ID: 753417
Sample Name: UniverseCity.exe
Cookbook: default.jbs
Time: 19:42:09
Date: 24/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

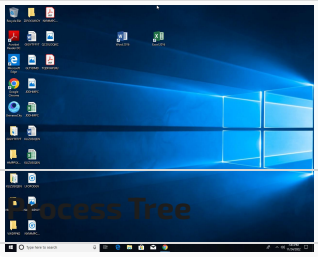
Windows Analysis Report

UniverseCity.exe

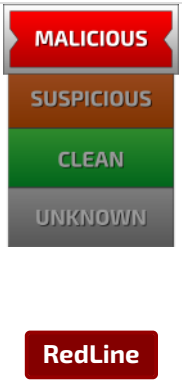
Overview

General Information

Sample Name:	UniverseCity.exe
Analysis ID:	753417
MD5:	2815815f0488b3..
SHA1:	c5845c0c743106..
SHA256:	14b87b3a9eb96e.
Tags:	185-206-213-32, CosmicWay, exe, FakeGaliXCity, RedLineStealer, UniverseCity
Infos:	



Detection



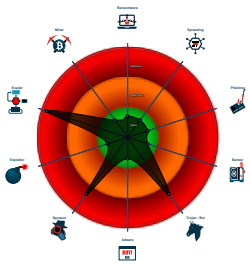
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Detected unpacking (changes PE se…
- Snort IDS alert for network traffic
- Hides threads from debuggers
- Tries to detect sandboxes and other…
- Tries to steal Crypto Currency Walle…
- Query firmware table information (lik…
- Tries to detect sandboxes / dynamic…
- Machine Learning detection for sam…
- Queries sensitive video device infor…
- Queries sensitive disk information (v…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- UniverseCity.exe (PID: 3836 cmdline: C:\Users\user\Desktop\UniverseCity.exe MD5: 2815815F0488B3D2307C3A914DDC1D7A)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": "185.206.213.32:42794",
  "Bot Id": "110",
  "Authorization Header": "e47b0f61fb0cc49a8eafd0acb2a1befc"
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
Process Memory Space: UniverseCity.exe PID: 3836	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: UniverseCity.exe PID: 3836	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.4 - Destination IP: 185.206.213.32

Timestamp:	192.168.2.4185.206.213.3249696427942850286 11/24/22-19:43:22.900750
SID:	2850286
Source Port:	49696
Destination Port:	42794
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.4 - Destination IP: 185.206.213.32

Timestamp:	192.168.2.4185.206.213.3249696427942850027 11/24/22-19:43:19.130595
SID:	2850027
Source Port:	49696
Destination Port:	42794
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 185.206.213.32 - Destination IP: 192.168.2.4

Timestamp:	185.206.213.32192.168.2.442794496962850353 11/24/22-19:43:20.869342
SID:	2850353
Source Port:	42794
Destination Port:	49696
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Data Obfuscation

Detected unpacking (changes PE section rights)

Copyright Joe Security LLC 2022

Malware Analysis System Evasion

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Anti Debugging

Hides threads from debuggers

Tries to detect sandboxes and other dynamic analysis tools (window names)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

