JoeSandbox Cloud BASIC

ID: 795655
Sample Name: BTVA.jpg.lnk
Cookbook: default.jbs
Time: 06:46:09
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

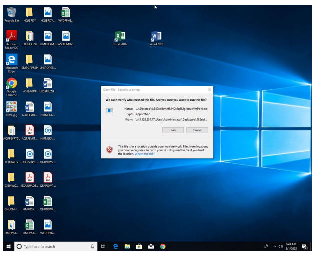
Windows Analysis Report

BTVA.jpg.lnk

Overview

General Information

Sample Name:	BTVA.jpg.lnk
Analysis ID:	795655
MD5:	50c81ec9e93c…
SHA1:	d91a27e9cb7e…
SHA256:	d304e28d717a…
Tags:	Amadey lnk



Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

Name: ...r\Desktop\u\582eblhmhfNHDMqEMgKmukYmPoN.exe
Type: Application
From: \\45.128.234.77\Users\Administrator\Desktop\u\582ebl...

Run Cancel

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only run this file if you trust the location. What's the risk?

Errors

⚠ No process behavior to analyse as no analysis process or sample was found

Detection

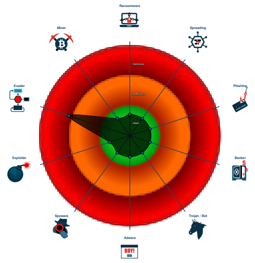
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Score:	20
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Uses an obfuscated file name to hid…

Classification



Malware Configuration

⊘ **No configs have been found**

Yara Signatures

⊘ **No yara matches**

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

⊘ **No Snort rule has matched**

Joe Sandbox Signatures

Hooking and other Techniques for Hiding and Protection

Uses an obfuscated file name to hide its real file extension (double extension)

Mitre Att&ck Matrix

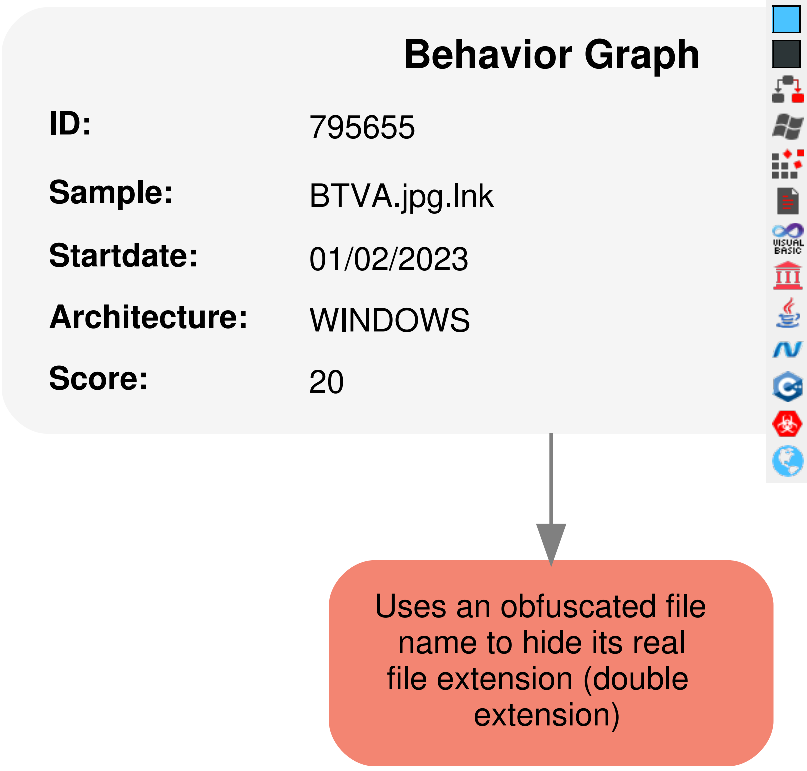
Initial Access	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**	**Credential Access**	**Discovery**	**Lateral Movement**	**Collection**	**Exfiltration**	**Command and Control**	**Network Effects**	**Remote Service Effects**	**Impact**
Valid Accounts	Windows Management Instrumentation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

