

ID: 404271
Cookbook: browseurl.jbs
Time: 21:14:37
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report https://nt.embluemail.com/p/cl?data=3YZv0BlJbftfm9/Ve/nz8p/seVvfdz2Le2+1ZXk0LOjQU+QcnnZLoMMoa6mY23iqNfwKYtM500Jx312dmC8FWw==!-!5h1gq9!-!http://bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ= 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
AV Detection: 4
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 7
Contacted Domains 7
Contacted URLs 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 14
No static file info 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 15
UDP Packets 16
DNS Queries 17
DNS Answers 18
HTTP Request Dependency Graph 18
HTTP Packets 18
HTTPS Packets 20
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: iexplore.exe PID: 6464 Parent PID: 800 21
General 21
File Activities 22
Registry Activities 22
Analysis Process: iexplore.exe PID: 6532 Parent PID: 6464 22
General 22
File Activities 22
Registry Activities 22
Disassembly 22

Copyright Joe Security LLC 2021

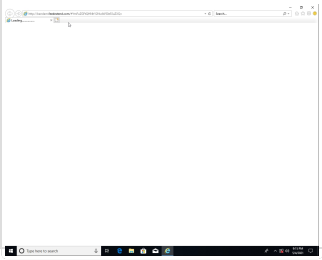
Analysis Report https://nt.embluemail.com/p/cl?data=3Y…

Overview

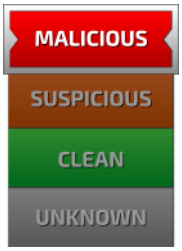
General Information

Sample URL:	https://nt.embluemail.com/p/cl?data=3YZv0BlJbftfm9/Ve/nz8p/seVvfdz2Le2+1ZXk...312dmC8FWw==!-!5h1gq9!-!bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=
Analysis ID:	404271
Infos:	

Most interesting Screenshot:



Detection



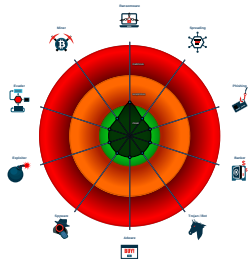
Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub…

Antivirus detection for URL or domain

Classification



Startup

- **System is w10x64**
- iexplore.exe (PID: 6464 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6532 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6464 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

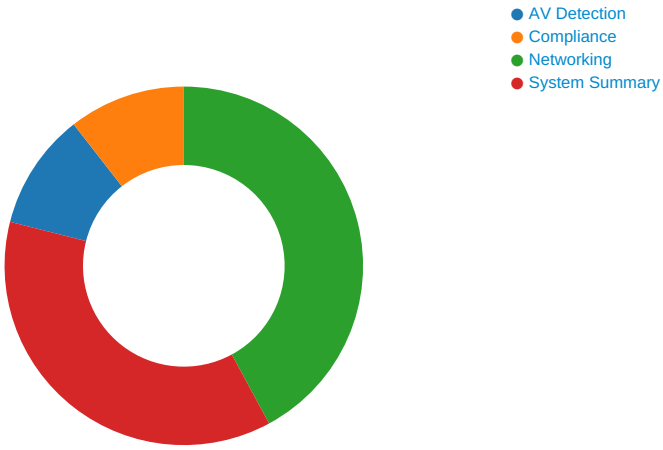
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:



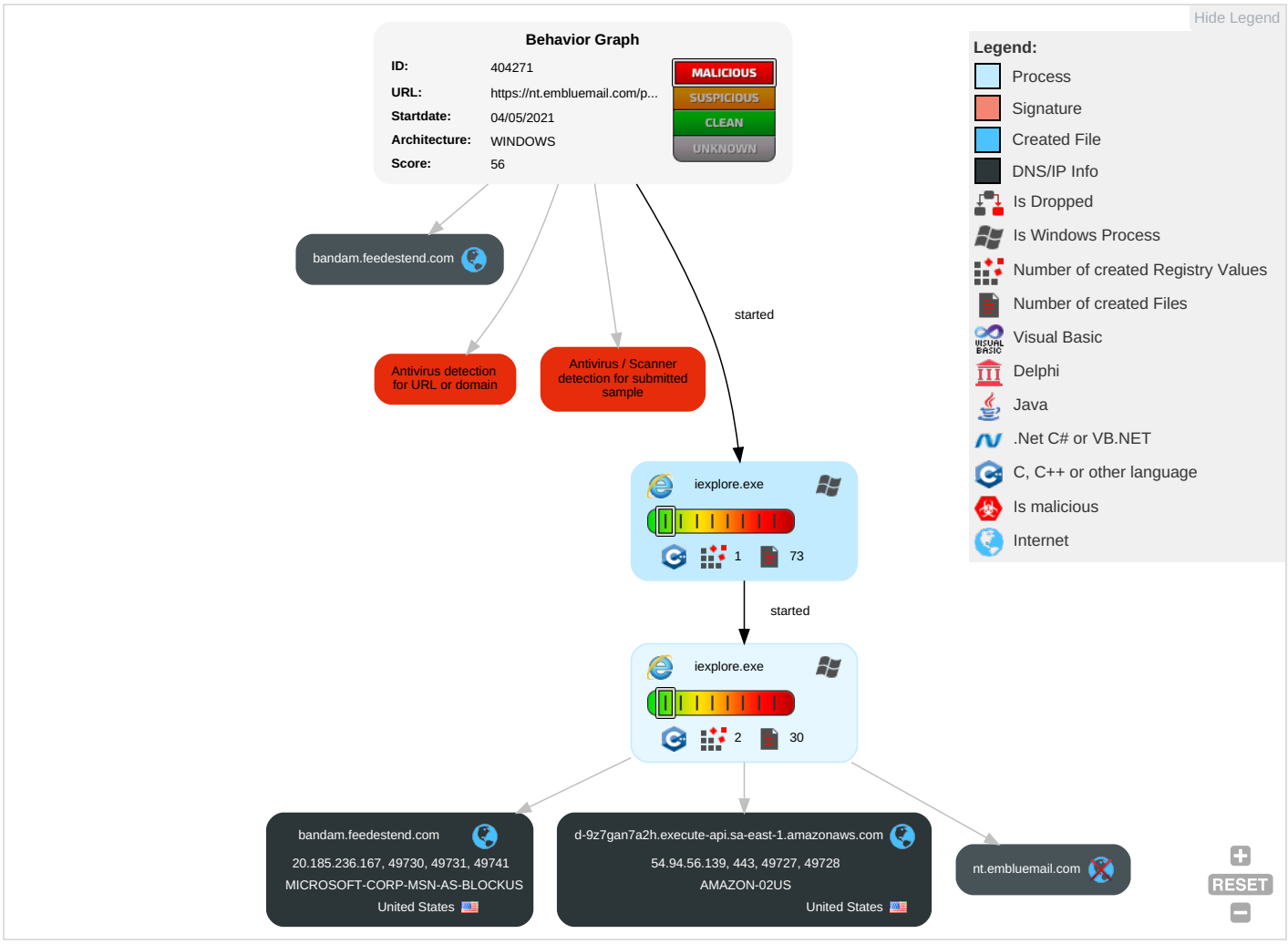
Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

