ID: 438547
Cookbook: browseurl.jbs
Time: 18:26:37
Date: 22/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

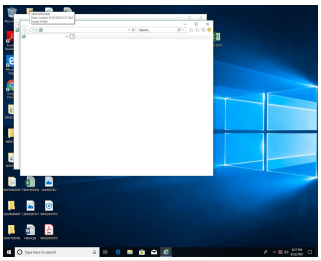
Windows Analysis Report http://bbowles@boohoffpa.co…

Overview

General Information

Sample URL:	http://bbowles@boohoffpa.com
Analysis ID:	438547
Infos:	

Most interesting Screenshot:



Errors

URL not reachable

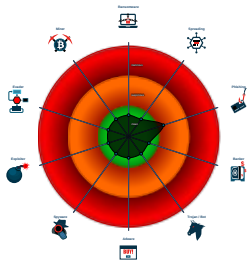
Detection

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

Signatures

URL contains potential PII (phishing…

Classification



Process Tree

- **System is w10x64**
- iexplore.exe (PID: 5908 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 528 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 660 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

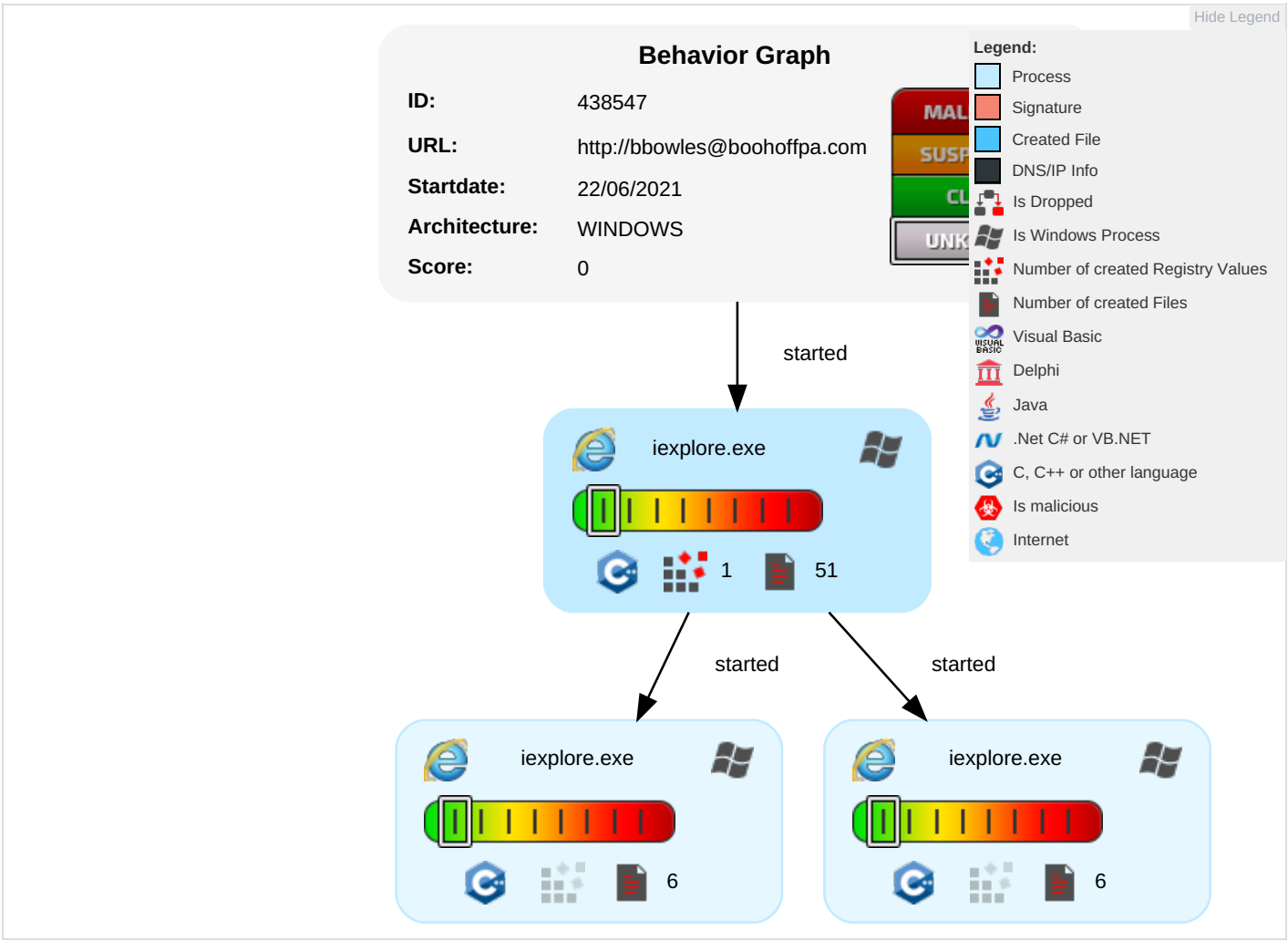
Click to jump to signature section

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	Masquerading 1	OS Credential Dumping	File and Directory 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	Process Injection 1	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

