A11A6E330B1853E1CA53C1836C1144E65F98CE7C00F43683F5F42873
Malicious:	false
Reputation:	low
Preview:	TH02..... .....SM01X...,.....IPM.Activity.....h..\r.....h.....F.rH..h.....9.....h^F.w..../GUrH..h.... ....VUr...h.OUr0.....h.\r.....^.i...h..w....=.....h....@..... ...h....H.....0....T.....d...x.....2h.|\r.....k_.D.....e.....!h..... h.....0.....#h..Ur8.....$h.....8....."h.....'h.U.....1h....<.....0h...4...../hl...h....H.rH..h;.\r p.....-h.....+h.....=..... .....F7.....FIPM.Activity....Form....Standard....Journal Entry...IPM.Microsoft.FolderDesign.FormsDescription.....F.k .....1122110020000000.GwwMicrosoft...This form is used to create journal entries.....kf..... .....&.....(.....(... ...@..... .....ffffffff.....wwwwwwww.p....pp.....p.....pw.....pw..DDDDO..

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\48B20F25-693B-4953-AE33-6DC7E35E4C09

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	155810
Entropy (8bit):	5.351320581847901
Encrypted:	false
SSDEEP:	1536:y+C/FPgfTB7U9guw19Q9DQA+zQak4F77nXmvidlXRjE6Llz6y:pDQ9DQA+zTXWM
MD5:	6959F9612DBAFF84C6B514C69F763FED
SHA1:	07EAFC3A9C65A2A2E51597FBFAB56D851D08B2BE
SHA-256:	7182DD40EB002A5A2EB799F46B5A014907A95E5AC164D96344CF5C4A20118211
SHA-512:	BE431084DEE4CF3B129C7F318E6C7A6736435043E37C67109955784739AD106572D5CD3DCF4728139B27685A832DDB321B37C7F6083CD6B13C5070349A7A59AA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2023-05-28T12:16:31">.. Build: 16.0.16521.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:authentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:headerValue="Passport1.4 from-PP='{}&p=''" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAuthorityU

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7E172931.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	PNG image data, 82 x 97, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	6656
Entropy (8bit):	7.954985686638339
Encrypted:	false
SSDEEP:	192:K1RDqBun4m1oxmq4s/4gft5Oq53y1QNS8hfb/xFZL:IBqBu4DEZY1V5ii5BbZ
MD5:	51E42E87ABD47D220C5653E551CBAEB4
SHA1:	9BA8B181F30BA71B2DE7DD84BAE76E0D9731377F
SHA-256:	1A29C69909D7311174E1EA029EB280F3B433571CBBB7EB7D20BC444C62685CD4
SHA-512:	730980F48936C91621EF2DD2C73FD4125CE717350FF1D5DA0718D6B5CDB00D741F7EEB1FC768542B732F354C14E85FFF6DF305881C585073B3EBE32DCAD1241
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...R...a.....E.....sRGB.....IDATx^.\....>U.....fL.0.dPP..!D.....!..(.Q#.h..F!qA#.-&..W.b.>..q..d...a.f...z..e.z.....[....g..@.....2@.... 3@...4U.ad..4!..j 2....&..TM... .@...02.d..HS5.F~...u]B..q.....s\.8.....k....8.N....P..~...:.FO.pt.....Z..?.o.....:}..A..M...8w.....b...u.W}.....G...).S..W.....:4..S>q._.#8...;.(....Y.....K.x\...Cu. :.F.H.1.L+U.(.[...&.yg..#^.....#.E.2..n.....z~.{.??O.4.Q...TM..F...v.U...^...7...m.}...-@..$O..T.z.....-.~6.{..K...I.9...@.,.....S..W..p.^....dcP..{f.....bU...|.5....b\O..b.....T...g.....|...'.. .g.....`.ko\0.)'...R.....@.4...O.(..^X...%.Y~J...*.n..w.M.m.8MSz..,.my..$3.....WPoV.i.'..~._>>t`.:....<.%U ;..q...T....F..Kl.K.....i$I....z...U..Y2.c^.V\.=.E...=YQ.b.]\.Q.....Y ^H...a.F.%Q.....o.....M'.....Y...b....`....2..a...Y..$2..o6 .W.@.]U.$.E}.#^Y8g..M....m.....Td.#.....H.kb...Q...R.v.... ?.....0.....X.aF....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{03D323D6-A084-447A-BE3F-719FAF9418DA}.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	4020
Entropy (8bit):	3.1750090668020516
Encrypted:	false
SSDEEP:	48:hpw6Dft60UvjxtSMfSdhfopebTxHTqSMf+uaFx0CizYPi4IZWkf0/N2:Y6bt6FBSycHTG8FxkYyovV2
MD5:	C9C804E6BF7738366DDE0C28007AC8C1
SHA1:	5AE71DCF25090182ABF80819FEB1664319FB3E02
SHA-256:	A138D7CC5BF058CB4663040DCB54FD76A0B26F560C916BB7C63C689E6B13C82F
SHA-512:	74EF8923B8AB964775DB3F5CBAF15660067DDEC95AC05A5AD863AC88767D78D006C3C87A10367577229878EA5265DD4B51EB62B9DE27696F2C54CD0AF89DA87
Malicious:	false
Reputation:	low
Preview:	.....-.-.-.-.-.-.-.-.-. .F.o.r.w.a.r.d.e.d. .m.e.s.s.a.g.e. .-.-.-.-.-.-.-.-.-...F.r...n.:. .F.u.n.d. .R.e.c.o.v.e.r.y. .<.H.Y.P.E.R.L.I.N.K. .".m.a.i.l.t.o.:.m.o.n.e.y...b.a.c.k...s.w.e.@.g.m.a.i.l...c.o.m."... . .....m.o.n.e.y...b.a.c.k...s.w.e.@.g.m.a.i.l...c.o.m.>...D.a.t.e.:. .f.r.e. .2.6. .m.a.j. .2.0.2.3. .k.l. .1.6.:.0.3...S.u.b.j.e.c.t.:. .M.o.n.e.y.-.B.a.c.k. .F.u.n.d. .R.e.c.o.v.e.r.y. .A.v.t.a.l...T.o.:. .H.Y.P.E.R.L.I.N.K. .".m.a.i.l.t.o.:.W.a.d.s.t.r.o.m...a.@.g.m.a.i.l...c.o.m."... . .....@...<...@...J...f...j...t...H...B..... ....