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	Impa
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	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modif Syste Partit
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	Non-Application Layer Protocol 4	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devic Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 5	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delet Devic Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 4	SIM Card Swap		Carri Billing Fraud

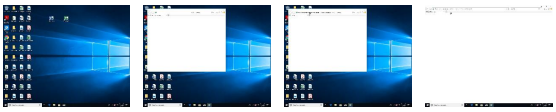
Behavior Graph

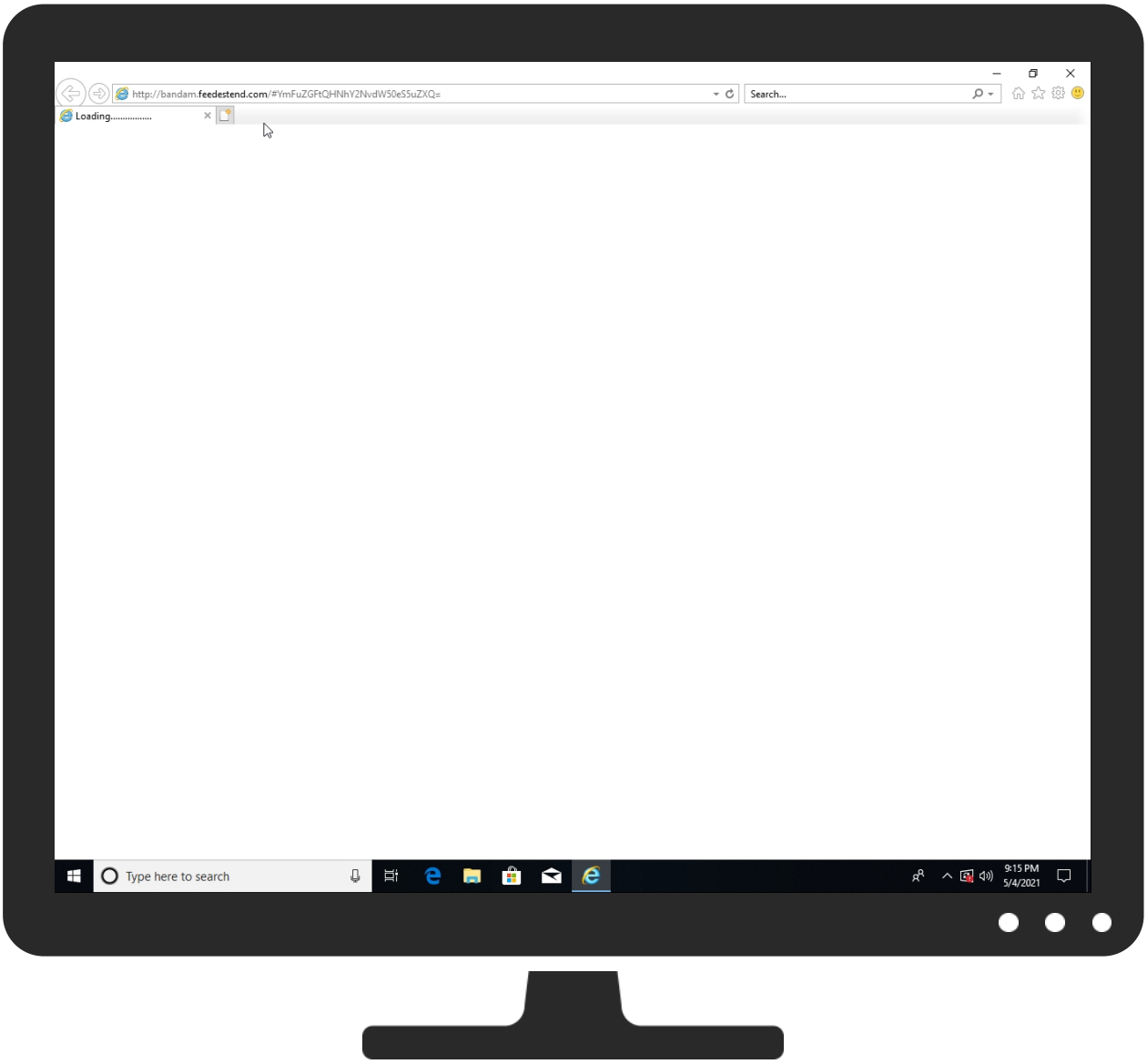


Screenshots

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://https://nt.embluemail.com/p/cl?data=3YZv0BlJbftfm9/Ve/nz8p/seVvfdz2Le2+1ZXk0LOjQU+QcnnZLoMMoa6mY23iqNfwKYtM500Jx312dmC8FWw==!-!5h1gq9!-!bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=	0%	Avira URL Cloud	safe	
http://https://nt.embluemail.com/p/cl?data=3YZv0BlJbftfm9/Ve/nz8p/seVvfdz2Le2+1ZXk0LOjQU+QcnnZLoMMoa6mY23iqNfwKYtM500Jx312dmC8FWw==!-!5h1gq9!-!bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=	100%	SlashNext	Fake Login Page type: Phishing & Social Engineering	
http://bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=Root	0%	Avira URL Cloud	safe	
http://bandam.feedestend.com/	0%	Avira URL Cloud	safe	
http://bandam.feedestend.com/favicon.ico	0%	Avira URL Cloud	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://www.wikipedia.com/	0%	URL Reputation	safe	
http://https://blencovents.net/o/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bandam.feedestend.com	20.185.236.167	true	false		unknown
d-9z7gan7a2h.execute-api.sa-east-1.amazonaws.com	54.94.56.139	true	false		high
nt.embluemail.com	unknown	unknown	false		high