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

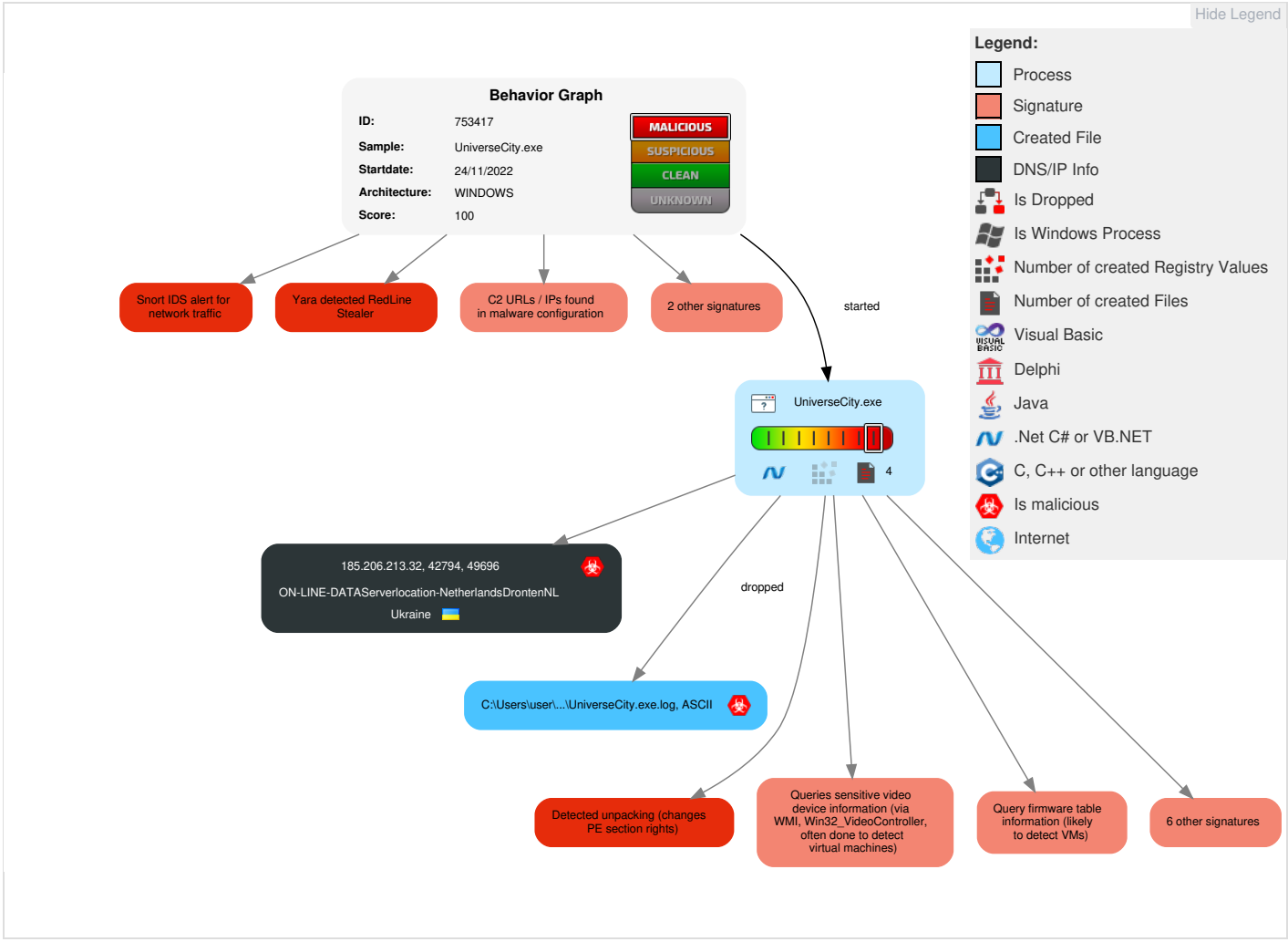
Remote Access Functionality

Yara detected RedLine Stealer

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	2 2 1 Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	1 OS Credential Dumping	6 5 Security Software Discovery	Remote Services	3 Data from Local System	Exfiltration Over Other Network Medium	1 Non-Standard Port	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 Disable or Modify Tools	LSASS Memory	1 1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 5 1 Virtualization/Sandbox Evasion	Security Account Manager	5 5 1 Virtualization/Sandbox Evasion	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 2 4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

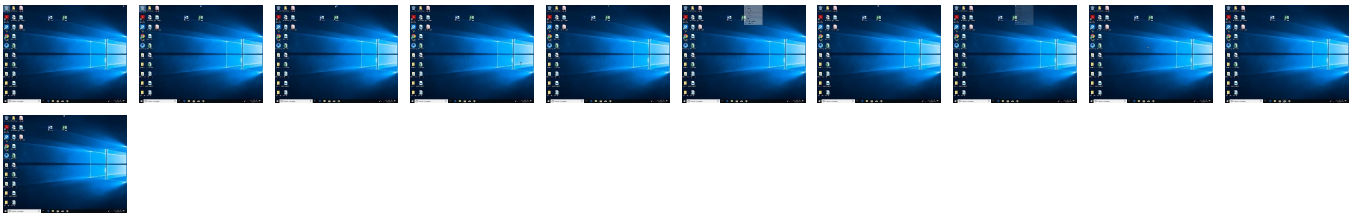
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
UniverseCity.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://www.w3.o	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1	0%	URL Reputation	safe	
185.206.213.32:42794	0%	Virustotal		Browse
185.206.213.32:42794	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.206.213.32:42794	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	UniverseCity.exe, 00000000.00000002.3952 42356.00000000037C9000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000 373C000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	UniverseCity.exe, 00000000.00000002.3952 42356.00000000037C9000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000 373C000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://tempuri.org/	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.391774735.000000000 3411000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adobe.c/g	UniverseCity.exe, 00000000.00000003.3786 99909.0000000002BBC000.00000004.00000020 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.389446590.000000000 2BBD000.00000004.00000020.00020000.00000 000.sdmp, UniverseCity.exe, 00000000.000 00003.378769956.0000000002BBD000.0000000 4.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high

