河南省教育信息安全监测中心

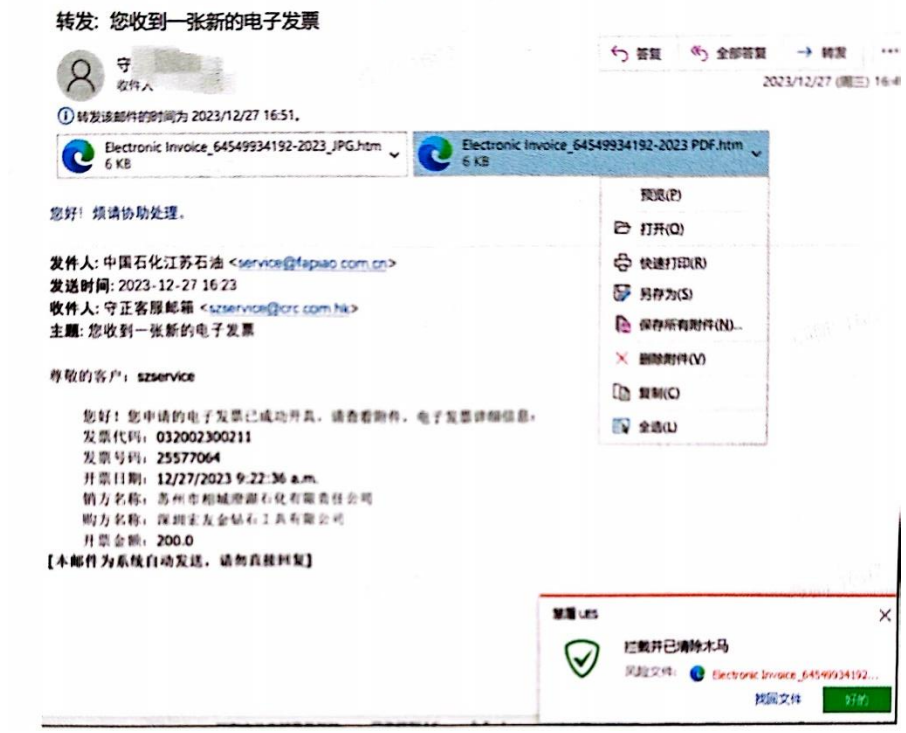
关于防范钓鱼邮件攻击的预警通报

2024 年 2 月 26 日

关于防范钓鱼邮件攻击的预警通报

事件描述

近期监测到黑客组织频繁对我国重要行业部门发起广撒网式钓鱼邮件攻击，邮件主题以电子发票为主，通过诱导点击查看发票信息窃取受害者邮箱账号密码。



相关钓鱼邮件截图

攻击特点

经初步分析，该黑客组织使用的域名和 IP 存在如下特点:

一是域名服务器指向 ns1.webserversystems.com、ns2.webserversystems.com;

二是频繁使用 143.95.XX.XX 网段 IP 地址，以 143.95.224.166 为主。

安全建议

请各单位重点做好以下工作：

一是及时通报预警相关情况，提高网络安全防范意识，避免点击不明邮件、未知链接等，谨慎下载运行可疑程序。

二是及时封禁相关恶意域名、IP，安装杀毒软件，更新病毒库，并开启实时监控功能。

三是加强安全监测，发生重大网络安全事件及时处置并报告。

相关恶意域名

序号	相关恶意域名
1	*.hkwordpress.com
2	28.hkwordpress.com
3	77.hkwordpress.com
4	a0887033.xsph.ru
5	a0895829.xsph.ru
6	antonada.ru.com
7	awodpressxs.za.com
8	bcdtravel.com.py
9	believeservices.life
10	bmxu9.ru.com
11	bv6.sa.com
12	cetorax.com
13	checobeauty.com
14	chlnafloc.com
15	comiccon.rs
16	cornicabra.za.com
17	ddfk.mypi.co
18	dev-bluf009.pantheonsite.io
19	dev-felix09.pantheonsite.i0
20	deviscaperealtors.in
21	dev-ulie009.pantheonsite.i0
22	djtty.mypi.co