Contacted URLs

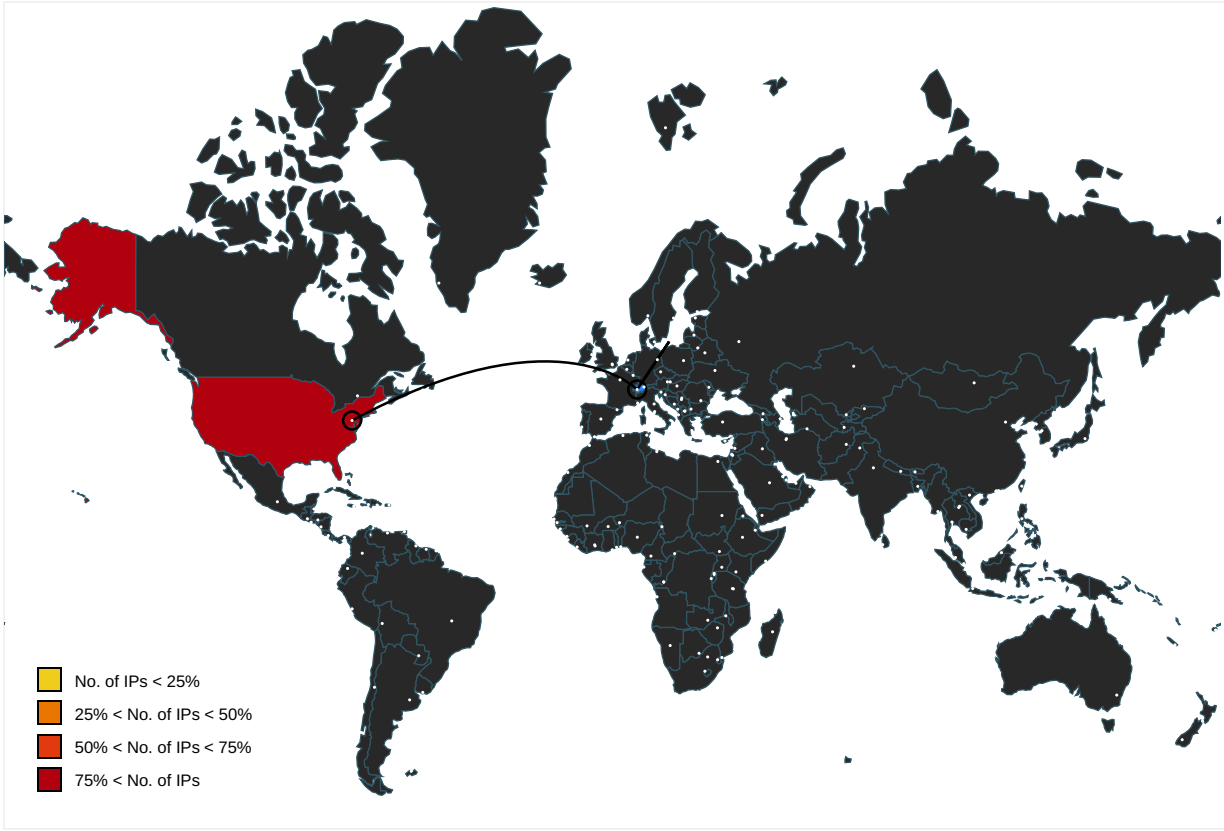
Name	Malicious	Antivirus Detection	Reputation
http://bandam.feedestend.com/	false	• Avira URL Cloud: safe	unknown
http://bandam.feedestend.com/favicon.ico	false	• Avira URL Cloud: safe	unknown
http://bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=Root	{13E99110-AD0D-11EB-90EB-ECF4BBEA1588}.dat.1.dr	true	• Avira URL Cloud: safe	unknown
http://www.nytimes.com/	msapplication.xml3.1.dr	false		high
http://bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=	~DF537922E49D7A1954.TMP.1.dr	true	• SlashNext: Fake Login Page type: Phishing & Social Engineering	unknown
http://www.youtube.com/	msapplication.xml7.1.dr	false		high
http://www.wikipedia.com/	msapplication.xml6.1.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.com/	msapplication.xml.1.dr	false		high
http://www.live.com/	msapplication.xml2.1.dr	false		high
http://https://blencovents.net/o/	RBDAB6LU.htm.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.webtoolkit.info/	RBDAB6LU.htm.2.dr	false		high
http://www.reddit.com/	msapplication.xml4.1.dr	false		high
http://www.twitter.com/	msapplication.xml5.1.dr	false		high

Contacted IPs

Copyright Joe Security LLC 2021



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.185.236.167	bandam.feedestend.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
54.94.56.139	d-9z7gan7a2h.execute-api.sa-east-1.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404271
Start date:	04.05.2021
Start time:	21:14:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://https://nt.embluemail.com/p/cl?data=3YZv0BlJbftfm9/Ve/nz8p/seVvfdz2Le2+1ZXk0LOjQU+QcnnZLoMMoa6mY23iqNfwKYtM500Jx312dmC8FWw==!-!5h1gq9!-!bandam.feedestend.com/#YmFuZGFtQHNhY2NvdW50eS5uZXQ=
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:	13
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

Copyright Joe Security LLC 2021

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal56.win@3/16@3/2
Cookbook Comments:	• Adjust boot time • Enable AMSI

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.{13E9910E-AD0D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8506362854520193
Encrypted:	false
SSDEEP:	192:r+Z9Zi2+Wgtiif09TzMfrBbxDUsfw9ajX:rKzB1kL19VDZ
MD5:	9A70D28072A9D2D402951C9A014F486E
SHA1:	2EC95A318C8469487CA856FA8A13B2960799BCFB
SHA-256:	321890123D5892B3F00D14FACD657C90382BFD8713377CBB407159DC61689404
SHA-512:	9FD4A65CFA180C737BDD68723CA3A5144D9C07BCF7C67A71C6C791F98A8A45B2049B0CD59E04525AB11550B43DB12552B0628E70B536E062B46B1C479BDF3C B
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\{13E99110-AD0D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	24228
Entropy (8bit):	1.6454651183520814
Encrypted:	false
SSDEEP:	48:Iw0GcprxGwpadG4pQNGrapbStZGQpByGHHpcXaTGUp8dGzYpmtlOGopR7jGGGmNg:roZrQf6tBStzjJ2XqWjMX+Xemg
MD5:	44B741AA655B1661195CFAD7C10660AE
SHA1:	2B6DEA9744249EBF117928CD2924C14C96EECCA3
SHA-256:	0D47E4DA95F3A599437343969ABA61E9D6F2DFD2564692E48EF5CFBEDCCFFFE9
SHA-512:	2CB31475DA1D6ADDA483445E86C66A54D087A46862D83476F6BC500DC802BE32B17139EB0B739EDD9D5FBC6F3D191259EF9E2A06F8A643B40484A26F4D6EA4 7
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\{13E99111-AD0D-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5673151035032187
Encrypted:	false
SSDEEP:	48:IwkEGcpryvGwpafG4pQiYGrapbSCZGQpKoG7HpRDaTGIpG:rPZcQx63BSCzAzTDeA
MD5:	48F91C6DE4A30388E961A6E1A4CD0E10
SHA1:	9B0706DED1675D8EC84A0CE18BA8EAE8332E769A
SHA-256:	8F3D4395C88EAF272AC3B3380246FB08A2D0BCB5DFC53DD2E488DFD86C38A83F
SHA-512:	3DD62ECEEF4400D775ADB0C3447F5BC0DE3D5FEDAF4DA8B97C95EDEDF45D11734076B15A86E0A97CF8F6A12B40807A7CE33DFC5F2261E56660587FE29C324 6E
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-17529550060\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.087242189199775
Encrypted:	false
SSDEEP:	12:TMHdNMNxOER/G6nWimI002EtM3MHdNMNxOER/G6nWimI00OYGVbkEtMb:2d6NxO8SZHKd6NxO8SZ7YLb
MD5:	1B1A7105D79CA76BE936F0961531D5CC
SHA1:	7A3DC50599D9BAA19BDABACBF2F65824268B2E30
SHA-256:	F02BD0CC350512EFB404806E1F26E7B34B471792D87E2E42C70BDB38FB9AE22A
SHA-512:	4053BD20544120465C4398F8FB9C354338DABA97D9B30D8B0CBF8E7E20285004140D9E4B7AEF011DC875C93300A0DA5A247373EEC296F741F7A72B32B5B904F0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xea72afb2,0x01d74119</date>< accdate>0xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<? xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.twitter.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0 xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Twitter.url"/></tile ></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.086582998774493
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-18270793970\msapplication.xml	
SSDEEP:	12:TMHdNMNxe2k0+tj+cnWimI002EtM3MHdNMNxe2k0+tj+cnWimI00OYGkak6EtMb:2d6NxrMSZHKd6NxrMSZ7Yza7b
MD5:	053A746110CB781F7D7DA3E4BD4DEF6C
SHA1:	5C9DE8D4E66C352CCBE61721B68597E014E7AD68
SHA-256:	36BEC784ACA35DC636EC85C172F00ED36D7B1349D895F3E16E3465317989856F
SHA-512:	4146B597E036AAF15E2C937720115A054957FD9ACD032FD4C9CB3D1D62B2106D739ED9C763F08C6E0D9170058277E8AC9265B0D48628760F87227D939BD45C72
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xea6dead6,0x01d74119</date><accdate>0xea6dead6,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.amazon.com/"/><date>0xea6dead6,0x01d74119</date><accdate>0xea6dead6,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Amazon.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-21706820\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	662
Entropy (8bit):	5.1066125315446325
Encrypted:	false
SSDEEP:	12:TMHdNMNxvLR/G6nWimI002EtM3MHdNMNxvLR/j3nWimI00OYGmZEtMb:2d6NxvFSZHKd6Nxvp3SZ7Yjb
MD5:	50DE467EF40119CCD0677E2D54F400C1
SHA1:	E3CA05BDDD6758254FE480A48735ECAE48E5B47A
SHA-256:	64A8E1A19874FE566D7DB351E0E9EF8D0A996B963FC8185046704341767E1E62
SHA-512:	7EC81CA283FF2D50EF3F36343993FD23874BFCE6CD974FD27BD94A04A9323B0CF95C090838A2DC3AD0758888FCB9914B032F0BA78774ACC4345C7FEEC70675
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.wikipedia.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0xea7511fb,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Wikipedia.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-4759708130\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	647
Entropy (8bit):	5.07727268746815
Encrypted:	false
SSDEEP:	12:TMHdNMNxiaSnWimI002EtM3MHdNMNxiaSnWimI00OYGd5EtMb:2d6NxkSZHKd6NxkSZ7YEjb
MD5:	501A0479D70C382E8BBB2DDBF505CCB9
SHA1:	BC05521DBF364E2B2FDFAA0E1149554AD4CC053B
SHA-256:	41E47B3605D83E94D902CC7803B32FCF77819FB414AEA5C244B8A2734E4186D4
SHA-512:	CFE2BDB418A8554AF7A64E3C2697C96319025CF9943AD0A79DB84694BDDCC37ECEBF4B14C46441B21A4DCE96339CF4D61234DAF4A3E36B37786520A1309244 6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xea704d80,0x01d74119</date><accdate>0xea704d80,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.live.com/"/><date>0xea704d80,0x01d74119</date><accdate>0xea704d80,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Live.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.098305468768132
Encrypted:	false
SSDEEP:	12:TMHdNMNxhGwUYj3nWimI002EtM3MHdNMNxhGwUYj3nWimI00OYG8K075EtMb:2d6NxQ743SZHKd6NxQ743SZ7YrKajb
MD5:	7041FCF0CFD367A2AFCA7064614D2C10
SHA1:	36B94941962D6CA1DDBE400FF4DADAE1E565A3DE
SHA-256:	B946EA6B443E9E2864F700D5F0A3D4CF81DF74E03FB64474E5A7DD34B6F3F77C