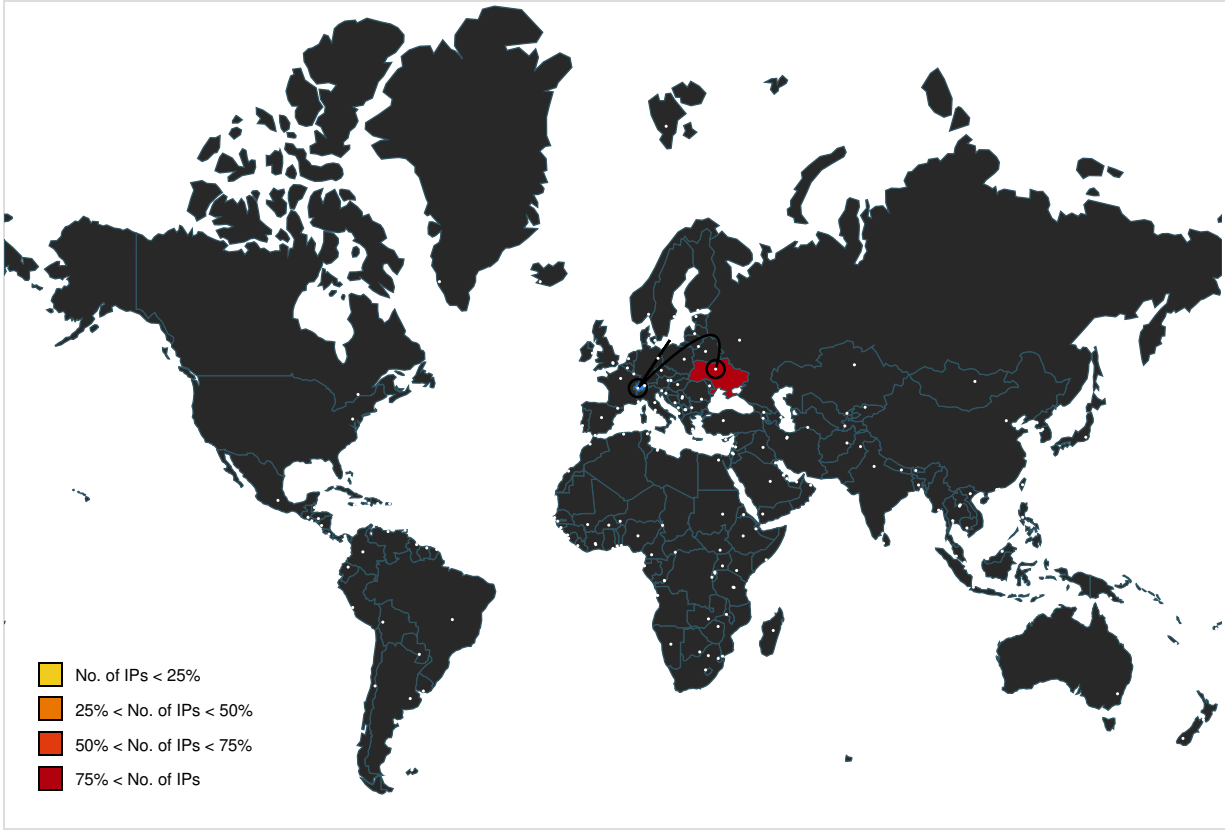
Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultx	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	UniverseCity.exe, 00000000.00000002.3952 42356.00000000037C9000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000 373C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id1Response	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.391774735.000000000 3411000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	UniverseCity.exe, 00000000.00000002.3952 42356.00000000037C9000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000 373C000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/soap/envelope/	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	UniverseCity.exe, 00000000.00000002.3952 42356.00000000037C9000.00000004.00000800 .00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000 373C000.00000004.00000800.00020000.00000 000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possesspropertyI	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	UniverseCity.exe, 00000000.00000002.3917 74735.0000000003411000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Renew	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/SymmetricKey	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.w3.o	UniverseCity.exe, 00000000.00000002.3933 76642.00000000035DD000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/fault	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	UniverseCity.exe, 00000000.00000002.3920 74868.0000000003481000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2004/10/wscoor/RegisterResponse	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Cancel	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	UniverseCity.exe, 00000000.00000002.391774735.0000000003411000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	UniverseCity.exe, 00000000.00000002.395242356.00000000037C9000.00000004.00000800.00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000373C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	UniverseCity.exe, 00000000.00000002.391774735.0000000003411000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/tlsnego#TLS_Wrap	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2002/12/policy	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/dk	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Issue	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	UniverseCity.exe, 00000000.00000002.395242356.00000000037C9000.00000004.00000800.00020000.00000000.sdmp, UniverseCity.exe, 00000000.00000002.394744089.000000000373C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/Issue	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Commit	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContext	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/Issue	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT	UniverseCity.exe, 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1	UniverseCity.exe, 00000000.00000002.391774735.0000000003411000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.206.213.32	unknown	Ukraine		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	753417
Start date and time:	2022-11-24 19:42:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UniverseCity.exe
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:	3
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.troj.spyw.evad.winEXE@1/1@0/1
EGA Information:	Failed
HDC Information:	Failed

Copyright Joe Security LLC 2022

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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:43:25	API Interceptor	64x Sleep call for process: UniverseCity.exe modified