C:\Users\user\AppData\Local\Temp\~DFB841930F9A1C369D.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped

Size (bytes):	163840
Entropy (8bit):	0.4071295179725752
Encrypted:	false
SSDEEP:	192:uCb5/ny+11kop6T8sIGlTK7MA4Y1uUgMsxyiQAHwNNgiXHW8AbApN/:jSg2oGpK/4pUgMviQtAiXHhMi
MD5:	FA170EC4281278D28EEF2EB4517C2E8F
SHA1:	B2E72D07D05F4E15218DEF0E575F9AE9CE82CD1C
SHA-256:	F78B582BD43E32740D9F94AB8990CDAE33F500D0399614946F42385403C912E8
SHA-512:	20B13A51CAA7C034C2FEB156F6796DAFCCF70C261C7022C0D3337A5B9E7683D0BF1BDE925547883DF43EE38F55E10B6E45621A8E6276E2B8E2E900881C22A883
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\Documents\Outlook Files\Outlook.pst

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	Microsoft Outlook email folder (>=2003)
Category:	dropped
Size (bytes):	271360
Entropy (8bit):	1.719836036289843
Encrypted:	false
SSDEEP:	768:hOQISF8lJv86GYQKdJNBfnE+J6GhTDhN6krJ4e1G5tmg0urztTewUruGrzA:09IKPte3tE+J6QZN6+Jr7g0ufkZf
MD5:	E00F7A6365B4815E3446BE42A947194E
SHA1:	18F619FCC3C4D280E40EFC9EF8393968F8BD2EE0
SHA-256:	DB8226DE5773E691CBF8E3447E2226678B20C55B670173081BA44D585DD061CD
SHA-512:	7990D8AA67CCAD53386B3A01FB719A3ED97F9B3F921DE32F16F6B9A4BC3997960218CC10378189C22E971625EC7BB0252BF38DB438CDD5F0117AA665B1192D9
Malicious:	false
Reputation:	low
Preview:	!BDN..W_SM.....\.....&.....w.....@.....@...@.....@.....$.....D.....+....."....%..... .....4.....@vH.=..... .....

