

JOeSandbox Cloud BASIC



ID: 321440

Sample Name: test.txt

Cookbook: default.jbs

Time: 06:14:18

Date: 22/11/2020

Version: 31.0.0 Red Diamond

Table of Contents

| | |
|---|---|
| Table of Contents | 2 |
| Analysis Report test.txt | 3 |
| Overview | 3 |
| General Information | 3 |
| Detection | 3 |
| Signatures | 3 |
| Classification | 3 |
| Startup | 3 |
| Malware Configuration | 3 |
| Yara Overview | 3 |
| Sigma Overview | 3 |
| Signature Overview | 3 |
| Mitre Att&ck Matrix | 4 |
| Behavior Graph | 4 |
| Screenshots | 5 |
| Thumbnails | 5 |
| Antivirus, Machine Learning and Genetic Malware Detection | 6 |
| Initial Sample | 6 |
| Dropped Files | 6 |
| Unpacked PE Files | 6 |
| Domains | 6 |
| URLs | 6 |
| Domains and IPs | 6 |
| Contacted Domains | 7 |
| Contacted IPs | 7 |
| General Information | 7 |
| Simulations | 7 |
| Behavior and APIs | 7 |
| Joe Sandbox View / Context | 8 |
| IPs | 8 |
| Domains | 8 |
| ASN | 8 |
| JA3 Fingerprints | 8 |
| Dropped Files | 8 |
| Created / dropped Files | 8 |
| Static File Info | 8 |
| General | 8 |
| File Icon | 8 |
| Network Behavior | 8 |
| Code Manipulations | 9 |
| Statistics | 9 |
| System Behavior | 9 |
| Analysis Process: notepad.exe PID: 1708 Parent PID: 5636 | 9 |
| General | 9 |
| File Activities | 9 |
| Disassembly | 9 |
| Code Analysis | 9 |

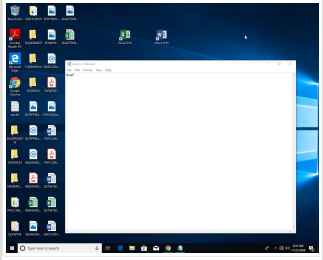
Analysis Report test.txt

Overview

General Information

| | |
|--------------|-------------------|
| Sample Name: | test.txt |
| Analysis ID: | 321440 |
| MD5: | 8d41627e46d5b8.. |
| SHA1: | cc40d8f62aa3775.. |
| SHA256: | 8898a8a3459079.. |

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

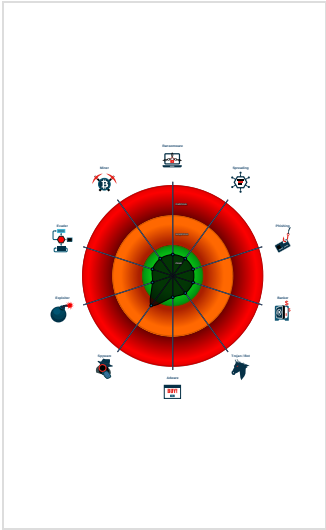
UNKNOWN

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


Signatures

Queries the volume information (nam...

Classification



Startup

- System is w10x64
-  notepad.exe (PID: 1708 cmdline: 'C:\Windows\system32\notepad.exe' C:\Users\user\Desktop\test.txt MD5: BB9A06B8F2DD9D24C77F389D7B2B58D2)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- System Summary
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection



💡 Click to jump to signature section

There are no malicious signatures, [click here to show all signatures](#).

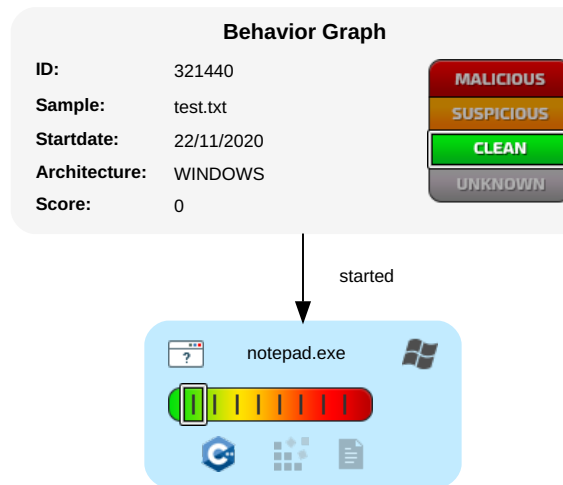
Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | Network Effects | Remote Service Effects | Impact |
|------------------|------------------------------------|--------------------------------------|--------------------------------------|---------------------|-----------------------|----------------------------------|-------------------------|---------------------------|--|---------------------|---|---|-------------------------|
| Valid Accounts | Windows Management Instrumentation | Path Interception | Process Injection 1 | Process Injection 1 | OS Credential Dumping | Process Discovery 1 | Remote Services | Data from Local System | Exfiltration Over Other Network Medium | Data Obfuscation | Eavesdrop on Insecure Network Communication | Remotely Track Device Without Authorization | Modify System Partition |
| Default Accounts | Scheduled Task/Job | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Rootkit | LSASS Memory | System Information Discovery 1 1 | Remote Desktop Protocol | Data from Removable Media | Exfiltration Over Bluetooth | Junk Data | Exploit SS7 to Redirect Phone Calls/SMS | Remotely Wipe Data Without Authorization | Device Lockout |

Behavior Graph

Legend:

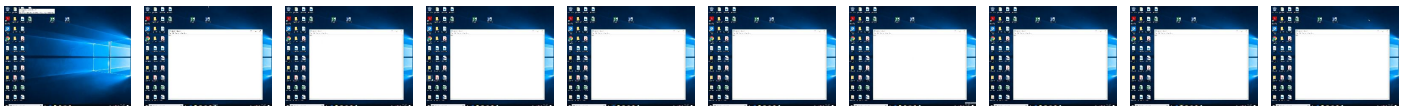
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

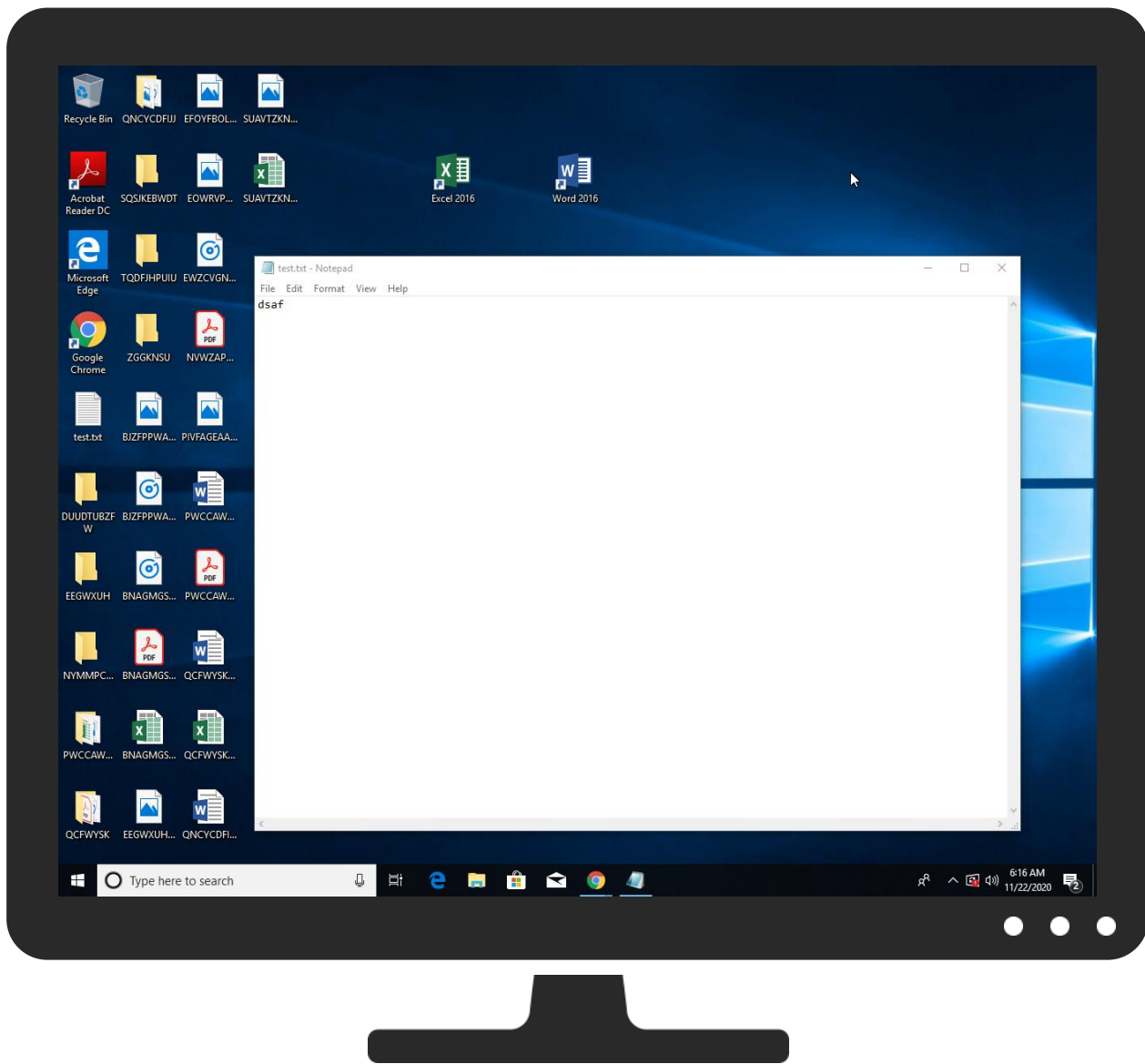


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

| | |
|--|--|
| Joe Sandbox Version: | 31.0.0 Red Diamond |
| Analysis ID: | 321440 |
| Start date: | 22.11.2020 |
| Start time: | 06:14:18 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 3m 59s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | test.txt |
| 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: | 23 |
| 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: | <ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | CLEAN |
| Classification: | clean0.winTXT@1/0@0/0 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | <ul style="list-style-type: none">• Successful, ratio: 100%• Number of executed functions: 0• Number of non-executed functions: 0 |
| Cookbook Comments: | <ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .txt |
| Warnings: | Show All <ul style="list-style-type: none">• Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, Usoclient.exe• Report size getting too big, too many NtProtectVirtualMemory calls found. |

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context


Created / dropped Files

No created / dropped files found

Static File Info

| General | |
|-----------------------|---|
| File type: | ASCII text, with no line terminators |
| Entropy (8bit): | 2.0 |
| TrID: | |
| File name: | test.txt |
| File size: | 4 |
| MD5: | 8d41627e46d5b8556d0d3e30ec15538e |
| SHA1: | cc40d8f62aa37759291bbc2d37728e8f9ad66232 |
| SHA256: | 8898a8a3459079ed8a03f66c2ae22f0f6c340af31a9756f67dae8e02807d7c97 |
| SHA512: | b0f9f266906aff90b14987e7f3189c9d87c00aad57bf4f26b0f330945cf12bc18d0c5f60ba555507cc8b68d029f361bfbе20a9755f7af20c6914ca4d7ba7612 |
| SSDEEP: | 3:1:1 |
| File Content Preview: | dsaf |

File Icon

| | |
|---|------------------|
|  | |
| Icon Hash: | 74f4e4e4e4e4e4e4 |

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: notepad.exe PID: 1708 Parent PID: 5636

General

| | |
|-------------------------------|--|
| Start time: | 06:15:07 |
| Start date: | 22/11/2020 |
| Path: | C:\Windows\System32\notepad.exe |
| Wow64 process (32bit): | false |
| Commandline: | 'C:\Windows\system32\notepad.exe' C:\Users\user\Desktop\test.txt |
| Imagebase: | 0x7ff7977d0000 |
| File size: | 245760 bytes |
| MD5 hash: | BB9A06B8F2DD9D24C77F389D7B2B58D2 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | C, C++ or other language |
| Reputation: | moderate |

File Activities

| File Path | Offset | Length | Completion | Count | Source Address | Symbol |
|-----------|--------|--------|------------|-------|----------------|--------|
|-----------|--------|--------|------------|-------|----------------|--------|

Disassembly

Code Analysis