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\CLR_v4.0_32\UsageLogs\UniverseCity.exe.log

Process:	C:\Users\user\Desktop\UniverseCity.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2201
Entropy (8bit):	5.326033842196865
Encrypted:	false
SSDEEP:	48:MIHK5HKXEAHKzvQfHK7HKhBHKdHKBSTHtHmYHKhQnoPtHoxHlmHKx1qHAHVHxLH0:Pq5qXLqzAq7qLqdqsNGYqhQnoPtIxHbt
MD5:	9D13095367E03502A903DEBCA7487DF4
SHA1:	75CAC4CD0867B1EF8422118EA22520E546F1C893
SHA-256:	D6C7B642CBA4757549117405242B88C6383A2F555ACD121CC70D6BF604698469
SHA-512:	F61C92128B02D520071F3A271FEF5B847AB58C0F7D53D188EE18504CECD67FCB3F03005130C8240FE7946CAA5F611A443789921DE2E86C70D7A656695B226219

Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\Syst

Static File Info

General

File type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Entropy (8bit):	7.993226453571658
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:	UniverseCity.exe
File size:	4881408
MD5:	2815815f0488b3d2307c3a914ddc1d7a
SHA1:	c5845c0c743106ac27622d32689a24e2f52a9ab7
SHA256:	14b87b3a9eb96e080373e2a7203b664b63cec8cc163bbd10b028ecf5441f7f67
SHA512:	bc4e8c73de9a1a6db1984397a3339c62fb03e3bf145e0b2bb66596afa74b5944a73445ec04d5b5613b177e7aed9950408d96cf7481b3f856d76abf338ec1ff49
SSDEEP:	98304:sbtWGDueBJmf8eGjoA120pwKD6rjOXRe3qTZZQlYRpFvGHtGqKpIZ8:nGNO86AEawwNhZzpc8qiA
TLSH:	0D36336EF3D60AB1E45C01B1002E9BCF4B7675071D25DA2ABB4C738D9F72342BE69291
File Content Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L...t..P.....#.....- .....@.....`.....n.J.....0.....tw.....`.d..$.....

File Icon

Icon Hash:	c48e0f4f27a6f8f0

Static PE Info

General

Entrypoint:	0xddd12d
Entrypoint Section:	.MPRESS2
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE, DEBUG_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5000A574 [Fri Jul 13 22:47:16 2012 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	e045c920c82e7a05da4487cce2e427b2

Authenticode Signature

Signature Valid:	
Signature Issuer:	
Signature Validation Error:	

Error Number:	
Not Before, Not After	
Subject Chain	
Version:	
Thumbprint MD5:	
Thumbprint SHA-1:	
Thumbprint SHA-256:	
Serial:	

Entrypoint Preview
Instruction
pushad
call 00007FE930736655h
pop eax
add eax, 00000B5Ah
mov esi, dword ptr [eax]
add esi, eax
sub eax, eax
mov edi, esi
lodsw
shl eax, 0Ch
mov ecx, eax
push eax
lodsd
sub ecx, eax
add esi, ecx
mov ecx, eax
push edi
push ecx
dec ecx
mov al, byte ptr [ecx+edi+06h]
mov byte ptr [ecx+esi], al
jne 00007FE930736648h
sub eax, eax
lodsb
mov ecx, eax
and cl, FFFFFFF0h
and al, 0Fh
shl ecx, 0Ch
mov ch, al
lodsb
or ecx, eax
push ecx
add cl, ch
mov ebp, FFFFFD00h
shl ebp, cl
pop ecx
pop eax
mov ebx, esp
lea esp, dword ptr [esp+ebp*2-00000E70h]
push ecx
sub ecx, ecx
push ecx
push ecx
mov ecx, esp
push ecx
mov dx, word ptr [edi]
shl edx, 0Ch
push edx
push edi

Instruction
add ecx, 04h
push ecx
push eax
add ecx, 04h
push esi
push ecx
call 00007FE9307366B3h
mov esp, ebx
pop esi
pop edx
sub eax, eax
mov dword ptr [edx+esi], eax
mov ah, 10h
sub edx, eax
sub ecx, ecx
cmp ecx, edx
jnc 00007FE930736678h
mov ebx, ecx
lodsb
inc ecx
and al, FEh
cmp al, E8h
jne 00007FE930736644h
inc ebx
add ecx, 04h
lodsd
or eax, eax
js 00007FE930736658h
cmp eax, edx
jnc 00007FE930736637h
jmp 00007FE930736658h
add eax, ebx
js 00007FE930736631h
add eax, edx
sub eax, ebx
mov dword ptr [esi-04h], eax
jmp 00007FE930736628h
call 00007FE930736655h
pop edi
add edi, FFFFFF4Dh
mov al, E9h
stosb
mov eax, 00000B56h
stosd
call 00007FE930736655h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9dd000	0x130	.MPRESS2
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9de000	0x17774	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1a64c160	0x24a8	
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	

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9dd078	0x20	.MPRESS2
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.MPRESS1	0x1000	0x9dc000	0x48f400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.MPRESS2	0x9dd000	0xc97	0xe00	False	0.5276227678571429	data	5.654337414624995	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x9de000	0x17774	0x17800	False	0.39691032247340424	data	5.472894526519017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
REGISTRY	0x9de0ec	0x445	ASCII text, with CRLF line terminators		
REGISTRY	0x9de55c	0x30e	ASCII text, with CRLF line terminators		
REGISTRY	0x9de894	0xbe4	ASCII text, with CRLF line terminators		
REGISTRY	0x9df4a0	0x355	ASCII text, with CRLF line terminators		
REGISTRY	0x9df820	0x348	ASCII text, with CRLF line terminators		
REGISTRY	0x9dfb90	0x380	ASCII text, with CRLF line terminators		
TYPELIB	0x9dff60	0xb7b4	data	English	United States
RT_CURSOR	0x97a02c	0x134	empty		
RT_CURSOR	0x97a160	0x134	empty		
RT_CURSOR	0x97a294	0x134	empty		
RT_CURSOR	0x97a3c8	0x134	empty		
RT_CURSOR	0x97a4fc	0x134	empty		
RT_CURSOR	0x97a630	0xcac	empty		
RT_CURSOR	0x97b2dc	0x134	empty		
RT_CURSOR	0x97b410	0xcac	empty		
RT_CURSOR	0x97c0bc	0x10ac	empty		
RT_CURSOR	0x97d168	0x10ac	empty		
RT_CURSOR	0x97e214	0x10ac	empty		
RT_CURSOR	0x97f2c0	0x10ac	empty		
RT_CURSOR	0x98036c	0x10ac	empty		
RT_CURSOR	0x981418	0x10ac	empty		
RT_CURSOR	0x9824c4	0x10ac	empty		
RT_CURSOR	0x983570	0x10ac	empty		
RT_CURSOR	0x98461c	0x10ac	empty		
RT_CURSOR	0x9856c8	0x10ac	empty		
RT_CURSOR	0x986774	0x10ac	empty		
RT_CURSOR	0x987820	0x134	empty		
RT_CURSOR	0x987954	0x134	empty		
RT_CURSOR	0x987a88	0x134	empty		
RT_CURSOR	0x987bbc	0x134	empty		
RT_ICON	0x9ebbb4	0x6fb0	Device independent bitmap graphic, 83 x 166 x 32, image size 27556		
RT_MENU	0x98eca0	0x2be	empty	Chinese	China