Behavior Graph

Hide Legend

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



Behavior Graph

ID: 795655

Sample: BTVA.jpg.lnk

Startdate: 01/02/2023

Architecture: WINDOWS

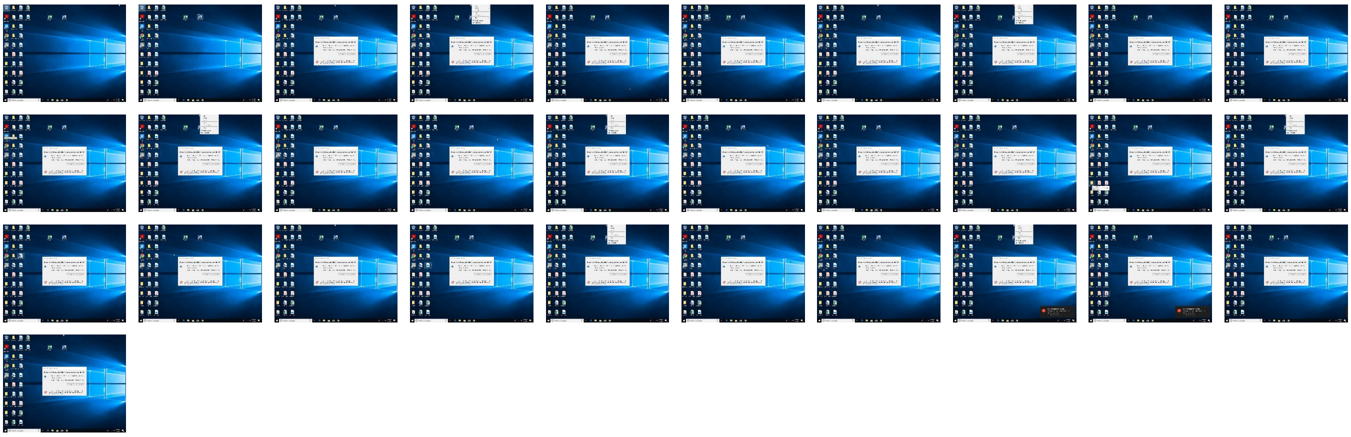
Score: 20

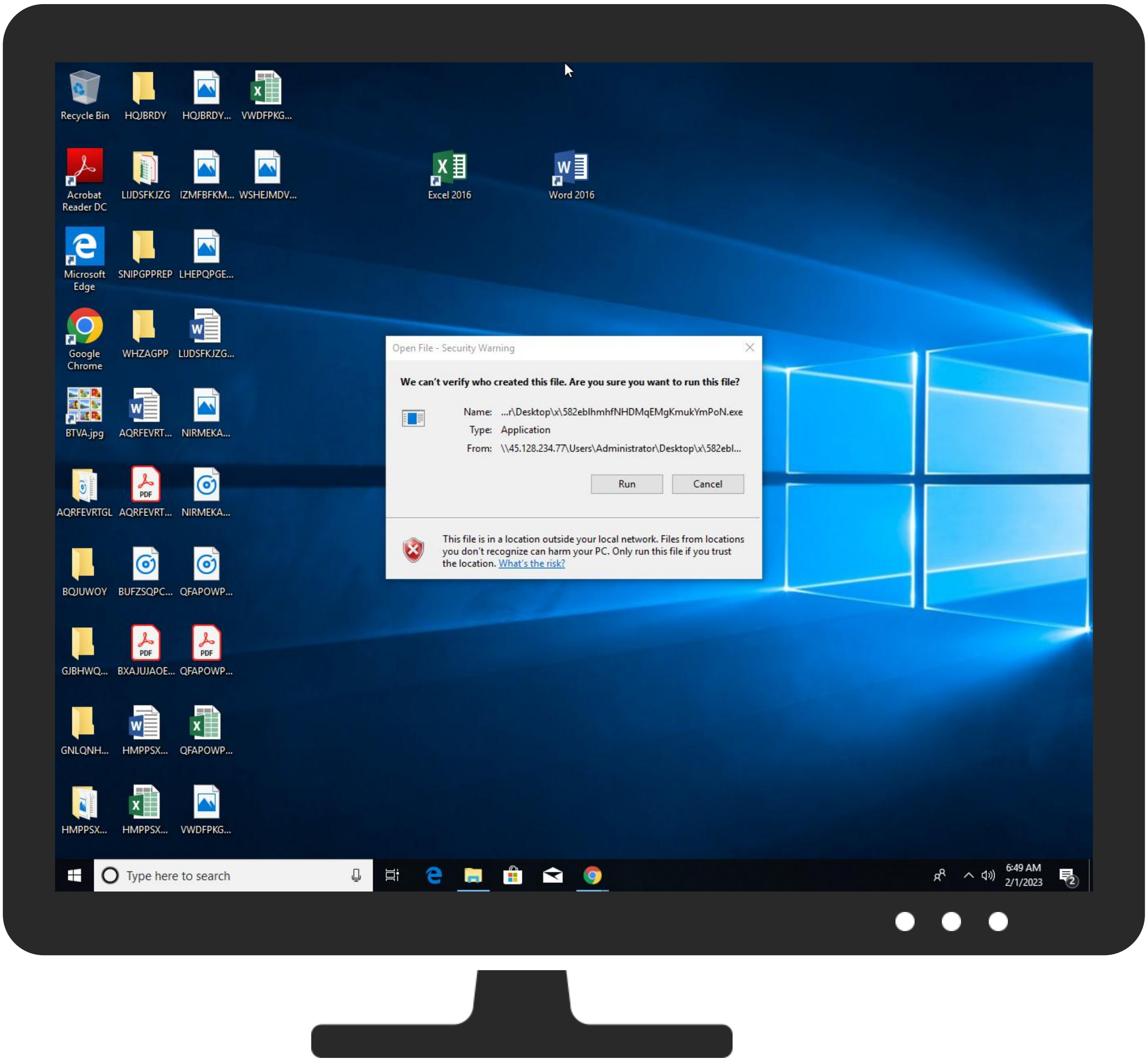
Uses an obfuscated file name to hide its real file extension (double extension)