23	drupal.d4mmedia.com
24	eaudl.ru.com
25	ehwr0.ru.com
26	esada.sa.com
27	f16.hkwordpress.com
28	f40.hkwordpress.com
29	f43.hkwordpress.com
30	f44.hkwordpress.com
31	f49.hkwordpress.com
32	faithchainhk.com
33	freddiesnack.cz
34	heaea.mypi.co
35	http://28.hkwordpress.com/dfr/lognet2023.php
36	http://28.hkwordpress.com/f56/Tsend.php
37	http://28.hkwordpress.com/fad/Tsend.php
38	http://28.hkwordpress.com/zp9/lognet2023.php
39	http://77.hkwordpress.com/wp-admin/domain/lognet2023.php
40	http://checobeauty.com/rteqwteq/lognet2023.php
41	http://esada.sa.com/fonts/lognet.php
42	http://f16.hkwordpress.com/wp-includes/js/2Aond.php
43	http://f16.hkwordpress.com/wp-includes/js/code/lognet2023.php
44	http://f16.hkwordpress.com/wp-includes/js/DDH/GlobalSources
45	http://f16.hkwordpress.com/wp-includes/js/DDH/GlobalSources
46	http://f16.hkwordpress.com/wp-includes/js/jcrop/loh/lognet2023.php
47	http://f16.hkwordpress.com/wp-includes/js/jcrop/vem/Line.php
48	http://f40.hkwordpress.com/wp-admin/404/lognet2023.php
49	http://f40.hkwordpress.com/wp-admin/compere/lognet2023.php
50	http://f40.hkwordpress.com/wp-admin/lognet2023.php
51	http://f43.hkwordpress.com/euro/pdfnglw.php
52	http://f43.hkwordpress.com/pdfpdfnglw.php
53	http://f44.hkwordpress.com/wp-includes/r/c/n.php
54	http://f44.hkwordpress.com/wp-includes/r/rr.php
55	http://f49.hkwordpress.com/wp-admin/js/Out/'yark.php
56	http://f49.hkwordpress.com/wp-admin/js/quotation/Tsend
57	http://mmhkcrm.com/ognet.php
58	http://socialwork.hkwordpress.com/wp-includes/somkey/lognet2023.php
59	https://bmxu9.ru.com/pol/lognet.php
60	https://bmxu9.ru.com/ww/lognet.php
61	https://bv6.sa.com/sflognet2023.php
62	https://cetorax.com/ttoo/lognet.php
63	https://comiccon.rs/lognet.php
64	https://cornicabra.za.com/zuzs/lognet.php

65	https://ddfk.mypi.co/vv/lognet.php
66	https://ddfk.mypi.co/xxx/lognet.php
67	https://dev-felix09.pantheonsite.io/ye/lognet.php
68	https://deviscaperealtors.in/YE/lognet.php
69	https://dev-ulie009.pantheonsite.io/8888/ognet.php
70	https://drupal.d4mmedia.com/lognet.php
71	https://ehwr0.ru.com/ww/lognet.php
72	https://esada.sa.com/pannello2/mobile/export/ognet2023 (7).php
73	https://interesartemedia.com/wp-includes/lognet.php
74	https://jianlonggroups,com/mail/ngo/lognet.php
75	https://jianlonggroups.com/mail/xx/first.php
76	https:/jianlonggroups,com/mail/xx/orz/lognet.php
77	https://jianlonggroups.com/mail/xx/sf/lognet.php
78	https://kancelariaprestige.com.pl/wp-content/dwmin/de/lognet.php
79	https://kancelariaprestige.com.p/wp-content/ttz/ozt/defi/lognet.php
80	https://macollperu.com/XD/ognet.php
81	https://mollidura.sa.com/aal/lognet2023.php
82	https://mtc.edu.np/sample/lognet.php
83	htps:/new.nextdaypharmacy.co.uk'vendor/phpunitphpunivsrc' til/p p/sflognet. php
84	https://qehc4.za.com//wap-log/lognet.php
85	https://steam-professionals.com/lognet.php
86	https:/sunkissedembroidery.com/kkkk/lognet.php
87	https://worldtouristsdestination.com/lognet.php
88	https://yaj0.sa.com/aa/lognet.php
89	https://yaj0.sa.com/abc/hello (1).php
90	https://yepf4.sa.com/wp-source/lognet2023.php
91	https://yiky9.sa.com/lognet2023.php
92	https://yo4.sa.com/bnb/lognet2023.php
93	ikwd.mypi.co
94	interesartemedia.com
95	jianlonggroups.com
96	jttdj.mypi.co
97	kancelariaprestige.com.pl
98	lqyiiyu.com
99	macollperu.com
100	marearia.ru.com
101	meritegypttours.com
102	micp4.za.com
103	mmhkcrm.com
104	mollidura.sa.com
105	motoexim.com
106	mtc.edu.np

107	new.nextdaypharmacy.co,uk
108	nwoj8.za.com
109	obtaining-criticality.us.to
110	putzfeen.tk
111	qehc4.za.com
112	rumah-hijab.com
113	socialwork.hkwordpress.com
114	steam-professionals.com
115	studio-saitrix.ru
116	sunkissedembroidery.com
117	sunugalnews.com
118	tpstagelight.com
119	worldtouristsdestination.com
120	wwwfreehostingtrustcom.xxxy.info
121	wwwl2selectricalcomau.freewww.info
122	wwwwkojimammm.freewww.info
123	yaj0.sa.com
124	yepf4.sa.com
125	ygnj9.sa.com
126	yiky9.sa.com
127	yo4.sa.com

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西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052