C:\Users\user\Documents\Outlook Files\~Outlook.pst.tmp

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	131072
Entropy (8bit):	0.2147511172499627
Encrypted:	false
SSDEEP:	24:+4qkQB9VXqkC0go77uFm+jxBLOAcKfWMMMUZEnMpeycWEMn5vZ+vC8pp88Yv0dET:khgo2nEKfWMMMUZ5GWhOvBY9AevLCG
MD5:	1FB06D0F5A90CEEC80D16158093A4A72
SHA1:	656CAD6392257DC4D9F41614C67112990A62A235
SHA-256:	323430FFCB2B93BA7A976D2A6D828DEAEC19E1EF88B3DBF1395F6FBF83776BE6
SHA-512:	6ED7005F7E1A21551D27E6BB609FB1DF0A0CE30C9FEFB3CFAD49CC71E189972FBDD1E40D5C5845ED0763BE9A77F34B33D135504B946CB69A3B630DE6275139E
Malicious:	false
Reputation:	low
Preview:	.gcC...D.....~.....#.!BDN..W_SM.....\.....&.....w.....@.....@...@.....@.....$ .....D.....+....."....% ....4.....@vH.=...~.....B.....#..... .....

C:\Windows\INF\Outlook\outlperf.h

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	4.697154350883648
Encrypted:	false

SSDEEP:	12:HevrLo2k2/VmkaYyaJ3VUxe4DaPaldVXN+I1okaDHDaQay/C45jG2DpkZ:gLo2FVDaYNJ3Ko4DaygFN+oFabe1wCQE
MD5:	BC71FF7DA14ECA943FA0AD815F72B8CB
SHA1:	CECCD0CFF2DD12AEDE7DE14457D15D00687165BB
SHA-256:	48E537902C03A3EEE4790FC97EE072CDDC7C1A90122702DD18243D8C12A0D99A
SHA-512:	08CD022D34C1B9B080322C3CFA15CC22E3353D42BA55C729723378DC177E8A0E979C6644BC2F97B2E36CB5E864FA37FF05DA6DBA5794A39380E72182015AB32
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	#define OBJECTTYPE 0..#define RPCATTEMPTED 2..#define RPCSUCCEEDED 4..#define RPCFAILED 6..#define RPCCANCEL 8..#define RPCSHOWN 10..#define RPCFOREGROUND 12..#define RPCTIMEAVG 14..#define RPCTIMEAVG10 16..#define RPCTIMEAVG50 18..#define RPCTIMEAVG200 20. .#define RPCTIMEMIN 22..#define RPCTIMEMAX 24..#define RPCCONNCOUNT 26..#define RPCSRVOBJCOUNT 28..#define CONTEXTHANDLECOUNTAD 30..#define BINDINGHANDLECOUNTAD 32..#define CONTEXTHANDLECOUNTSTORE 34..#define BINDINGHANDLECOUNTSTORE 36..

C:\Windows\INF\Outlook\outlperf.ini

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	Generic INItialization configuration [languages]
Category:	dropped
Size (bytes):	2695
Entropy (8bit):	5.33674634085226
Encrypted:	false
SSDEEP:	48:mJy8LzDyWt1D6lj50fvikpfNec0v6fevt8rN+rn9pNREVkWVmCU4ah6+65vq+69D:m/LzfzD6t50f1sZ6Wl8RerzEVkWh1am+
MD5:	509A7197AE66401D1DA76F4BAC1DD0A8
SHA1:	A30F0CF0161ADDBDD3B04B482FEF651EE4EAE322
SHA-256:	EE9E288C3495FD548FD49095BE08807F215FC0780064E179011098C0C7461A34
SHA-512:	4041C1073CB15ADA49D284CF612A95502CE74AC1EF69FD1B9DFDF84EDDD074150B6092C8534E49807AD3166F97127477E3497368AE845D369EBBFC2ACFC6C0 1
Malicious:	false
Preview:	[info]..drivername=Outlook..symbolfile=outlperf.h....[languages]..009=English....[text]..OBJECTTYPE_009_NAME=Outlook..OBJECTTYPE_009_HELP=Gives perfor mance metrics for outlook server connectivity...RPCATTEMPTED_009_NAME=RPCs Attempted..RPCATTEMPTED_009_HELP=Number of RPCs that outlook attempted to send to the server...RPCSUCCEEDED_009_NAME=RPCs Succeeded..RPCSUCCEEDED_009_HELP=Number of RPCs that outlook successfully sent to the server. ..RPCFAILED_009_NAME=RPCs Failed..RPCFAILED_009_HELP=Number of RPCs that were attempted, but failed...RPCCANCEL_009_NAME=RPCs Cancelled..RPC CANCEL_009_HELP=Number of RPCs that were sent to the server, but the user cancelled...RPCSHOWN_009_NAME=RPCs UI Shown..RPCSHOWN_009_HELP=Num ber of RPCs that were sent to the server, and took long enough to show progress UI...RPCFOREGROUND_009_NAME=RPCs Attempted - UI..RPCFOREGROU ND_009_HELP=Number of RPCs that outlook attempted that blocked the UI...RPCTIMEAVG_009_NAME=Time Avg (all)..RPCTIMEAVG_009_HELP=The average