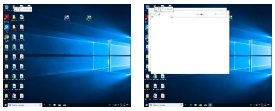
Behavior Graph

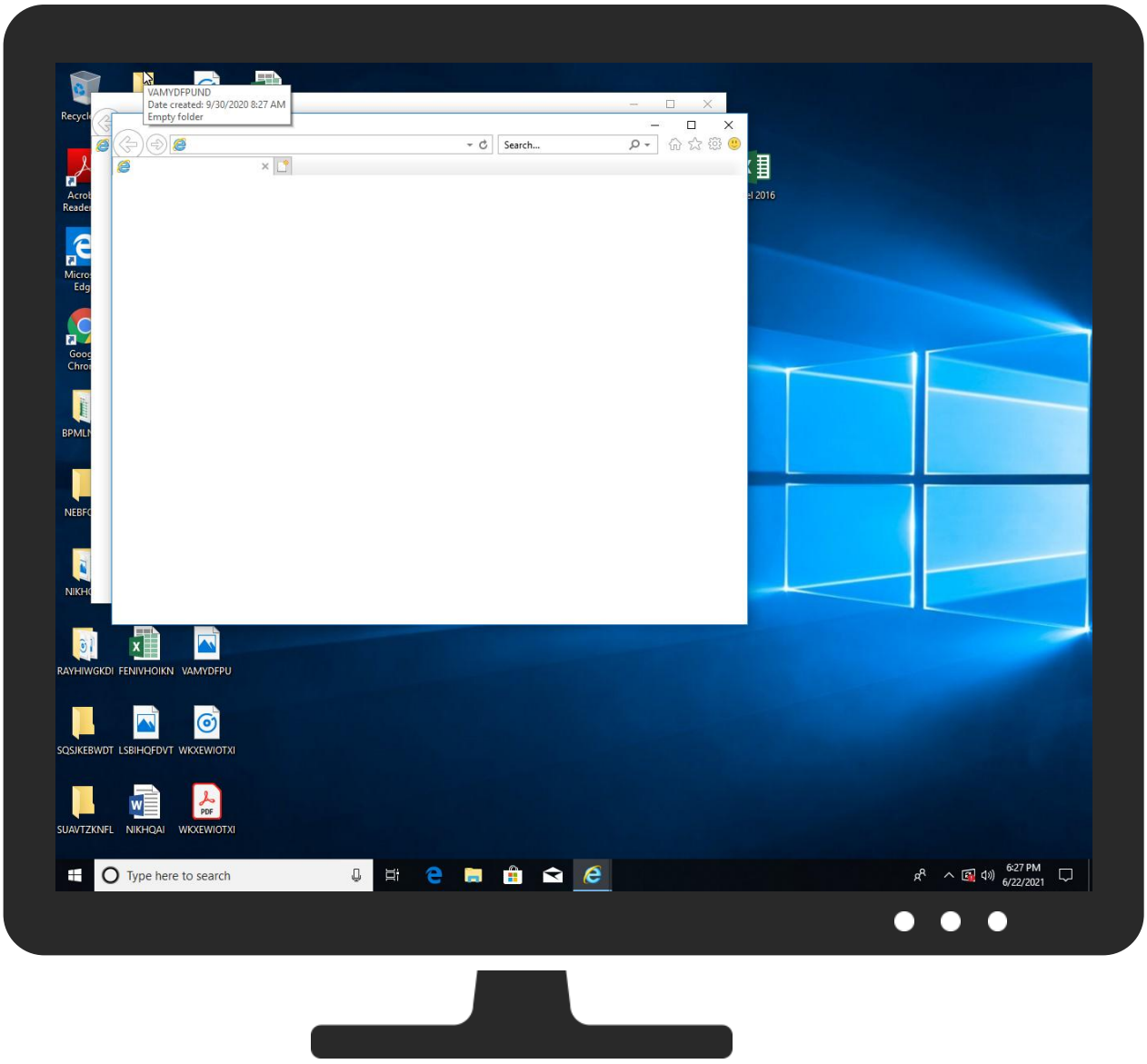


Screenshots

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
http://bbowles@boohoffpa.com	0%	Avira URL Cloud	safe	

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:	32.0.0 Black Diamond
Analysis ID:	438547
Start date:	22.06.2021
Start time:	18:26:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://bbowles@boohoffpa.com
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:	7
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@5/6@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Unable to create IE instance
Warnings:	Show All
Errors:	• URL not reachable