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-6757900\msapplication.xml	
SHA-512:	79E4F9BCA646650134FF6DA98F460DC21AF478325A1F86BFADF89C57BE34423906622AC1BA5CDFFB865A085F4530EBAB617BA066FA2EFA6534B6870EE732A00D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xea7511fb,0x01d74119</date><accdate>0xea7511fb,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.youtube.com/"/><date>0xea7511fb,0x01d74119</date><accdate>0xea7511fb,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Youtube.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin-8760897390\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.090973694827981
Encrypted:	false
SSDEEP:	12:TMHdNMNx0nR/G6nWimI002EtM3MHdNMNx0nR/G6nWimI00OYGxEtMb:2d6Nx0JSZHKd6Nx0JSZ7Ygb
MD5:	F81650DA01DAF65EBDF5BE5AF1AC86A7
SHA1:	38BBE047B5AAE5599C0FB6154EEF5EBC13ABDE74
SHA-256:	6F58DD3F0487C791B159582C05CE5EBEC4FFD27B41F0E54F2DAE024CFFA297AA
SHA-512:	1883422A08396BD945F15D2E35A8F68F16201E8FE333B963D40F82748BE5B9DDC4E7C8A5BAB3AA75C056F0749E97D77A61D981D2FB90EF8618062AD1D89EDCA
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.reddit.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Reddit.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20259167780\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	656
Entropy (8bit):	5.126877468527568
Encrypted:	false
SSDEEP:	12:TMHdNMNxxR/G6nWimI002EtM3MHdNMNxxR/G6nWimI00OYG6Kq5EtMb:2d6NxbSZHKd6NxbSZ7Yhb
MD5:	BC9DCBEA3DB4200720FC9DCD41CA8D11
SHA1:	0FB406D4DC629549AC50138533CEAFBD2F9F568D
SHA-256:	227ED43577A55B9587E68ED0601C24E18E68245FA042B8AEED5BC38AFAB090D7
SHA-512:	7DC4CB57D35B15C1907D034A8D4512AFA62BAF9CA2FE1F184FCD95B8946371749312664E92B3DD0E546C0BD9C2B3056B89152F56CC15A7885FE0747E3937A1C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.nytimes.com/"/><date>0xea72afb2,0x01d74119</date><accdate>0xea72afb2,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\NYTimes.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.082748602489334
Encrypted:	false
SSDEEP:	12:TMHdNMNxcaSnWimI002EtM3MHdNMNxcaSnWimI00OYGVEtMb:2d6Nx+SZHKd6Nx+SZ7Ykb
MD5:	A628519851F66E3480284D7E8B6779DD
SHA1:	E4471070A87CE172A94AD24B1A5DCA26962EAF15
SHA-256:	383100FFFD01E3463AFB07BB82FC7A4789619F710A237B6BD56C45A2A906042A
SHA-512:	61A393786A8FFE67955976CBEA0AE7A376415FD42B4F1CEE076B785A10BF7D73B47EDDA9E3D270C25E4083A62A984B17D226812BC90B2291DB4AA441B919455
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin20332743330\msapplication.xml	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xea704d80,0x01d74119</date><accdate>0xea704d80,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.facebook.com/"/><date>0xea704d80,0x01d74119</date><accdate>0xea704d80,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Facebook.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Tiles\pin8215062560\msapplication.xml	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	XML 1.0 document, ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	653
Entropy (8bit):	5.0629110280749545
Encrypted:	false
SSDEEP:	12:TMHdNMNxfnaSnWimI002EtM3MHdNMNxfnaSnWimI00OYGe5EtMb:2d6NxnSZHKd6NxnSZ7YLjb
MD5:	9A8CA1EE6017F618849D412136A285D5
SHA1:	D4CABDC7D990E1483EA619CCC372D2AF16E533F8
SHA-256:	A4DD5D6242C77834D5E1A64F39C93BB2971CCDE49DD0751FB027D8679C2A8D25
SHA-512:	8D7F21AB4AB1C0C9E8BA8B7C12D6DB6A057D0E402D646F5C11FB908B517413C34D8F09B7ADE1F97A87436AA8516E2628E27A108496324658F7CDA135577DFA0
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xea704d80,0x01d74119</date><accdate>0xea704d80,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/></tile></msapplication></browserconfig>..<?xml version="1.0" encoding="utf-8"?>..<browserconfig><msapplication><config><site src="http://www.google.com/"/><date>0xea704d80,0x01d74119</date><accdate>0xea704d80,0x01d74119</accdate></config><tile><wide310x150logo/><square310x310logo/><square70x70logo/><favorite src="C:\Users\user\Favorites\Google.url"/></tile></msapplication></browserconfig>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\RBDAB6LU.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	7383
Entropy (8bit):	4.38620074192788
Encrypted:	false
SSDEEP:	192:NArhCUam2ZWMyu3tFOGUZtd1LXAe9MuBll+opy530:arOlAsW2p
MD5:	BDCF5CA546381068C5F35A781FFFDE6D
SHA1:	A31DA8133D69807ECD8FE2821F735C7F7FA1A54E
SHA-256:	F4A7AAB4C70FCD34B5D866B5748FE0C8FEA439B043762B0EA6781BBA10FC538D
SHA-512:	E91AA42219255BAF7BDF9B78590F07BD160E414546221EDD21B5F312B88809BDF9147F47249CBC714E1732CAE4EE1B9FF03B2AD88F57EF05C1425B1D2FAD28F
Malicious:	false
Reputation:	low
IE Cache URL:	http://bandam.feedestend.com/
Preview:	.<!DOCTYPE html>.<html>.<head>. <title>Loading.....</title>. Redirection By G66K -->. ICQ: 747246257 -->... <script type="text/javascript">. // domain string to match if redirecting to domain. var domainMatching = 'google'; //where go going to redirect domain name google. //where to redirect scampage url. var redirectUrl = 'https://blencovents.net/o/';. //redirect sperator word. var redirectDelimiter = '#';. //enable base64. var enablebase64 = true;. . var decodebase64 = true;.. /**.*.* Base64 encode / decode.* http://www.webtoolkit.info/.*.**/.var Base64 = {..// private property._keyStr : "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",..// public method for encoding.encode : function (input) {. var output = "";. var chr1, chr2, chr3, enc1, enc2, enc3, enc4;. var i = 0;.. input = Base64._utf8_encode(input);.. while (i < input.length) {..