C:\Windows\SysWOW64\PerfStringBackup.INI

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	856456
Entropy (8bit):	3.424585245442674
Encrypted:	false
SSDEEP:	3072:nJQGb/6IPolY/OhyIGmZkzTMWcnqgspmTbO1gK/Spm3PfqKBLamVkqhwxpR8UUUF:C1nqgsp2OtBaiY
MD5:	DCCE5FDA282F7296C105A3873060F7E1
SHA1:	876013B7EB661FF7B33845DBFAD468D70B29EB39
SHA-256:	E2C4415CCAF2F1CCE8448F8EF0B297CE0BDD085FB36072F0E784F403ECC20082
SHA-512:	FEECE5A6337CF404312FA2C4CE55054104A3AF3531A78588A43836B5D4D94620CF3216E672935079D7C5DE4C10A576C54D075D76CA62340C8DD18F88EC6C71F
Malicious:	false
Preview:	.....[.P.e.r.f.l.i.b.].....B.a.s.e. .I.n.d.e.x.=.1.8.4.7.....L.a.s.t. .C.o.u.n.t.e.r.=.9.3.0.6.....L.a.s.t. .H.e.l.p.=.9.3.0.7.....[.P.E.R.F._...N.E.T. .C.L.R. .D.a.t.a.].....F.i.r.s.t. .C.o.u. n.t.e.r.=.3.9.8.6.....F.i.r.s.t. .H.e.l.p.=.3.9.8.7.....L.a.s.t. .C.o.u.n.t.e.r.=.3.9.9.8.....L.a.s.t. .H.e.l.p.=.3.9.9.9.....[.P.E.R.F._...N.E.T. .C.L.R. .N.e.t.w.o.r.k.i.n.g.].....F.i.r.s.t. .C. o.u.n.t.e.r.=.3.7.1.4.....F.i.r.s.t. .H.e.l.p.=.3.7.1.5.....L.a.s.t. .C.o.u.n.t.e.r.=.3.7.2.4.....L.a.s.t. .H.e.l.p.=.3.7.2.5.....[.P.E.R.F._...N.E.T. .C.L.R. .N.e.t.w.o.r.k.i.n.g. .4... 0...0...0.].....F.i.r.s.t. .C.o.u.n.t.e.r.=.4.4.7.2.....F.i.r.s.t. .H.e.l.p.=.4.4.7.3.....L.a.s.t. .C.o.u.n.t.e.r.=.4.4.9.8.....L.a.s.t. .H.e.l.p.=.4.4.9.9.....[.P.E.R.F._...N.E.T. .D.a.t.a. .P.r. o.v.i.d.e.r. .f.o.r. .O.r.a.c.l.e.].....F.i.r.s.t. .C.o.u.n.t.e.r.=.3.9.5.6.....F.i.r.s.t. .H.e.l.p.=.3.9.5.7.....L.a.s.t. .C.o.u.n.t.e.r.=.3.9.8.4.....L.a.s.t. .H.e.l.p.=.3.9.8.5.....[.P.E.R.F._. ..N.E.T. .

C:\Windows\SysWOW64\PerfStringBackup.TMP

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	856456
Entropy (8bit):	3.424585245442674
Encrypted:	false
SSDEEP:	3072:nJQGb/6IPolY/OhyIGmZkzTMWcnqgspmTbO1gK/Spm3PfqKBLamVkqhwxpR8UUUF:C1nqgsp2OtBaiY
MD5:	DCCE5FDA282F7296C105A3873060F7E1