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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{2C1FA25A-D3C2-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	39624
Entropy (8bit):	1.9698488993518743
Encrypted:	false
SSDEEP:	192:r8Z3ZN2wWP7htPIfPm5BMsuekvjlyLW+Ks:r8JknP++Elekvj4i+Ks
MD5:	8EB1079B51CD33DB3CF22AE56B75ABC8
SHA1:	4E4AA475E01EB5CD3D45833F37D85D2D0A5BBDD4
SHA-256:	CF8D6AB5BF20EAF4600B307FD448FA1157BB8827FC789F9AFEF38E4A1C2A9DB3
SHA-512:	0E538F6CAFF2D1AA5F9264C552195F9C60402BC3F25538F3DC97EB7BA947DB27D625A5B61F3D4BFBE318FDCF7F7245106D4FB43A405CE1794AA3A6F27A7EF81C
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2C1FA25C-D3C2-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5713502635828598
Encrypted:	false
SSDEEP:	48:IwFGcprQGwpaDG4pQrGrapbS9GQpBeGHHpczTGUpG:rbZ4Q16fBSHjt2NA
MD5:	6088E2D39BE843F4CE2992FDD8A133EE
SHA1:	4A83E797E5908D653C08C3D3A196BE15CDD17BEC
SHA-256:	83C9F4DF6A47C301B3CB67A4F20104D2A869BA3728DF75822A17B1DEC8A9F5D6
SHA-512:	66FCD01EE321D3D14FCB03287F1D2BFA088F7CC49E06DB54ACB8FD277BEF117F07BE9D4EF71DA491B4B1519A88F695B59C8E4FE0DED34E81143A77F837EF33F3
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2C1FA25E-D3C2-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5740497429876874

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{2C1FA25E-D3C2-11EB-90E5-ECF4BB2D2496}.dat	
Encrypted:	false
SSDEEP:	48:IwWGcpr/fGwpak0G4pQimGrapbShqGQpBJtGGHHpcJ7RTGUpG:rKZ/pQkE6ioBSEjd21A
MD5:	6250646F1203F9A99913A823698D9671
SHA1:	2E0FD4C222EC99D7275F42FEB506C67C84B47EA0
SHA-256:	5243F6AC09045536AC0DE25E0CA5C7DFF3ABFAC7B2EF928806FB9D5B5D095A56
SHA-512:	3644508D6AEAD6E734B23353ECBF2EF14C090C03C83209E3D1B95661963E8F61EC085A5FC122776D85871CF54261F7C1500B031C6F294D6D800FDD4E51F8D9F5
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\~DF00B808E4ADDA9C45.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.3121569684630243
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwdh9lwdB9l2dY:kBqoxKAuvScS+IOe
MD5:	B468C87BB72DF8050A04F09F339D0F80
SHA1:	65351FC6353083B3CFB818B14E268CCA6571A772
SHA-256:	99232E8CF2D25105E37CE6144873B39E615EFB6F4F1CD6EE1178A4F99908357C
SHA-512:	2A8B558434903E18CFC8756DADB2488F7A3ED2681C84105914CD8CADCF92BDCA2937574F2EAA2A0517B7375204A6F0666A7A20F160513F14036B463CBC8E5FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF3919968C317FF79C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.314037824825452
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwJU29lwJB9l2JY:kBqoxKAuvScS+JSJ0JY
MD5:	B75377D181884FC9F379E2DF5C4679E2
SHA1:	4B712B3A8A1DF62B1B04161985A3E402FA8A3E02
SHA-256:	7FA5B20FC010224B36AD36139C38E623E88D0936F99E8D84F9FBF19861DCCE6A
SHA-512:	D374DED9DA4D874FDACF1B4BEE30E0070536DEA066EDAC9A70E1004441CAC32679F0D7F6FA8B6DEA6FCF4E94DC127AD853664066B8026D80783D39FAF0A71 75
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF74150F8D4F32A3FF.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13285
Entropy (8bit):	0.6314530063032683
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loa9loK9lWlVkeu2k52Gp2Gt3tu2GtR:kBqoIFzvkeXk57IZ
MD5:	7CA61D296775226EB6A2D7D9F91D7FA1
SHA1:	E34A653C45A291832F540FDDC8F2D97B03C1AA72
SHA-256:	0B98324A77FEF4F9471FD0369738C509EC3677E3E9DEBFD43ED899DFBA7DB06C
SHA-512:	2F838FA8E5726439164606B48A4FE748A2C7A4EC488C6DE970D03EE72B8697A21C60D3BDB638E4D68FE61659135A6BCFEAE1192A98E350F32F991CF8CAD8592
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF74150F8D4F32A3FF.TMP	
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

No static file info

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 5908 Parent PID: 792

General

Start time:	18:27:28
Start date:	22/06/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 528 Parent PID: 5908

General

Start time:	18:27:29
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:17410 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: iexplore.exe PID: 660 Parent PID: 5908

General

Start time:	18:27:30
Start date:	22/06/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5908 CREDAT:17414 /prefetch:2
Imagebase:	0xe20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly