FBI FLASH

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

29 May 2025

FLASH Number

20250529-001

WE NEED YOUR HELP! If you identify any suspicious activity within your enterprise or have related information, please contact your local FBI Cyber Squad immediately with respect to the procedures outlined in the Reporting Notice section of this message.

**Note: By reporting any related information to FBI Cyber Squads, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

Infrastructure Used to Manage Domains Related to Cryptocurrency Investment Fraud Scams between October 2023 and April 2025

Summary

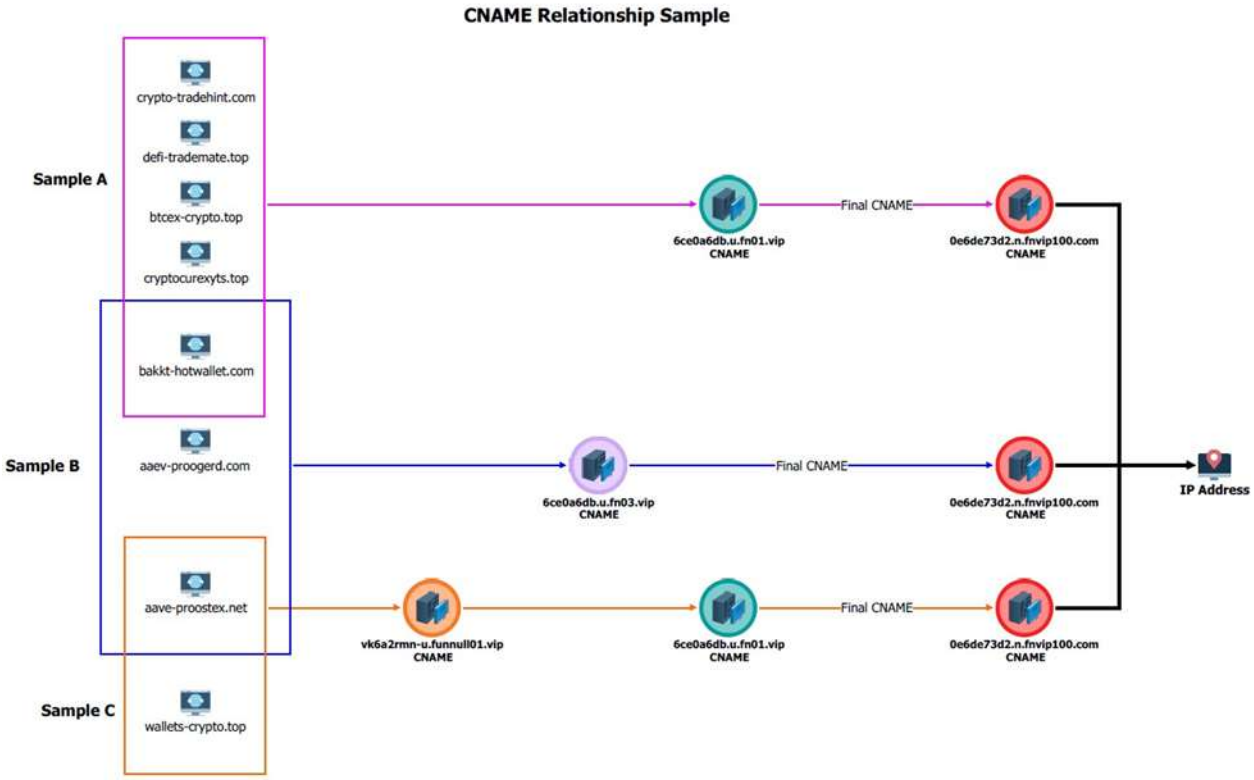
The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) associated with malicious cyber activities linked to Funnull Technology Inc. (Funnull). Funnull is a Philippines-based company which provides computer infrastructure for thousands of websites associated with cryptocurrency investment fraud (CIF) scams, commonly referred to as "pig butchering," and other illicit activities. During CIF scams, perpetrators pose as potential romantic partners or friends to gain victims' trust, who are then convinced to invest in virtual currency. The perpetrators direct their victims to deposit money into what appear to be legitimate investment platforms, such as websites or applications. Ultimately, money sent to these platforms is not invested, and instead goes directly to the scammers. Funnull facilitates these scams by purchasing IP addresses and providing hosting services and other internet infrastructure to groups performing these frauds. Funnull acquires these facilities from legitimate providers in the United States and sells them to cyber criminals. This