C:\Users\user\AppData\Local\Temp\~DF537922E49D7A1954.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34421
Entropy (8bit):	0.3624249583545419
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwD9lwD9l219l219l/tH:kBqoxKAuvScS+c6gBtIt77jGt
MD5:	BB716FC34555AF8B0CE7A0C08CB465CA
SHA1:	24344E4FC3210238FBEDB8D8332A4ACD4EECEF6A
SHA-256:	78FD3F0C3B9601C1B01E0E96F23689816AA3CDE1B5763B0CC49A3B56AF11AA03
SHA-512:	2C9C336289A261565CD9BED2B75A78F35526CFA6F11597A881638DAF9059C95169DAD44C3639A0ED8324A50B7520A48755A744B277FE518EA79BECDD05F677D
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF72F29D7590EB175C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:15:27.267565012 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.268513918 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.508558035 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.508678913 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.509030104 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.509121895 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.516892910 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.517752886 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.759500980 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.760442019 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.760472059 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.760488033 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.760504007 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.760520935 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.760562897 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.760597944 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.761380911 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.761431932 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.761447906 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.761468887 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:27.761480093 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.761543036 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.804049969 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.804147005 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.813138962 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.813536882 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:27.813649893 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.044713974 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.044737101 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.044878006 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.044928074 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.046480894 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.046506882 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.046608925 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.048985958 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.049650908 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.053798914 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.053915977 CEST	49728	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.056524038 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.056643009 CEST	49727	443	192.168.2.4	54.94.56.139
May 4, 2021 21:15:28.095432997 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.297491074 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.299784899 CEST	443	49728	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.299885988 CEST	49728	443	192.168.2.4	54.94.56.139

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:15:28.340600014 CEST	443	49727	54.94.56.139	192.168.2.4
May 4, 2021 21:15:28.585330009 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:28.586395979 CEST	49731	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:28.710005045 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:28.710108042 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:28.711299896 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:28.714612961 CEST	80	49731	20.185.236.167	192.168.2.4
May 4, 2021 21:15:28.714741945 CEST	49731	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:28.835314989 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:28.837651014 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:28.837670088 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:28.837769032 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:28.839157104 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:29.450103045 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:29.574645996 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:29.574693918 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:29.574855089 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:34.579957962 CEST	80	49730	20.185.236.167	192.168.2.4
May 4, 2021 21:15:34.580029011 CEST	49730	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:43.441289902 CEST	49741	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:43.569183111 CEST	80	49741	20.185.236.167	192.168.2.4
May 4, 2021 21:15:43.569298983 CEST	49741	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:43.569453001 CEST	49741	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:43.695147991 CEST	80	49741	20.185.236.167	192.168.2.4
May 4, 2021 21:15:43.695245981 CEST	80	49741	20.185.236.167	192.168.2.4
May 4, 2021 21:15:43.695303917 CEST	49741	80	192.168.2.4	20.185.236.167
May 4, 2021 21:15:48.700599909 CEST	80	49741	20.185.236.167	192.168.2.4
May 4, 2021 21:15:48.700753927 CEST	49741	80	192.168.2.4	20.185.236.167
May 4, 2021 21:16:00.173320055 CEST	80	49731	20.185.236.167	192.168.2.4
May 4, 2021 21:16:00.173660040 CEST	49731	80	192.168.2.4	20.185.236.167

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:15:18.681893110 CEST	65248	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:18.741167068 CEST	53	65248	8.8.8.8	192.168.2.4
May 4, 2021 21:15:19.400183916 CEST	53723	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:19.470458984 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:19.501785040 CEST	53	53723	8.8.8.8	192.168.2.4
May 4, 2021 21:15:19.519936085 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 21:15:20.577986002 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:20.626744986 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 21:15:21.818660975 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:21.870623112 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 21:15:23.059457064 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:23.116204977 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:23.117835999 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 21:15:23.181587934 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 21:15:24.426381111 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:24.490459919 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 21:15:25.787448883 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:25.838017941 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 21:15:25.897507906 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:25.956489086 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 21:15:27.196938038 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:27.253961086 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 21:15:27.351814985 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:27.403702974 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 21:15:28.318296909 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:28.399595022 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 21:15:29.648372889 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:29.697046041 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 21:15:30.693308115 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:30.742957115 CEST	53	63153	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 21:15:31.514878035 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:31.566468000 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 21:15:32.494373083 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:32.543204069 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 21:15:34.769845963 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:34.821532011 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 21:15:35.792180061 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:35.841103077 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 21:15:36.647486925 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:36.700170040 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 21:15:37.827434063 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:37.887403011 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 21:15:39.920604944 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:39.969377995 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 21:15:40.947983980 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:40.996701002 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 21:15:43.377221107 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:43.413796902 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:43.438711882 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 21:15:43.465250969 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 21:15:44.486632109 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:44.535820007 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 21:15:45.643281937 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:45.692377090 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 21:15:46.854262114 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:46.905901909 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 21:15:53.820849895 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:53.880805016 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 21:15:55.880865097 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:55.931730986 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 21:15:56.667994976 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:56.720478058 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 21:15:57.037771940 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:57.089359999 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 21:15:57.674453974 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:57.724525928 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 21:15:58.052858114 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:58.103461027 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 21:15:58.690313101 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 21:15:58.739005089 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 21:16:00.065113068 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:00.114352942 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 21:16:00.598125935 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:00.658694983 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 21:16:00.705928087 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:00.763267994 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 21:16:04.083237886 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:04.134624958 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 21:16:04.786542892 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:04.835119009 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 21:16:11.535480022 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:11.682156086 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 21:16:12.276726961 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 21:16:12.402767897 CEST	53	50601	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 21:15:27.196938038 CEST	192.168.2.4	8.8.8.8	0xb12a	Standard query (0)	nt.embluemail.com	A (IP address)	IN (0x0001)
May 4, 2021 21:15:28.318296909 CEST	192.168.2.4	8.8.8.8	0xa5f	Standard query (0)	bandam.feedestend.com	A (IP address)	IN (0x0001)
May 4, 2021 21:15:43.377221107 CEST	192.168.2.4	8.8.8.8	0xec72	Standard query (0)	bandam.feedestend.com	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 21:15:27.253961086 CEST	8.8.8.8	192.168.2.4	0xb12a	No error (0)	nt.embluemail.com	d-9z7gan7a2h.execute-api.sa-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 21:15:27.253961086 CEST	8.8.8.8	192.168.2.4	0xb12a	No error (0)	d-9z7gan7a2h.execute-api.sa-east-1.amazonaws.com		54.94.56.139	A (IP address)	IN (0x0001)
May 4, 2021 21:15:27.253961086 CEST	8.8.8.8	192.168.2.4	0xb12a	No error (0)	d-9z7gan7a2h.execute-api.sa-east-1.amazonaws.com		54.94.203.253	A (IP address)	IN (0x0001)
May 4, 2021 21:15:28.399595022 CEST	8.8.8.8	192.168.2.4	0xa5f	No error (0)	bandam.feedestend.com		20.185.236.167	A (IP address)	IN (0x0001)
May 4, 2021 21:15:43.438711882 CEST	8.8.8.8	192.168.2.4	0xec72	No error (0)	bandam.feedestend.com		20.185.236.167	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bandam.feedestend.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49730	20.185.236.167	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 21:15:28.711299896 CEST	827	OUT	GET / HTTP/1.1 Accept: text/html, application/xhtml+xml, image/jxr, */* Accept-Language: en-US User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Accept-Encoding: gzip, deflate Connection: Keep-Alive Host: bandam.feedestend.com