Name	RVA	Size	Type	Language	Country
RT_MENU	0x98ef60	0x32e	empty	Chinese	China
RT_MENU	0x98f290	0x2e8	empty	Chinese	China
RT_STRING	0x98f578	0x1f8	empty	English	United States
RT_STRING	0x98f770	0x1f8	empty	English	United States
RT_STRING	0x98f968	0x224	empty	English	United States
RT_STRING	0x98fb8c	0x1c2	empty	English	United States
RT_STRING	0x98fd50	0x1f8	empty	English	United States
RT_STRING	0x98ff48	0x388	empty	English	United States
RT_STRING	0x9902d0	0x714	empty	English	United States
RT_STRING	0x9909e4	0x74a	empty	English	United States
RT_STRING	0x991130	0x716	empty	English	United States
RT_STRING	0x991848	0x7ce	empty	English	United States
RT_STRING	0x992018	0x658	empty	English	United States
RT_STRING	0x992670	0x660	empty	English	United States
RT_STRING	0x992cd0	0x660	empty	English	United States
RT_STRING	0x993330	0x660	empty	English	United States
RT_STRING	0x993990	0x660	empty	English	United States
RT_STRING	0x993ff0	0x66c	empty	English	United States
RT_STRING	0x99465c	0x6c0	empty	English	United States
RT_STRING	0x994d1c	0x6c0	empty	English	United States
RT_STRING	0x9953dc	0x6c0	empty	English	United States
RT_STRING	0x995a9c	0x6c0	empty	English	United States
RT_STRING	0x99615c	0x6c0	empty	English	United States
RT_STRING	0x99681c	0x640	empty	English	United States
RT_STRING	0x996e5c	0x640	empty	English	United States
RT_STRING	0x99749c	0x640	empty	English	United States
RT_STRING	0x997adc	0x640	empty	English	United States
RT_STRING	0x99811c	0x640	empty	English	United States
RT_STRING	0x99875c	0x2a4	empty	English	United States
RT_STRING	0x998a00	0x24c	empty	English	United States
RT_STRING	0x998c4c	0x234	empty	English	United States
RT_STRING	0x998e80	0x208	empty	English	United States
RT_STRING	0x999088	0x204	empty	English	United States
RT_STRING	0x99928c	0x27c	empty	English	United States
RT_STRING	0x999508	0x2a0	empty	English	United States
RT_STRING	0x9997a8	0x2a0	empty	English	United States
RT_STRING	0x999a48	0x2a0	empty	English	United States
RT_STRING	0x999ce8	0x2a0	empty	English	United States
RT_STRING	0x999f88	0x2dc	empty	English	United States
RT_STRING	0x99a264	0x300	empty	English	United States
RT_STRING	0x99a564	0x300	empty	English	United States
RT_STRING	0x99a864	0x300	empty	English	United States
RT_STRING	0x99ab64	0x300	empty	English	United States
RT_STRING	0x99ae64	0x2c0	empty	English	United States
RT_STRING	0x99b124	0x280	empty	English	United States
RT_STRING	0x99b3a4	0x280	empty	English	United States
RT_STRING	0x99b624	0x280	empty	English	United States
RT_STRING	0x99b8a4	0x280	empty	English	United States
RT_STRING	0x99bb24	0x48a	empty	English	United States
RT_STRING	0x99bfb0	0x81e	empty	English	United States
RT_STRING	0x99c7d0	0x7ec	empty	English	United States
RT_STRING	0x99cfbc	0x84c	empty	English	United States
RT_STRING	0x99d808	0x862	empty	English	United States
RT_STRING	0x99e06c	0x88c	empty	English	United States
RT_STRING	0x99e8f8	0xf70	empty	English	United States
RT_STRING	0x99f868	0xdfa	empty	English	United States
RT_STRING	0x9a0664	0xe38	empty	English	United States
RT_STRING	0x9a149c	0xef4	empty	English	United States
RT_STRING	0x9a2390	0xcf8	empty	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x9a3088	0x1072	empty	English	United States
RT_STRING	0x9a40fc	0x1064	empty	English	United States
RT_STRING	0x9a5160	0xfd6	empty	English	United States
RT_STRING	0x9a6138	0x1082	empty	English	United States
RT_STRING	0x9a71bc	0xe0e	empty	English	United States
RT_STRING	0x9a7fcc	0xec6	empty	English	United States
RT_STRING	0x9a8e94	0x1008	empty	English	United States
RT_STRING	0x9a9e9c	0xe3e	empty	English	United States
RT_STRING	0x9aacdc	0xf74	empty	English	United States
RT_STRING	0x9abc50	0xe08	empty	English	United States
RT_STRING	0x9aca58	0x95c	empty	English	United States
RT_STRING	0x9ad3b4	0xa1a	empty	English	United States
RT_STRING	0x9addd0	0x8fe	empty	English	United States
RT_STRING	0x9ae6d0	0xa98	empty	English	United States
RT_STRING	0x9af168	0x9be	empty	English	United States
RT_STRING	0x9afb28	0x8d8	empty	English	United States
RT_STRING	0x9b0400	0xb56	empty	English	United States
RT_STRING	0x9b0f58	0x98a	empty	English	United States
RT_STRING	0x9b18e4	0xac8	empty	English	United States
RT_STRING	0x9b23ac	0xa96	empty	English	United States
RT_STRING	0x9b2e44	0x686	empty	English	United States
RT_STRING	0x9b34cc	0x632	empty	English	United States
RT_STRING	0x9b3b00	0x69c	empty	English	United States
RT_STRING	0x9b419c	0x704	empty	English	United States
RT_STRING	0x9b48a0	0x63a	empty	English	United States
RT_STRING	0x9b4edc	0x788	empty	English	United States