SHA1:	876013B7EB661FF7B33845DBFAD468D70B29EB39
SHA-256:	E2C4415CCAF2F1CCE8448F8EF0B297CE0BDD085FB36072F0E784F403ECC20082
SHA-512:	FEECE5A6337CF404312FA2C4CE55054104A3AF3531A78588A43836B5D4D94620CF3216E672935079D7C5DE4C10A576C54D075D76CA62340C8DD18F88EC6C71F
Malicious:	false
Preview:	.....[.P.e.r.f.l.i.b.].....B.a.s.e. .I.n.d.e.x.=.1.8.4.7.....L.a.s.t. .C.o.u.n.t.e.r.=.9.3.0.6.....L.a.s.t. .H.e.l.p.=.9.3.0.7.....[.P.E.R.F._...N.E.T. .C.L.R. .D.a.t.a.].....F.i.r.s.t. .C.o.u.n.t.e.r.=.3.9.8.6.....F.i.r.s.t. .H.e.l.p.=.3.9.8.7.....L.a.s.t. .C.o.u.n.t.e.r.=.3.9.9.8.....L.a.s.t. .H.e.l.p.=.3.9.9.9.....[.P.E.R.F._...N.E.T. .C.L.R. .N.e.t.w.o.r.k.i.n.g.].....F.i.r.s.t. .C.o.u.n.t.e.r.=.3.7.1.4.....F.i.r.s.t. .H.e.l.p.=.3.7.1.5.....L.a.s.t. .C.o.u.n.t.e.r.=.3.7.2.4.....L.a.s.t. .H.e.l.p.=.3.7.2.5.....[.P.E.R.F._...N.E.T. .C.L.R. .N.e.t.w.o.r.k.i.n.g. .4...0...0...0.].....F.i.r.s.t. .C.o.u.n.t.e.r.=.4.4.7.2.....F.i.r.s.t. .H.e.l.p.=.4.4.7.3.....L.a.s.t. .C.o.u.n.t.e.r.=.4.4.9.8.....L.a.s.t. .H.e.l.p.=.4.4.9.9.....[.P.E.R.F._...N.E.T. .D.a.t.a. .P.r.o.v.i.d.e.r. .f.o.r. .O.r.a.c.l.e.].....F.i.r.s.t. .C.o.u.n.t.e.r.=.3.9.5.6.....F.i.r.s.t. .H.e.l.p.=.3.9.5.7.....L.a.s.t. .C.o.u.n.t.e.r.=.3.9.8.4.....L.a.s.t. .H.e.l.p.=.3.9.8.5.....[.P.E.R.F._...N.E.T. .

C:\Windows\System32\perfc009.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	133672
Entropy (8bit):	3.4045308547957878
Encrypted:	false
SSDEEP:	1536:X1iTlxFbXxIPoO2NAYW22glhzEmhVd0Rev54d:XtxFbXxIPoO2NAYW22glhzEpev54d
MD5:	CD989A7EF2086A5952A945991A8E731D
SHA1:	BF9DBF42367872448D1A8C107C132C5C6355D156
SHA-256:	A9DD4213B016C7C37E18394710657327BB6DD083A6EBF9D97D94A31829A630E1
SHA-512:	EEA18B26AC27C2F03F7FE115439EA4BE713680B58C403ABAD3668ECE50CFE63A730E28AEC2249988237B8133C4BD9C1F17106C7FB004BDA4E0BBB0F7FF94035A
Malicious:	false
Preview:	1...1.8.4.7...2...S.y.s.t.e.m...4...M.e.m.o.r.y...6...%. .P.r.o.c.e.s.s.o.r. .T.i.m.e...1.0...F.i.l.e. .R.e.a.d. .O.p.e.r.a.t.i.o.n.s./.s.e.c...1.2...F.i.l.e. .W.r.i.t.e. .O.p.e.r.a.t.i.o.n.s./.s.e.c...1.4...F.i.l.e. .C.o.n.t.r.o.l. .O.p.e.r.a.t.i.o.n.s./.s.e.c...1.6...F.i.l.e. .R.e.a.d. .B.y.t.e.s./.s.e.c...1.8...F.i.l.e. .W.r.i.t.e. .B.y.t.e.s./.s.e.c...2.0...F.i.l.e. .C.o.n.t.r.o.l. .B.y.t.e.s./.s.e.c...2.4...A.v.a.i.l.a.b.l.e. .B.y.t.e.s...2.6...C.o.m.m.i.t.t.e.d. .B.y.t.e.s...2.8...P.a.g.e. .F.a.u.l.t.s./.s.e.c...3.0...C.o.m.m.i.t. .L.i.m.i.t...3.2...W.r.i.t.e. .C.o.p.i.e.s./.s.e.c...3.4...T.r.a.n.s.i.t.i.o.n. .F.a.u.l.t.s./.s.e.c...3.6...C.a.c.h.e. .F.a.u.l.t.s./.s.e.c...3.8...D.e.m.a.n.d. .Z.e.r.o. .F.a.u.l.t.s./.s.e.c...4.0...P.a.g.e.s./.s.e.c...4.2...P.a.g.e. .R.e.a.d.s./.s.e.c...4.4...P.r.o.c.e.s.s.o.r. .Q.u.e.u.e. .L.e.n.g.t.h...4.6...T.h.r.e.a.d. .S.t.a.t.e...4.8...P.a.g.e.s. .O.u.t.p.u.t./.s.e.c...5.0...P.a.g.e. .W.r.i.t.e.s./.s.e.c...5.2...B.r.o.w.s.e.r...5.4...A.n.n.o.u.

C:\Windows\System32\perfh009.dat

Process:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	711942
Entropy (8bit):	3.2750038779489223
Encrypted:	false
SSDEEP:	3072:NUdGNuowE4j0PrRZnpETMDZ8M6d0PHd1zsS3MgjBmbsCJnpEiLxVrFfarYCH6b/o:78M6d0IBb/8c
MD5:	E7524976DB303DF6346CF3024872DD9C
SHA1:	31CAF98E58524AB40F9A786F4504869AFABA1F3A
SHA-256:	2CDA416A24A4B10CC28E873E038CED3207D1EFB4A1D07A4594D5728B48EAE4FD
SHA-512:	D87AB126F26BE07DFF3928D8D1AC2496531410DDFBFA2D7D24A8E53BCF12A95FEE9789C06172241488562127773 2C1F33540BFE9A75D36DE68D51411ECF176E
Malicious:	false
Preview:	3...T.h.e. .S.y.s.t.e.m. .p.e.r.f.o.r.m.a.n.c.e. .o.b.j.e.c.t. .c.o.n.s.i.s.t.s. .o.f. .c.o.u.n.t.e.r.s. .t.h.a.t. .a.p.p.l.y. .t.o. .m.o.r.e. .t.h.a.n. .o.n.e. .i.n.s.t.a.n.c.e. .o.f. .a. .c.o.m.p.o.n.e.n.t. .p.r.o.c.e.s.s.o.r.s. .o.n. .t.h.e. .c.o.m.p.u.t.e.r.....5...T.h.e. .M.e.m.o.r.y. .p.e.r.f.o.r.m.a.n.c.e. .o.b.j.e.c.t. . .c.o.n.s.i.s.t.s. .o.f. .c.o.u.n.t.e.r.s. .t.h.a.t. .d.e.s.c.r.i.b.e. .t.h.e. .b.e.h.a.v.i.o.r. .o.f. .p.h.y.s.i.c.a.l. .a.n.d. .v.i.r.t.u.a.l. .m.e.m.o.r.y. .o.n. .t.h.e. .c.o.m.p.u.t.e.r... . .P.h.y.s.i.c.a.l. .m.e.m.o.r.y. .i.s. .t.h.e. .a.m.o.u.n.t. .o.f. .r.a.n.d.o.m. .a.c.c.e.s.s. .m.e.m.o.r.y. .o.n. .t.h.e. .c.o.m.p.u.t.e.r... . .V.i.r.t.u.a.l. .m.e.m.o.r.y. .c.o.n.s.i.s.t.s. .o.f. .t.h.e. .s.p.a.c.e. .i.n. .p.h.y.s.i.c.a.l. .m.e.m.o.r.y. .a.n.d. .o.n. .d.i.s.k... . . M.a.n.y. .o.f. .t.h.e. .m.e.m.o.r.y. .c.o.u.n.t.e.r.s. .m.o.n.i.t.o.r. .p.a.g.i.n.g.,. .w.h.i.c.h. .i.s. .t.h.e. .m.o.v.e.m.e.n.t. .o.f. .p.a.g.e.s. .o.f. .c.o.d.e. .a.n.d. .d.a.t.a. .b.e.t.

Static File Info

General

File type:	CDFV2 Microsoft Outlook Message
Entropy (8bit):	6.942954359969189
TrID:	• Outlook Message (71009/1) 58.92% • Outlook Form Template (41509/1) 34.44% • Generic OLE2 / Multistream Compound File (8008/1) 6.64%
File name:	Fwd_ Money-Back Fund Recovery Avtal.msg
File size:	287744
MD5:	7e6f449c9ca36dd1ee915b141e7d0793

SHA1:	b9f06ca54a6fe902c2aa11bd4b209cab44c16377
SHA256:	b611ba8a90974b4b9559aa60ea9987bd370463d4223d0b66ab2b01179f9b19a4
SHA512:	876ce21920c1cc92e645b7279a7f738edb23809842dda9352ea56c5ffd6146752cb1d2b6575bf66b2ff175aedcf7fb405d6a1da5e9f265133528b58dda27e0da
SSDEEP:	6144:snhVyIHFV8fgV8WHW8b1RGlrE9Z4gRMNW1/Q7hegIHTPd2:EhQlqQWkqmrQhHIB2
TLSH:	A4546C1539E55606F2B79E324DE290939537FD82AD30CA8F2189730E0B73A41D962B7B
File Content Preview:	.....>.....