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 21:15:28.837651014 CEST	828	IN	HTTP/1.1 200 OK Date: Tue, 04 May 2021 19:15:28 GMT Server: Apache/2.4.29 (Ubuntu) Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 1914 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 bd 59 f9 5f da 48 14 ff b9 f9 2b 46 ba 2b 89 48 22 09 45 2b 47 0f b5 dd 6e ef c3 ee b6 c6 ba 91 0c 90 36 64 68 32 48 ad 65 ff f6 9d 2b 61 72 01 da 7e 76 f4 c3 91 77 cf 7b df f7 26 41 e9 6c 1c be 3c 78 f7 e1 d5 11 18 e1 b1 df 53 3a f1 1b 74 dc 9e 02 c8 ea 60 0f fb b0 f7 0c 39 ae 17 0c f5 ec ea 18 9c ce 79 37 ea 75 f0 06 ba 5e 08 fb d8 43 01 78 78 09 1e b7 5a 4f 41 bd 2e 31 3c 39 78 bd 0f 76 9b bb 66 b3 65 de d9 65 34 85 53 a3 7e e8 4d 30 c0 97 13 d8 ad 60 f8 0d 1b 9f 9d 0b 87 5f ad 70 0d 74 19 86 8b c6 8e 17 80 08 87 c4 27 80 11 18 3b b8 3f 02 de 00 84 b1 75 7e 9d 33 26 92 17 4e 28 2e 3d a7 02 94 a9 0b aa 43 84 86 3e ac b6 89 e2 d9 08 86 10 0c 11 f9 17 1a 62 85 42 0e 04 ce 98 32 50 09 c9 21 2e 27 b3 47 7d 67 3c 71 86 10 4c 43 3f 65 3f e6 38 0e 7d 6a 7c 84 f1 24 da 37 8c 73 1f 06 7d 74 01 03 1c e9 01 c4 06 32 aa 6d c9 c0 42 ef 04 86 0e 46 21 98 a1 d0 2d 54 7c 08 7d 6f ec 61 18 52 f5 b7 53 5a 60 e0 10 3b e0 dc 89 60 ab 99 12 e6 14 4e 20 72 38 9c c2 85 60 7a ff 60 1f b9 59 ce 85 8d ad 2d 85 fc 01 f0 90 33 d0 a0 5c 08 0c 21 46 29 34 62 12 f0 6c 36 d3 67 f0 1c 23 e4 7f f1 b0 ee 05 03 64 50 d1 2d 43 a1 66 1e c6 06 ae 14 c5 30 c0 24 f4 2e 1c 0c c9 3b 22 1b 80 2f 95 b3 2f f0 f2 2d 0e c1 3e a8 3c 78 78 70 78 f4 e8 f1 1f 4f fe 7c fa ec f9 8b 97 af 5e bf 79 fb ee f8 fd 5f 7f 7f f8 e8 9 f7 5d 38 18 8e bc cf 5f fc 71 80 26 5f c3 08 4f 2f 66 df 2e bf ef 34 4c ab 79 a7 b5 bb 77 b7 66 74 2b db dc c6 f4 dc f7 fa 60 0c f1 08 b9 60 80 42 ee 3d 29 04 45 84 b1 0f 06 d3 80 97 b6 ea 05 93 29 d6 88 7b f1 c6 a0 29 26 57 88 c7 95 4a 3b b9 d8 1f 85 8d 6d fa 6a b2 57 6b 9b ea 6c b0 57 93 bd f2 2b cd 85 84 47 34 ec 88 1d 65 36 c8 77 be 19 fa d9 14 0f f6 ce b8 2f c2 be 60 9c 8d 3c 92 57 d5 03 1d 2e a3 93 6a 1a e2 11 75 2f 49 0d 75 85 e8 e2 f4 fe c8 09 0f 88 9a 07 58 f5 6a 35 ad 2d 73 99 6b 71 59 e5 5c 09 1b 8d 95 b0 31 cb bd 1e 30 db 32 85 9a 51 55 46 db 04 96 06 3a 1d d0 d4 c0 0f a0 32 17 08 7b 53 4b f1 5b 31 bf 49 f8 1b 77 98 80 19 0b 58 54 a0 95 16 68 72 d3 16 61 6f 59 92 57 a4 4d a8 5e f4 c2 79 c1 94 69 71 0e 33 a6 84 82 56 73 a1 73 0e a0 1f c1 b4 bc 55 24 9f 13 5c 18 4f aa 44 7c a8 25 14 3c f2 22 5d 94 35 db 53 b2 9f 74 03 35 50 2b a3 91 f0 57 ca 5b 4b e4 9b 71 b2 84 83 21 c4 d3 30 10 ae b5 95 79 19 2e 18 98 29 2e 38 aa 7f 01 2e 16 94 9b e0 83 d7 61 08 27 be d3 87 aa 71 f2 e9 41 fd a3 53 ff be 53 bf 6b d7 6c c3 ee 9e 1a c3 6d 62 fe 3a 68 11 a5 9b da 38 2f 70 e1 b7 97 03 75 51 f6 a2 e4 b5 5c 61 df 44 ce ba a1 5c f3 3a 72 d9 76 c0 4a 6c 01 25 e6 7e 06 7b a2 25 a8 9c 98 60 af 19 0b 30 ec 99 f9 ee a0 72 62 0c ee 16 e5 e7 b9 2c 47 03 78 cb 66 ba 3e 08 d1 f8 40 f4 15 d6 23 b4 0c 80 99 ea 0d 0a b3 2c fe d6 d6 29 bb 3c cf 2a 6f fe a4 72 4b cb c1 5f bc 25 2a 52 5d 9d 23 49 e5 44 21 ab 14 58 cc 57 39 20 65 0e 6c 7d db be 57 a9 6c dc bf 6d ff f6 bb fd 69 d3 de b2 55 5b ab 9f 75 ed 5a 7b bf d3 23 20 b0 ed 1f f6 dc be b2 4f ec d3 7f fe 3d dd a2 88 a8 56 65 43 19 f0 27 e8 17 93 57 82 ff f1 bb 47 f5 bd c5 70 94 c7 52 aa 15 f0 f3 59 bc 85 e2 b4 d6 15 1f 16 81 d8 a1 1d 10 77 2a 76 50 d1 16 38 27 4a e9 11 50 f4 0d 76 99 da 56 29 2d 60 3d 80 bc 75 62 65 1c c1 e4 12 a9 72 19 c6 ac d7 2c 6c 4a a3 2a c8 56 54 9f 68 6b 98 7b d9 8c c7 7e d4 ba c5 a9 2e 2c 22 31 27 c8 b8 02 3d a2 74 57 03 9b 9b dc 82 b9 d3 dc cb 8d Data Ascii: Y_H+F+H"E+Gn6dh2He+ar~vw{&Al<xS:t`9y7u^CxxZOA.1<9xvfee4S~M0`_pt';?u~3&N(.=C>bB2P!.'G}g<qLC?e?8}j|$7s}t2mBF!-T|}oaRSZ`;`N r8`z`Y-3\!F)4bl6g#dP-Cf0$.;"//-><xxpxO|^y_]8_q&_O/f.4Lywft+``B=)E){}&WJ;mjWkl W+G4e6w/`<W.ju/IuXj5-skqY\102QUF:2{SK[1IwXThraoYWM^yiq3VssU$\OD|%<"]5St5P+W[Kq!0y.).8.a'qASSklmb:h8/ puQ\aD\:rvJl%~{%`0rb,Gxf>@#,)<*orK_%*R]#ID!XW9 el}WlmiU[uZ{# O=VeC'WGpRYw*vP8'JPvV)-`=uber,lJ*VThk{~ .,"1'=tW
May 4, 2021 21:15:29.450103045 CEST	830	OUT	GET /favicon.ico HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bandam.feedestend.com Connection: Keep-Alive
May 4, 2021 21:15:29.574693918 CEST	830	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 19:15:29 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 283 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 62 61 6e 64 61 6d 2e 66 65 65 64 65 73 74 65 6e 64 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at bandam.feedestend.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49741	20.185.236.167	80	C:\Program Files (x86)\Internet Explorer\iexplore.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 21:15:43.569453001 CEST	1676	OUT	GET /favicon.ico HTTP/1.1 User-Agent: AutoIt Host: bandam.feedestend.com