RT_STRING	0x9b5664	0x8da	empty	English	United States
RT_STRING	0x9b5f40	0x84e	empty	English	United States
RT_STRING	0x9b6790	0x880	empty	English	United States
RT_STRING	0x9b7010	0x852	empty	English	United States
RT_STRING	0x9b7864	0x9d2	empty	English	United States
RT_STRING	0x9b8238	0x11b8	empty	English	United States
RT_STRING	0x9b93f0	0x11e6	empty	English	United States
RT_STRING	0x9ba5d8	0xfb0	empty	English	United States
RT_STRING	0x9bb588	0x120a	empty	English	United States
RT_STRING	0x9bc794	0xc5c	empty	English	United States
RT_STRING	0x9bd3f0	0x9e4	empty	English	United States
RT_STRING	0x9bddd4	0xa5a	empty	English	United States
RT_STRING	0x9be830	0x9c0	empty	English	United States
RT_STRING	0x9bf1f0	0xa2a	empty	English	United States
RT_STRING	0x9bfc1c	0xab6	empty	English	United States
RT_STRING	0x9c06d4	0x1cec	empty	English	United States
RT_STRING	0x9c23c0	0x1d70	empty	English	United States
RT_STRING	0x9c4130	0x1baa	empty	English	United States
RT_STRING	0x9c5cdc	0x1dc8	empty	English	United States
RT_STRING	0x9c7aa4	0x19b2	empty	English	United States
RT_STRING	0x9c9458	0xc0	empty	English	United States
RT_STRING	0x9c9518	0xc0	empty	English	United States
RT_STRING	0x9c95d8	0xc8	empty	English	United States
RT_STRING	0x9c96a0	0xc0	empty	English	United States
RT_STRING	0x9c9760	0xcc	empty	English	United States
RT_STRING	0x9c982c	0xba6	empty	English	United States
RT_STRING	0x9ca3d4	0xdca	empty	English	United States
RT_STRING	0x9cb1a0	0xc14	empty	English	United States
RT_STRING	0x9cbdb4	0xdf6	empty	English	United States
RT_STRING	0x9ccbac	0xd0c	empty	English	United States
RT_STRING	0x9cd8b8	0x8da	empty	English	United States
RT_STRING	0x9ce194	0xab4	empty	English	United States
RT_STRING	0x9cec48	0x944	empty	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x9cf58c	0x9fa	empty	English	United States
RT_STRING	0x9cff88	0xa06	empty	English	United States
RT_STRING	0x9d0990	0x356	empty	English	United States
RT_STRING	0x9d0ce8	0x160	empty	English	United States
RT_STRING	0x9d0e48	0x160	empty	English	United States
RT_STRING	0x9d0fa8	0x160	empty	English	United States
RT_STRING	0x9d1108	0x160	empty	English	United States
RT_STRING	0x9d1268	0x150	empty	English	United States
RT_STRING	0x9d13b8	0x140	empty	English	United States
RT_STRING	0x9d14f8	0x140	empty	English	United States
RT_STRING	0x9d1638	0x140	empty	English	United States
RT_STRING	0x9d1778	0x140	empty	English	United States
RT_STRING	0x9d18b8	0x154	empty	English	United States
RT_STRING	0x9d1a0c	0x18e	empty	English	United States
RT_STRING	0x9d1b9c	0x186	empty	English	United States
RT_STRING	0x9d1d24	0x17c	empty	English	United States
RT_STRING	0x9d1ea0	0x178	empty	English	United States
RT_STRING	0x9d2018	0x194	empty	English	United States
RT_STRING	0x9d21ac	0x270	empty	English	United States
RT_STRING	0x9d241c	0x248	empty	English	United States
RT_STRING	0x9d2664	0x248	empty	English	United States
RT_STRING	0x9d28ac	0x2b2	empty	English	United States
RT_STRING	0x9d2b60	0x222	empty	English	United States
RT_STRING	0x9d2d84	0x1c0	empty	English	United States
RT_STRING	0x9d2f44	0x1c0	empty	English	United States
RT_STRING	0x9d3104	0x1c0	empty	English	United States
RT_STRING	0x9d32c4	0x1c0	empty	English	United States
RT_STRING	0x9d3484	0x1c0	empty	English	United States
RT_STRING	0x9d3644	0x84	empty	English	United States
RT_RCDATA	0x9d36c8	0x54af	empty		
RT_RCDATA	0x9d8b78	0x897	empty		
RT_GROUP_CURSOR	0x9d9410	0x14	empty		
RT_GROUP_CURSOR	0x9d9424	0x14	empty		
RT_GROUP_CURSOR	0x9d9438	0x14	empty		
RT_GROUP_CURSOR	0x9d944c	0x14	empty		
RT_GROUP_CURSOR	0x9d9460	0x22	empty		
RT_GROUP_CURSOR	0x9d9484	0x22	empty		
RT_GROUP_CURSOR	0x9d94a8	0x14	empty		
RT_GROUP_CURSOR	0x9d94bc	0x14	empty		
RT_GROUP_CURSOR	0x9d94d0	0x14	empty		
RT_GROUP_CURSOR	0x9d94e4	0x14	empty		
RT_GROUP_CURSOR	0x9d94f8	0x14	empty		
RT_GROUP_CURSOR	0x9d950c	0x14	empty		
RT_GROUP_CURSOR	0x9d9520	0x14	empty		
RT_GROUP_CURSOR	0x9d9534	0x14	empty		
RT_GROUP_CURSOR	0x9d9548	0x14	empty		
RT_GROUP_CURSOR	0x9d955c	0x14	empty		
RT_GROUP_CURSOR	0x9d9570	0x14	empty		
RT_GROUP_CURSOR	0x9d9584	0x14	empty		
RT_GROUP_CURSOR	0x9d9598	0x14	empty		
RT_GROUP_CURSOR	0x9d95ac	0x14	empty		
RT_GROUP_CURSOR	0x9d95c0	0x14	empty		
RT_GROUP_ICON	0x9f4c20	0x14	data		
RT_VERSION	0x9f4c74	0x358	data	English	United States
RT_MANIFEST	0x9f500c	0x425	XML 1.0 document, ASCII text, with very long lines (1061), with no line terminators	English	United States
None	0x9d9d68	0x1dc	empty	Russian	Russia
None	0x9d9f44	0x724	empty	Russian	Russia
None	0x9da668	0x1f8	empty	Russian	Russia

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
None	0x9da860	0x204	empty	Russian	Russia
None	0x9daa64	0x188	empty	Russian	Russia
None	0x9dabec	0x11c	empty	Russian	Russia
None	0x9dad08	0x94	empty	Russian	Russia
None	0x9dad9c	0x7c	empty	Russian	Russia
None	0x9dae18	0x180	empty	Russian	Russia
None	0x9daf98	0x278	empty	Russian	Russia
None	0x9db210	0x7d8	empty	Russian	Russia
None	0x9db9e8	0x124	empty	Russian	Russia
None	0x9dbb0c	0x2e8	empty	Russian	Russia
None	0x9dbdf4	0x128	empty	Russian	Russia
None	0x9dbf1c	0x228	empty	Russian	Russia
None	0x9dc144	0x114	empty	Russian	Russia
None	0x9dc258	0x158	empty	Russian	Russia

Imports

DLL	Import
KERNEL32.DLL	GetModuleHandleA, GetProcAddress
ole32.dll	OleInitialize
OLEAUT32.dll	SafeArrayCreate
USER32.dll	GetProcessWindowStation

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	
Chinese	China	
Russian	Russia	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4185.206.213.3249696427942850286 11/24/22-19:43:22.900750	TCP	2850286	ETPRO TROJAN Redline Stealer TCP CnC Activity	49696	42794	192.168.2.4	185.206.213.32
192.168.2.4185.206.213.3249696427942850027 11/24/22-19:43:19.130595	TCP	2850027	ETPRO TROJAN RedLine Stealer TCP CnC net.tcp Init	49696	42794	192.168.2.4	185.206.213.32
185.206.213.32192.168.2.442794496962850353 11/24/22-19:43:20.869342	TCP	2850353	ETPRO MALWARE Redline Stealer TCP CnC - Id1Response	42794	49696	185.206.213.32	192.168.2.4

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:43:18.693483114 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:18.722625017 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:18.726129055 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:19.130594969 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:19.161923885 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:19.308361053 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:20.836399078 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:20.869342089 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:21.011712074 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:22.900749922 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:22.941775084 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:22.941839933 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:22.941886902 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:22.941932917 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:22.941987991 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:22.941994905 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:22.942058086 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:23.011904955 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.912053108 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.939960957 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.940021992 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.940057039 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.940085888 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.940196037 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.940273046 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.967849016 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.967904091 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.967935085 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.967983961 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.968269110 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.968297958 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.968331099 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.968363047 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.968411922 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.968472958 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.968477011 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.968564034 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.996155977 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996207952 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996241093 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996309996 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996339083 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996391058 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996531963 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.996648073 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.996655941 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996687889 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.996743917 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.996815920 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.996905088 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:36.997243881 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.997409105 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.997534037 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.997565031 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.997592926 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.997670889 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.997924089 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:36.998081923 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:37.024167061 CET	42794	49696	185.206.213.32	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2022 19:43:37.024219990 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024291992 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024322033 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024352074 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024401903 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:37.024766922 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024796963 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024919033 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.024983883 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025053978 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025084972 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025212049 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025309086 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025352001 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025489092 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025522947 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025625944 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025733948 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025765896 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025794029 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025821924 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025898933 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.025928020 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026026011 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026057005 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026170969 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026201010 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026202917 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:37.026298046 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026329994 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026387930 CET	49696	42794	192.168.2.4	185.206.213.32
Nov 24, 2022 19:43:37.026410103 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026635885 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026665926 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026694059 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026724100 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026802063 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026909113 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026943922 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.026973009 CET	42794	49696	185.206.213.32	192.168.2.4
Nov 24, 2022 19:43:37.027055979 CET	42794	49696	185.206.213.32	192.168.2.4

Statistics

No statistics

System Behavior

Analysis Process: UniverseCity.exe PID: **3836**, Parent PID: **3528**

General

Target ID:	0
Start time:	19:42:59
Start date:	24/11/2022

Path:	C:\Users\user\Desktop\UniverseCity.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\UniverseCity.exe
Imagebase:	0x400000
File size:	4881408 bytes
MD5 hash:	2815815F0488B3D2307C3A914DDC1D7A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.392074868.0000000003481000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D84CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D84CF06	unknown
C:\Users\user\AppData\Local\Microsoft\Wind?ws	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C69BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UniverseCity.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB5C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\UniverseCity.exe.log	0	2201	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB5C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D825705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D825705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D82CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D7803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D825705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D825705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C691B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	20	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	14	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	2	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	5	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	2	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	10	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	45	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	3	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	36	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	3	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	45	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	3	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	69	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	3	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	31	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	273	end of file	2	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	44	6C691B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	6C691B4F	ReadFile

Disassembly

No disassembly