河南省教育信息安全监测中心
关于 “银狐”黑客组织钓鱼攻击
的预警通报

河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2024 年 4 月 3 日

关于“银狐”黑客组织钓鱼攻击的预警通报

事件描述

近期工作发现，多家重要单位遭“银狐”黑客组织钓鱼攻击。

一是长期持续活跃，主要针对各领域财务人员。该黑客组织自2023 年 4 月以来持续活动，主要针对重要行业单位的财务人员实施钓鱼攻击，以窃取相关数据和实现远程控制为目的。

二是抢占搜索引擎，诱导用户安装仿冒软件。通过搭建仿冒常用软件下载页面，并购买大量搜索引擎关键词（广告位）的方式，使其在搜索引擎的结果显示中排名靠前，诱导受害者下载安装仿冒的软件安装包。

三是利用即时通讯，发送夹带恶意程序的信息。通过微信等即时通讯工具发送夹带恶意下载器木马的钓鱼信息，并使用“2023 年企业重点人群税收补贴政策”等带有诱惑性的标题，诱使受害者点击。

四是自动识别判断，逃避沙箱等常规安全检测。远控木马组件具备检测虚拟机以及主流杀毒软件的功能，如发现是虚拟机环境或360、火绒等杀毒软件，则不进行后续恶意操作。

安全建议

为确保重要网络系统安全，请各单位增强网络安全防护意识，在确保安全的前提下督促指导本部门将相关 IOC 添加至安全设备黑名单中，强化网络安全防护，同时密切关注自身系统、设备外联恶意域名和 IP 的情况，及时消除安全风险。如发现遭攻击情况及时处置并报告。

“银狐”黑客组织 IOC 资产列表

序号	IP 地址
1	143.92.57.121
2	38.55.204.70
3	38.55.184.74
4	164.155.255.240
5	164.88.140.82
6	202.79.169.51
7	134.122.184.51
8	116.213.43.187
9	8.217.254.61
10	164.88.107.68
11	164.155.255.222
12	137.220.135.169
13	134.122.184.48
14	206.238.198.120
15	143.92.57.10
16	122.10.26.102
17	47.57.6.49
18	216.83.53.8
19	198.44.248.9
20	154.91.65.177
21	118.107.47.66
22	27.124.46.211
23	45.200.51.127
24	223.26.52.70
25	154.39.239.56
26	118.107.47.24
27	164.88.184.76
28	216.83.53.161
29	206.238.115.59

30	38.55.185.76
31	27.50.63.22
32	216.83.58.135
33	216.83.48.165
34	27.124.20.167
35	27.124.20.141
36	27.124.4.232
37	143.92.61.27
38	118.107.47.93
39	223.26.52.2
40	202.79.172.93
41	27.124.47.12
42	27.124.45.15
43	154.39.250.33
44	154.211.20.240
45	8.217.213.141
46	143.92.36.133
47	27.124.20.143
48	202.79.174.69
49	47.75.103.13
50	165.3.86.252
51	96.43.110.54
52	164.155.252.72
53	143.92.53.162
54	118.107.47.84
55	27.124.46.70
56	122.10.27.109
57	27.124.6.69
58	27.124.2.130
59	112.213.101.146
60	38.55.185.93
61	38.55.204.77
62	27.50.59.159
63	27.124.20.163
64	216.83.58.167
65	118.107.47.88
66	27.124.18.185
67	122.10.26.86
68	38.55.184.67
69	202.79.172.238
70	27.50.59.150
71	27.124.20.176
72	143.92.60.11
73	216.83.58.177

74	103.148.125.109
75	202.79.173.58
76	134.122.184.19
77	122.10.110.157
78	202.79.172.235
79	202.79.173.167
80	116.213.43.89
81	143.92.58.143
82	202.79.172.241
83	154.91.229.196
84	134.122.184.37
85	134.122.184.25
86	47.76.169.139
87	137.220.135.176
88	112.213.116.146
89	202.79.172.65
90	134.122.184.58
91	164.155.255.106
92	123.254.107.244
93	103.214.140.174
94	216.83.53.177
95	164.88.107.196
96	38.55.185.88
97	143.92.49.138
98	154.82.93.100
99	154.91.229.174
100	101.33.34.106
101	45.195.52.169
102	38.165.9.247
103	154.19.160.92
104	118.107.42.180
105	202.79.172.222
106	154.82.93.99
107	134.122.184.41
108	118.107.47.5
109	47.104.145.97
110	38.55.185.94
111	27.124.46.41
112	202.79.172.99
113	202.79.172.230
114	164.155.255.48
115	118.107.47.23
116	38.165.14.239
117	27.124.6.64

118	143.92.58.180
119	164.88.140.69
120	8.217.101.29
121	137.220.135.213
122	134.122.184.3
123	120.27.10.22
124	143.92.32.153
125	216.83.58.181
126	118.107.42.131
127	38.55.196.221
128	27.124.40.157
129	223.26.52.78
130	27.124.46.76
131	137.220.135.22
132	134.122.133.18
133	112.213.101.110
134	202.79.172.134
135	8.218.106.149
136	38.55.205.228
137	118.107.47.87
138	202.79.169.165
139	163.197.241.154
140	143.92.35.21
141	112.213.116.133
142	38.55.184.88
143	38.165.14.231
144	163.197.240.144
145	202.79.172.87
146	134.122.184.55
147	122.10.27.116
148	47.104.133.7
149	38.165.12.242
150	202.79.175.103
151	38.55.184.92
152	143.92.48.23
153	47.104.140.16
154	202.79.172.110
155	134.122.134.14
156	216.83.53.133
157	38.55.184.90
158	38.55.184.243
159	163.197.241.149
160	154.91.65.118
161	202.79.172.107

162	122.10.26.245
163	156.254.126.18
164	156.251.17.145
165	143.92.35.72
166	206.238.198.118
167	45.195.53.201
168	223.26.52.96
169	165.3.120.78
170	116.213.43.250
171	27.124.46.157
172	202.79.173.149
173	202.79.169.52
174	118.107.47.59
175	47.242.238.212
176	38.165.9.237
177	47.76.50.128

序号	域名
1	shimo-oss1.oss-cn-hangzhou.aliyuncs.com
2	muchengoss.oss-cn-hongkong.aliyuncs.com
3	bucketossbj.oss-cn-hongkong.aliyuncs.com
4	baiduwenshen.oss-cn-hongkong.aliyuncs.com
5	osstesto.oss-cn-hongkong.aliyuncs.com
6	jubaopengosssi.oss-cn-hongkong.aliyuncs.com
7	shunfengoss.oss-cn-hongkong.aliyuncs.com
8	kefubahaohonsheng.oss-cn-
9	aliyunlianjieoss.oss-cn-hongkong.aliyuncs.com
10	jpbdoss.oss-cn-hongkong.aliyuncs.com
11	wangzheguilaioss.oss-cn-hongkong.aliyuncs.com
12	mustdll.oss-cn-hongkong.aliyuncs.com
13	supervt.oss-cn-hongkong.aliyuncs.com
14	whitefile.oss-cn-hongkong.aliyuncs.com
15	bucketyun11.oss-cn-hongkong.aliyuncs.com
16	condongjkhdsgdsd.oss-cn-hongkong.aliyuncs.com
17	423down.oss-cn-hongkong.aliyuncs.com
18	alibwj.oss-cn-hongkong.aliyuncs.com
19	alidll.oss-cn-hongkong.aliyuncs.com
20	alivt.oss-cn-hongkong.aliyuncs.com
21	ossbaiwenj.oss-cn-hongkong.aliyuncs.com
22	51yunpio.oss-cn-hongkong.aliyuncs.com
23	titi2-4.oss-cn-hangzhou.aliyuncs.com
24	variety.oss-cn-hongkong.aliyuncs.com
25	jubaopengosser.oss-cn-hongkong.aliyuncs.com

26	winios2024.oss-cn-hongkong.aliyuncs.com
27	11bucketyun.oss-cn-hongkong.aliyuncs.com
28	aexe.oss-cn-hongkong.aliyuncs.com
29	adll.oss-cn-hongkong.aliyuncs.com