Screenshots

Thumbnails

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





Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

Name: ...r\Desktop\x\582eblhmhfNHDMqEMgKmukYmPoN.exe
Type: Application
From: \\45.128.234.77\Users\Administrator\Desktop\x\582ebl...

Run Cancel

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only run this file if you trust the location. What's the risk?

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
BTVA.jpg.lnk	3%	ReversingLabs		
BTVA.jpg.lnk	0%	Virustotal		Browse

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	795655
Start date and time:	2023-02-01 06:46:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	14
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:	Power Change
Sample file name:	BTVA.jpg.lnk
Detection:	SUS
Classification:	sus20.evad.winLNK@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .lnk

Errors

- No process behavior to analyse as no analysis process or sam ple was found

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS Windows shortcut, Points to a file or directory, Icon number=325, Archive, ctime=Sat Dec 31 15:49:26 2022, mtime=Sat Dec 31 15:49:27 2022, atime=Sat Dec 31 15:49:27 2022, length=344576, window=hide
Entropy (8bit):	2.9726808797603415
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	BTVA.jpg.lnk
File size:	2601
MD5:	50c81ec9e93c43ee6142a56d96000886
SHA1:	d91a27e9cb7eb2f8ee8a952ec8d5db5cee1f90a9
SHA256:	d304e28d717a2af0c49337800bb901bdc85eb58ad82d32570b6ceb1df96da576
SHA512:	4a0035d4aec3488dbe659fdd720fcdb7a69b31e82226d0e3342a16d9c1c928f2dbedb709a665b2ff430678b6dfe7ba185129a03b51f19c32045dc8de7d6fcca2
SSDEEP:	24:8klg0oi9+/QT4I07nDfE589WqXIFJXwbXcqrsUAYYYop9DUAYEU:8k59fMI2DfnWqeJXcXtwfU
TLSH:	4A510F2527D6D306E370CA37E6E5C20AD22AB800BA11EB1F859482560C66609FD72B5E

File Content Preview:	L..................F.B.. ....5..6cs..5..6cs..5...B..E...................~........................F...*...................\\45.128.234.77\USERS.Administrator\Desktop\x\582eblhmhfNHDMqEMgKmukYmPoN.exe...C.:.\. W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.S.h.e.l.l.3

File Icon

Icon Hash:	b2ace8aaa8a9addd

Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	
Icon location:	C:\Windows\System32\Shell32.dll

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

⊘ **No statistics**

System Behavior

⊘ **No system behavior**

Disassembly

⊘ **No disassembly**