Static Mail

General

Subject:	Fwd: Money-Back Fund Recovery Avtal
From:	=?UTF-8?Q?Allan_Wadstr=C3=B6m?= <wadstrom.a@gmail.com>
To:	marcus.kronlund@pwntech.se
Cc:	
BCC:	
Date:	Fri, 26 May 2023 02:05:51 +0200
Communications:	---------- Forwarded message --------- Frn: Fund Recovery <money.back.swe@gmail.com <mailto:money.back.swe@gmail.com> > Date: fre 26 maj 2023 kl 16:03 Subject: Money-Back Fund Recovery Avtal To: Wadstrom.a@gmail.com <mailto:Wadstrom.a@gmail.com> <Wadstrom.a@gmail.com <mailto:Wadstrom.a@gmail.com> > Hejsan Allan. Hrmed skickar jag avtalet till dig frn Money-Back. Vran finansiella rdgivare Kendrick Johnston har signerat vr part och den nda signaturen som behver ske r frn din sida. MVH, Adrian Linden -- Best Regards, Office hours Team Support, Mon-Fr:9AM 7PM Fund Recovery Company Sat-Sun:Closed -- MVH Allan Wadstrm
Attachments:	a6fed136-d788-425b-9a6b-88a700cdd715.png Contract agreement.docx

Headers

Key	Value
Received	by mail-wm1-f47.google.com with SMTP id 5b1f17b1804b1-3f50020e0f8so14751265e9.0
GVYP280MB0559.SWEP280.PROD.OUTLOOK.COM with HTTPS; Fri, 26 May 2023 17	29:57
(2603	10a6:10:4b8::24) with Microsoft SMTP Server (version=TLS1_2,
2023 17	29:41 +0000
Transport; Fri, 26 May 2023 17	29:41 +0000
Authentication-Results	spf=pass (sender IP is 209.85.128.47)
Received-SPF	Pass (protection.outlook.com: domain of gmail.com designates
15.20.6433.18 via Frontend Transport; Fri, 26 May 2023 17	29:41 +0000
for <marcus.kronlund@pwntech.se>; Fri, 26 May 2023 10	29:41 -0700 (PDT)
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed;
h=to	subject:message-id:date:from:in-reply-to:references:mime-version
	x-gm-message-state:from:to:cc:subject:date:message-id:reply-to;
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed;
X-Gm-Message-State	AC+VfDwpNl33ImaZEDDGfE1JCLgcnWlfjKkDV6+s2o0ljFE9bHHVeLui

Key	Value
X-Google-Smtp-Source	ACHHUZ7uZP5dWxV+G25Kw9DCHJgKIqVQ1tP98+OdMaoIo9OgJyYBDwa6VzuFKMQgdu2GlYd+Dt7Zuif/UIR6oa0+IjY=
X-Received	by 2002:adf:f50b:0:b0:30a:a93c:c9df with SMTP id
May 2023 10	29:40 -0700 (PDT)
MIME-Version	1.0
References	<CANao+fvQAR4b2oLQN6Dod4psF75BjHE0otYEhM5wFDDBVbF1Lg@mail.gmail.com>
In-Reply-To	<CANao+fvQAR4b2oLQN6Dod4psF75BjHE0otYEhM5wFDDBVbF1Lg@mail.gmail.com>
From	=?UTF-8?Q?Allan_Wadstr=C3=B6m?= <wadstrom.a@gmail.com>
Date	Fri, 26 May 2023 02:05:51 +0200
Message-ID	<CAB-+hfGev1wD0deSQRFMMUm3uy=8vwS8VvJGpMXQdM5ijTUwdQ@mail.gmail.com>
Subject	Fwd: Money-Back Fund Recovery Avtal
To	marcus.kronlund@pwntech.se
Content-Type	multipart/mixed; boundary="000000000000f4278805fc9c14e7"
Return-Path	wadstrom.a@gmail.com
X-MS-Exchange-Organization-ExpirationStartTime	26 May 2023 17:29:41.3182
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason	OriginalSubmit
X-MS-Exchange-Organization-Network-Message-Id	f3e6a1b9-cf91-417f-4030-08db5e0ec9ea
X-EOPAttributedMessage	0
X-EOPTenantAttributedMessage	b63e747e-bad2-4f8e-a252-e2c847dd0c99:0
X-MS-Exchange-Organization-MessageDirectionality	Incoming
X-MS-PublicTrafficType	Email
X-MS-TrafficTypeDiagnostic	DBAEUR03FT013:EE_|MM1PPF9E97ECF67:EE_|GVYP280MB0559:EE_
X-MS-Exchange-Organization-AuthSource	DBAEUR03FT013.eop-EUR03.prod.protection.outlook.com
X-MS-Exchange-Organization-AuthAs	Anonymous
X-MS-Office365-Filtering-Correlation-Id	f3e6a1b9-cf91-417f-4030-08db5e0ec9ea
X-MS-Exchange-AtpMessageProperties	SA|SL
X-MS-Exchange-Organization-SCL	1
X-Microsoft-Antispam	BCL:0;
X-Forefront-Antispam-Report	CIP:209.85.128.47;CTRY:US;LANG:sv;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:mail-wm1-f47.google.com;PTR:mail-wm1-f47.google.com;CAT:NONE;SFS:(13230028)(4636009)(84050400002)(451199021)(8676002)(5660300002)(33964004)(6916009)(42186006)(76482006)(83380400001)(6666004)(1096003)(21490400003)(73392003)(26005)(82202003)(55446002)(336012)(86362001)(7636003)(356005)(7596003);DIR:INB;
X-MS-Exchange-CrossTenant-OriginalArrivalTime	26 May 2023 17:29:41.2713
X-MS-Exchange-CrossTenant-Network-Message-Id	f3e6a1b9-cf91-417f-4030-08db5e0ec9ea
X-MS-Exchange-CrossTenant-Id	b63e747e-bad2-4f8e-a252-e2c847dd0c99
X-MS-Exchange-CrossTenant-AuthSource	DBAEUR03FT013.eop-EUR03.prod.protection.outlook.com
X-MS-Exchange-CrossTenant-AuthAs	Anonymous
X-MS-Exchange-CrossTenant-FromEntityHeader	Internet
X-MS-Exchange-Transport-CrossTenantHeadersStamped	MM1PPF9E97ECF67
X-MS-Exchange-Transport-EndToEndLatency	00:00:15.9660198
X-MS-Exchange-Processed-By-BccFoldering	15.20.6433.015
X-Microsoft-Antispam-Mailbox-Delivery	ucf:0;jmr:0;auth:0;dest:I;ENG:(910001)(944506478)(944626604)(920097)(930097);
X-Microsoft-Antispam-Message-Info	=?us-ascii?Q?3Q6dBnn4lTLRBCbg+FRTYZOQb/OpEQwv5rzHWa/Ku3AihHZZtKyuzIJiVGo4?=
date	Fri, 26 May 2023 02:05:51 +0200

File Icon

Icon Hash:	deecb9d2afecdebf

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: OUTLOOK.EXE PID: 4108, Parent PID: 3452

General

Target ID:	0
Start time:	14:16:30
Start date:	28/05/2023
Path:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Microsoft Office\Office16\OUTLOOK.EXE" /f "C:\Users\user\Desktop\Fwd_ Money-Back Fund Recovery Avtal.msg
Imagebase:	0x1310000
File size:	23291112 bytes
MD5 hash:	7DD935BA9B57D9D7EFF63C67653E70B5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Outlook\RoamCache\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	14E4547	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Outlook\RoamCache\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	14E4547	CreateDirectoryW

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Addins\ColleagueImport.ColleagueImportAddin	1	binary	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 00 00 5D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	13DCD49	RegSetValueExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Addins\Microsoft.VbaAddinForOutlook.1	1	binary	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	13DCD49	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Addins\OneNote.OutlookAddin	1	binary	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	13DCD49	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Addins\OscAddin.Connect	1	binary	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	13DCD49	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Addins\UCAddin.LyncAddin.1	1	binary	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	13DCD49	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Addins\UmOutlookAddin.FormRegionAddin	1	binary	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	13DCD49	RegSetValueExA

Disassembly

No disassembly