序号	样本 MD5
1	2f9af47e72a6df4b45a9143b2f1ff421
2	a5b798db6a2f6e527870a7be40a4c5c6
3	df1ca4a8fab0457219e8b1f1952c4b84
4	a753cdc5f05b18f00577711e8341a76b
5	719ab2c961b9432cc5e1e16a7c503ae8
6	cd9a14ebbc0fc56d5b61f2cbeff18681
7	0edffab2af94b6261e129655f32c2f1a
8	91406db84c365a57ce3570ff80825cd4
9	150994da0e2f8cf5660460cbd5a65934
10	82ce263644fc8a59947e4d0321b00737
11	84a4535d7489b4cb6599dc8325d09d63
12	e2c9ae30f7bf613bb4b7359d6cb8b9f3
13	e592e41e879f5c7913a42a8119cf5f69
14	527cbe7eedb577b3210b3d7309de6d94
15	dfcdf1dbc37b35b8d3a40fcf176584f4
16	9dc226661fd60b13f459c8031f2fa668
17	8cc36c6441e6904f51e4a72878aa8f0f
18	6eb6b7ed66726acf908fcb60299f9e0b
19	1fc0594c118559d49aa48dd395a0a307
20	316ea891f71b5905767cb33c0d065d3e
21	374c819df0a846b1688c27a2e8455823
22	99ab3ede5678fe375117f1bdb985e1ef
23	94735f853e157df74eef3b6eb12606d8
24	b9c83524d916ca60361edc365931217b
25	0324f25190a9cb5e0aa28ad2be1d5501
26	59f282154cb69b296d680ad95d034c87
27	17ef8c8884cce07cf131c193a854374d
28	101138ccd72fbc63c1fef9cfc069928a
29	3ddd4a421e41ec9a4311022bca1b581a
30	e47c47ebe2d1abd27103e1110282caf0
31	5c85b5c8db5e82091e16112c9b9aa8ba
32	6cb5bf5a43b362738a3e799f0aa6c90a
33	281fefbe8ae2e580912a7749241461f2
34	7904842a7131e62a00aa8fbd28580f04
35	669a3a262d907dbe4b863feed1839c20
36	7db1525a94e6d0b52d120c3d188f0ed3
37	34d5a8f6abece85b4d02f624b5321a82

38	5103f764a1906a51b7da891e3f3f8dde
39	891a50ed2c8fc0b55b9573b78c4fe5e2
40	06c75271c589eb60c9b6e34735bfcb13
41	d003c49e410031903c397686aab42b5a
42	6b14ea0f793dbc1cce679ff10b2f9142
43	d2ba7f6a8aa4ebb3c97b7b62cb0e0aec
44	9992490e445f8da56acc64390239f960
45	6b2214a97788eff35ddefa82357f03cf
46	fd77506dd5c1338147c9edfaef9008b7
47	d9cc672ee25db65518c3b6715ae5076f
48	50faaa9eeb829d1274455f64a660af0d
49	1818827a4c4305986969bf19dab209c0
50	bc2ce775eebbcc93a3f7a9ee42928a3f
51	f0812851834e4e57cc0f7c5df360ec12
52	99f91006d933909d8257000e57729394
53	d4d8cc6c5cc8aec7390be7d2e22fcc06
54	e1e8998a9ca8b1c04808d7875a14c929
55	1319172e950f4a1d641bf41644a057d2
56	eb9570a321a4c53992e5b30cac863343
57	fbf9cee6136a056657f73be611ccb109
58	d15283ee7bd207f07dd5faad8cacea51
59	1095eb9b03cebc35699a6cb0d82db8f0
60	6a5fda1d553a919026be3f43f98a8ecb
61	0d4ac921804f3e7eed2d970008d0c5cb
62	790878ed2424e49f8e20e646e9709e8b
63	533b435b434982d1b5349f6d17daa794
64	46a2b9c49823636cdded2f9db719d5cf
65	af687412cddb0179662fecfb32b5bebd
66	519de6c974cc4f0aaf57caa32a2f41a1
67	a98d8f2f28700feea6b28d7bd71654e3
68	ad41754880670350a086b72040e833bc
69	9129713eb0d2e6b93a75014554a7cbb0
70	e34a553eafea8168723594970190ab65
71	ac3cb4ce313b71dd87f846c8a30ec416
72	e8a1af49433eb13b55ecd446b9a0e5b8
73	527050f0e7add6521248c8921fcc4743
74	f65f6d65395afca0859c444b0ec2bf27
75	de61d5b79056d46b24a9e46a49ada1f8
76	7d09c5ed072a9b884333c7419d7a30c6
77	73580530560707d23ff9fbd7d4acf455
78	c983aae1e85da46ece52438d9ec5e949
79	948eb6df6f86f441697c1fa4f4fef9d7
80	f2b4d0bff2f3ffecebea0457781625e6
81	e01d5dbfc37f8b114d8788724fe77677

82	3b40042a52899db2ddbb6388fec51f51
83	5125869e7a3e642dff5ce535c2a18a8f
84	c953cf1e06b00870ead2a6b06cfa0b02
85	93d6d71bc62fd34c8e7854ff1a19e5a0
86	03d75cd4addb34069ea66a3e451f403b
87	ba3d706bb5b99e425a89b9a8806ad87a
88	4383eaaf2592752f52d3b643172f6e49
89	02dc758a661f23ac2a7f5bcf5d4bac20
90	dbc79ae86ad01f26d1ac60114f9aaf38
91	885eb03b8e3945e63aaddb9a4e31318f
92	ead51163c12bb27c17521d92769cce5e
93	fc4aa28be11cd51c18ef9039fbfc4ec4
94	1e035961b42c6620f824744a4f7e0da6
95	8b6c646f5788dcce3db6598fcaca8ff5

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052