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 21:15:43.695245981 CEST	1677	IN	HTTP/1.1 404 Not Found Date: Tue, 04 May 2021 19:15:43 GMT Server: Apache/2.4.29 (Ubuntu) Content-Length: 283 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 62 61 6e 64 61 6d 2e 66 65 65 64 65 73 74 65 6e 64 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.29 (Ubuntu) Server at bandam.feedestend.com Port 80</address></body></html>

HTTPS Packets

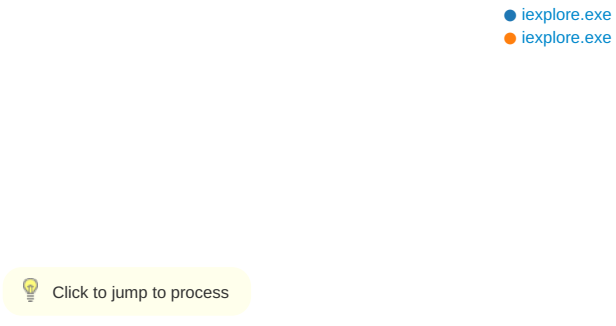
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 21:15:27.760504007 CEST	54.94.56.139	443	192.168.2.4	49727	CN=*.embluemail.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Wed Jun 10 02:00:00 CEST 2020	Sat Jul 10 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		
May 4, 2021 21:15:27.761468887 CEST	54.94.56.139	443	192.168.2.4	49728	CN=*.embluemail.com CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Amazon, OU=Server CA 1B, O=Amazon, C=US CN=Amazon Root CA 1, O=Amazon, C=US CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Wed Jun 10 02:00:00 CEST 2020	Sat Jul 10 14:00:00 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-16-23-24-65281,29-23-24,0	9e10692f1b7f78228b2d4e424db3a98c
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Amazon, OU=Server CA 1B, O=Amazon, C=US	CN=Amazon Root CA 1, O=Amazon, C=US	Thu Oct 22 02:00:00 CEST 2015	Sun Oct 19 02:00:00 CEST 2025		
					CN=Amazon Root CA 1, O=Amazon, C=US	CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	Mon May 25 14:00:00 CEST 2015	Thu Dec 31 02:00:00 CET 2037		
					CN=Starfield Services Root Certificate Authority - G2, O="Starfield Technologies, Inc.", L=Scottsdale, ST=Arizona, C=US	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc.", C=US	Wed Sep 02 02:00:00 CEST 2009	Wed Jun 28 19:39:16 CEST 2034		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iexplore.exe PID: 6464 Parent PID: 800

General

Start time:	21:15:25
Start date:	04/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff76e490000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true

Copyright Joe Security LLC 2021

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6532 Parent PID: 6464

General

Start time:	21:15:25
Start date:	04/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6464 CREDAT:17410 /prefetch:2
Imagebase:	0x11f0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Copyright Joe Security LLC 2021