information is being provided for general awareness, and the indicators in this report provide actionable information that may be used by recipients.

Technical Details

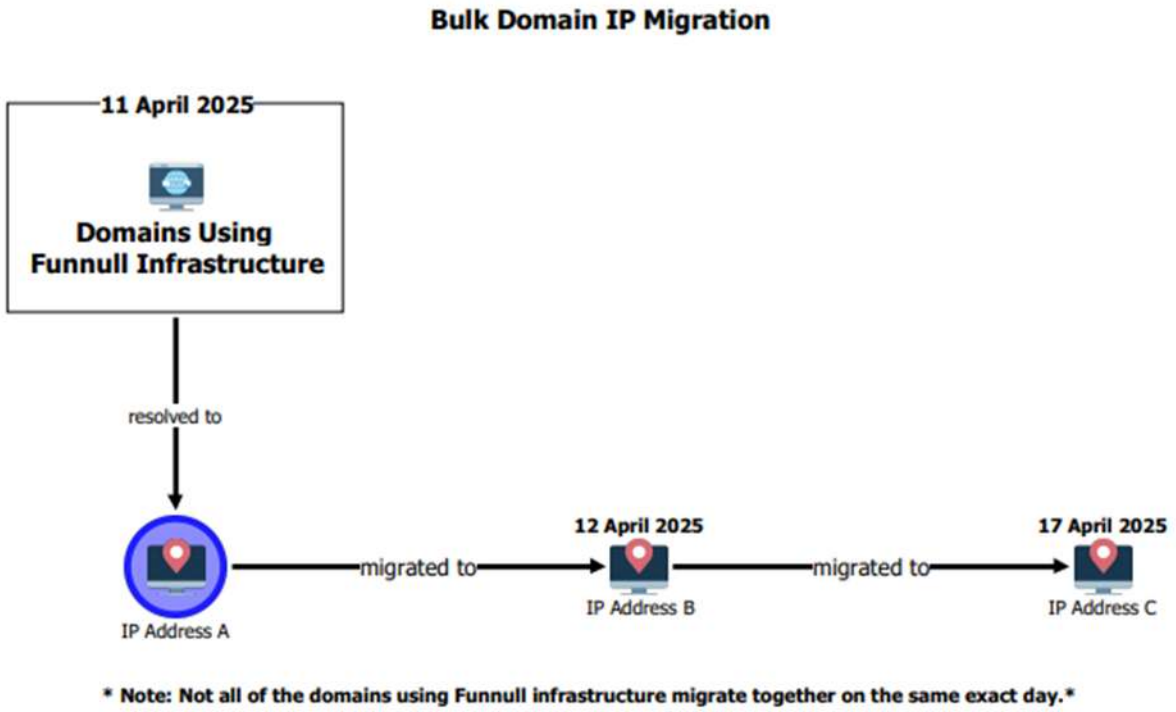
Execution:

Since January 2025, the FBI has identified 548 unique Funnull Canonical Names (CNAME) linked to over 332,000 unique domains. In April 2025, a sample of eight domains were analyzed to depict a CNAME analysis that resolved to four CNAMEs tied to Funnull infrastructure. Between February 2023 and April 2025, the eight domains showed three different patterns of CNAME activity.



Execution

Between October 2023 and April 2025, multiple patterns of IP address activity were observed from several domains using Funnull infrastructure. During this time frame, hundreds of domains using Funnull infrastructure simultaneously migrated from one IP address to another either on the same exact day or within the same timeframe.



Indicators

Execution: Funnull CNAMEs Associated with Domain Creation

CNAME	Root Domain
28bp.com.funnullcdn.com.	funnullcdn.com
wanqu_dev.funnullcdn.com.	funnullcdn.com
q9thn6pf-u.funnull01.vip.	funnull01.vip
lgzb18.com.funnullcdn.com.	funnullcdn.com
h5z9mtd8-u.funnull01.vip.	funnull01.vip.
wkg3b847-u.funnullv26.com.	funnullv26.com
b3b73d16.u.fn01.vip.	fn01.vip
funnull.com.funnullcdn.com.	funnullcdn.com
wanqu.funnullcdn.com.	funnullcdn.com
ace.bet.funnullcdn.com.	funnullcdn.com
vxjd26c7.funnullv23.com.	funnullv23.com
fun-pays.funnullcdn.com.	funnullcdn.com
6xugf2zr-u.funnull.vip.	funnull.vip

6xugf2zr-u.funnull01.vip.	funnull01.vip
ujpm29he-u.funnull01.vip.	funnull01.vip
28af5194.u.fn01.vip.	fn01.vip
301.funnull301.com.	funnull301.com
03f4debf.u.fn03.vip.	fn03.vip
2d567eaa.u.fn01.vip.	fn01.vip
a05e098a.u.fn01.vip.	fn01.vip
48qpsfm5-u.funnull01.vip.	funnull01.vip
703cfe31.u.fn03.vip.	fn03.vip
28af5194.u.fn03.vip.	fn03.vip
f7633b76.u.fn03.vip.	fn03.vip
d7368772.u.fn03.vip.	fn03.vip
8b72bbdb.u.fn03.vip.	fn03.vip
da738f71.u.fn02.vip.	fn02.vip
xd3b8uwm-u.funnull01.vip.	funnull01.vip
da738f71.u.fn01.vip.	fn01.vip
63f4b53f.u.fn03.vip.	fn03.vip
e470191c.u.fn01.vip.	fn01.vip
fcb58d89.u.fn01.vip.	fn01.vip
1ca6da29.u.fn03.vip.	fn03.vip
05a7bb35.u.fn03.vip.	fn03.vip
6xjztv47-u.funnullv23.com.	funnullv23.com
4nmj7xud-u.funnull01.vip.	funnull01.vip
06988305.u.fn03.vip.	fn03.vip
63246c94.u.fn03.vip.	fn03.vip
60e8f811.u.fn03.vip.	fn03.vip
93100b8e.u.fn03.vip.	fn03.vip
be369433.u.fn03.vip.	fn03.vip
6963c6dc.u.fn03.vip.	fn03.vip
684d4de3.u.fn03.vip.	fn03.vip
a71b1597.u.fn03.vip.	fn03.vip
5a62a3f8.u.fn03.vip.	fn03.vip
0f6ac9b1.u.fn01.vip.	fn01.vip
btxn2wya-u.funnull.vip.	funnull.vip
6443afcd.u.fn01.vip.	fn01.vip
ac2fdd8b.u.fn03.vip.	fn03.vip
1ca5435a.u.fn03.vip.	fn03.vip
766abf91.u.fn03.vip.	fn03.vip
bcd4e3ae.u.fn03.vip.	fn03.vip
b1153d06.u.fn03.vip.	fn03.vip
8cb5f909.u.fn03.vip.	fn03.vip
36c79537.u.fn03.vip.	fn03.vip
b0251cdd.u.fn03.vip.	fn03.vip

7cba2b41.u.fn01.vip.	fn01.vip
3ad011c9.u.fn03.vip.	fn03.vip
2aa08077.u.fn03.vip.	fn03.vip
8ack7xhf-u.funnull01.vip.	funnull01.vip
df5ac03e.u.fn03.vip.	fn03.vip
1a33208d.u.fn03.vip.	fn03.vip
1503e372.u.fn01.vip.	fn01.vip
17f77fb7.u.fn01.vip.	fn01.vip
9fd86a85.u.fn01.vip.	fn01.vip
bnf623g4-u.funnull01.vip.	funnull01.vip
9e5164d4.u.fn03.vip.	fn03.vip
bd399ac7.u.fn03.vip.	fn03.vip
a5bfe8e1.u.fn03.vip.	fn03.vip
7f039784.u.fn03.vip.	fn03.vip
bcf3b583.u.fn03.vip.	fn03.vip
6607b783.u.fn03.vip.	fn03.vip
98175973.u.fn03.vip.	fn03.vip
05a7bb35.u.fn01.vip.	fn01.vip
01b3b532.u.fn03.vip.	fn03.vip
224bb021.u.fn01.vip.	fn01.vip
224bb021.u.fn03.vip.	fn03.vip
29913296.u.fn03.vip.	fn03.vip
34b45099.u.fn03.vip.	fn03.vip
734a6e03.u.fn03.vip.	fn03.vip
4f9455d8.u.fn03.vip.	fn03.vip
fjtdqrb8-u.funnull01.vip.	funnull01.vip
5a785613.u.fn01.vip.	fn01.vip
5e5c8e60.u.fn03.vip.	fn03.vip
72f84162.u.fn01.vip.	fn01.vip
0d39c398.u.fn01.vip.	fn01.vip
cadd8fa8.u.fn01.vip.	fn01.vip
pqkvu8d6-u.funnull02.vip.	funnull02.vip
5a785613.u.fn02.vip.	fn02.vip
0659dffa.u.fn03.vip.	fn03.vip
1ca6da29.u.fn01.vip.	fn01.vip
cc7ba16b.u.fn01.vip.	fn01.vip
72f84162.u.fn02.vip.	fn02.vip
4nwzc2xs-u.funnull01.vip.	funnull01.vip
5a785613.u.fn03.vip.	fn03.vip
7cba2b41.u.fn02.vip.	fn02.vip
22dab045.u.fn03.vip.	fn03.vip
e897982d.u.fn03.vip.	fn03.vip
74a255dc.u.fn01.vip.	fn01.vip

8433da0e.u.fn03.vip.	fn03.vip
4462ae92.u.fn03.vip.	fn03.vip
a6352ca5.u.fn01.vip.	fn01.vip
95tzepfh-u.funnull01.vip.	funnull01.vip
f5656f14.u.fn02.vip.	fn02.vip
f5656f14.u.fn03.vip.	fn03.vip
3922e262.u.fn03.vip.	fn03.vip
d4ca4cce.u.fn03.vip.	fn03.vip
cadd8fa8.u.fn03.vip.	fn03.vip
376b70b6.u.fn01.vip.	fn01.vip
72f84162.u.fn03.vip.	fn03.vip
2dd7d0ec.u.fn01.vip.	fn01.vip
n2z3u5kc-u.funnull01.vip.	funnull01.vip
efc48cfe.u.fn03.vip.	fn03.vip
a05e098a.u.fn03.vip.	fn03.vip
2d567eaa.u.fn03.vip.	fn03.vip
e30d5705.u.fn03.vip.	fn03.vip
7cba2b41.u.fn03.vip.	fn03.vip
f5656f14.u.fn01.vip.	fn01.vip
da738f71.u.fn03.vip.	fn03.vip
cd55c99f.u.fn03.vip.	fn03.vip
be3c6189.u.fn03.vip.	fn03.vip
395gqubj-u.funnull01.vip.	funnull01.vip
0a6d4cf1.u.fn01.vip.	fn01.vip
c509c3e7.u.fn01.vip.	fn01.vip
98d62472.u.fn01.vip.	fn01.vip
82cbzgrx-u.funnull01.vip.	funnull01.vip
68f2d87f.u.fn03.vip.	fn03.vip
48cf44aa.u.fn03.vip.	fn03.vip
22d590fe.u.fn03.vip.	fn03.vip
xace3hbm-u.funnull.vip.	funnull.vip
xace3hbm-u.funnull01.vip.	funnull01.vip
430c2d37.u.fn03.vip.	fn03.vip
d3e899b9.u.fn03.vip.	fn03.vip
c509c3e7.u.fn03.vip.	fn03.vip
0a6d4cf1.u.fn03.vip.	fn03.vip
79tekgma-u.funnull.vip.	funnull.vip
79tekgma-u.funnull01.vip.	funnull01.vip
0e6370a9.u.fn02.vip.	fn02.vip
de6mhqgz-u.funnull01.vip.	funnull01.vip
0o1kibu135.funnull6.com.	funnull6.com
a4d2e421.u.fn01.vip.	fn01.vip
a4d2e421.u.fn02.vip.	fn02.vip

c1ec496b.u.fn03.vip.	fn03.vip
d270a621.u.fn03.vip.	fn03.vip
ry7azv4k-u.funnull01.vip.	funnull01.vip
82wryse9-u.funnull01.vip.	funnull01.vip
e6345a96.u.fn01.vip.	fn01.vip
467332ef.u.fn03.vip.	fn03.vip
7a3829f0.u.fn01.vip.	fn01.vip
aeb59c84.u.fn03.vip.	fn03.vip
8c303f3a.u.fn03.vip.	fn03.vip
2wm97f5v-u.funnull.vip.	funnull.vip
642cacc0.u.fn03.vip.	fn03.vip
f2a10b9e.u.fn01.vip.	fn01.vip
8dfa37fa.u.fn01.vip.	fn01.vip
5a62a3f8.u.fn01.vip.	fn01.vip
f42a34db.u.fn03.vip.	fn03.vip
edecb6fe.u.fn01.vip.	fn01.vip
caaae22b.u.fn03.vip.	fn03.vip
8udykvsq-u.funnullv23.com.	funnullv23.com
68jfhytx-u.funnull01.vip.	funnull01.vip
50907ed7.u.fn01.vip.	fn01.vip
100301.funnull301.com.	funnull301.com
0o1kibuxij.funnull301.com.	funnull301.com
10e4d5o.funnull.org.	funnull.org
679a64a0.u.fn03.vip.	fn03.vip
3724d94b.u.fn03.vip.	fn03.vip
2wm97f5v-u.funnull01.vip.	funnull01.vip
cb58d89.u.fn01.vip.	fn01.vip
3e90cca6.u.fn03.vip.	fn03.vip
d3b8uwm-u.funnull01.vip.	funnull01.vip
17f77fb7.u.fn03.vip.	fn03.vip
9fd86a85.u.fn03.vip.	fn03.vip
6443afcd.u.fn03.vip.	fn03.vip
4kwsdta6-u.funnull01.vip.	funnull01.vip
0e6370a9.u.fn03.vip.	fn03.vip
03f4debf.u.fn01.vip.	fn01.vip
03f4debf.u.fn02.vip.	fn02.vip
48cf44aa.u.fn01.vip.	fn01.vip
ehbw3ftr-u.funnull01.vip.	funnull01.vip
c0c5fe40.u.fn03.vip.	fn03.vip
qctws5jk-u.funnull01.vip.	funnull01.vip
648fdef1.u.fn01.vip.	fn01.vip
cadd8fa8.u.fn02.vip.	fn02.vip
cexbz3n2-u.funnull01.vip.	funnull01.vip

6d0d2da0.u.fn01.vip.	fn01.vip
0d39c398.u.fn03.vip.	fn03.vip
5a62a3f8.u.fn02.vip.	fn02.vip
n79twf42-u.funnull.vip.	funnull.vip
0d39c398.u.fn02.vip.	fn02.vip
cf7633b76.u.fn03.vip.	fn03.vip
gaqbcr92-u.funnull01.vip.	funnull01.vip
be3c6189.u.fn01.vip.	fn01.vip
bnftu5ap-u.funnull.vip.	funnull.vip
mpa7ukbx-u.funnull.vip.	funnull.vip
y7t9d3mr-u.funnull01.vip.	funnull01.vip
ac4v59y8-u.funnull01.vip.	funnull01.vip
jctaev3h-u.funnull02.vip.	funnull02.vip
8ffe0976.u.fn03.vip.	fn03.vip
0e09cf30.u.fn03.vip.	fn03.vip

For a full list of CNAMEs attributed to Funnull click this link.

Execution: Domain Names Associated with Funnull Infrastructure

Domain Names			
aaev-proogerd.com	asx-martdesks.com	auuiewold.com	binanko8.top
aaev-proolne.top	asx-mealxtd.com	auxumer.top	bingx-cryptojep.com
aave-prooben.com	asx-merdzc.com	auyrtwold.com	bingx-cryptotean.top
aave-proosteg.top	asx-pctoq.com	bakktbftu.top	bingxer-cryptohdrt.top
aave-proostex.net	asx-redirectext.com	bakkt-cc.com	birmexcrpdxr.com
aayedryup.top	asx-royce.com	bakkt-cfd.com	birmex-trpelo.top
adiacdfk9.top	asx-tallettfa.top	bakkt-crypto.com	bitcoincvb.top
aggfhu88.top	asx-tdcjs.com	bakkt-defiwallet.com	bitcoinhdrt.top
aggkline22.top	asx-termtrading.com	bakkthldgs-crypto.com	bitcoinirapro.com
aggwykofe.top	asxtermyfg.com	bakkt-hotwallet.com	bit-coinmcdfk9.top
agjlqua.top	asx-tfdrex.com	bakkthrd.com	bit-coinmgftsz.top
ahkhpn.top	asx-yallet.com	bakkthytc.com	bitcointvi.com
ahthend.top	atomiccfdpyr.com	bakktrdsfde.com	bitcoitradcdfk9.top
ambireamb.com	atomiccfdyheig.top	bakkttiop.com	bitcoitradyuopd.com
ascendexgyt.com	atomprodcty.top	bakkt-trade.com	bitcuidfk9.top
ascendexvcy.top	atomprotgur.top	bakkt-ud.com	bitfinex-defiwallet.com
asxamtst.com	auchelworld.top	bakkt-xp.com	bitfract-protbs.top
asx-avekon.com	auchelworldice.com	bevcmcdfk9.top	bitgoae.com
asx-avensk.com	audtlwold.com	bevcm-rumpd.com	bitopiklc.com
asx-batceds.com	auheowold.com	bevcmubdr.top	bitopniz.top
asx-carext.net	auhtwoldtq.com	bicfatmex.top	bitso-cryptocrs.com
asx-martdeskeia.com	aupoghrt.top	biemexdfk9.top	bitsohdrt.top
	autfewold.com	bifcktmex.com	bitsompdf.top

bitstardcrtyu.com
bitstarlopyr.com
bitstarmietc.com
bitstarnuads.top
bitstarnuand.com
bittebse.com
bitvastprocia.com
bitvastpromheao.com
bive-coinddwo03.top
bive-coinfgts.com
bive-coinymsd.top
bkt-hrad.com
bktrdf.com
blackrockdejr.com
blackrockfdg42.com
blackrockkgtd.com
blckrokdfk9.top
blckroking.top
blckrokivng.com
blockdcgchain.top
bloctkchuainets.com
blofinice.com
blofinvir.top
bltfinex-mo.net
bruhkd.com
brxhkd.top
btcc-co.com
btcc-do.com
btcc-ic.com
btcc-io.com
btcc-mo.com
btcc-od.com
btcc-on.com
btcc-tt.com
btcc-ty.top
btcc-us.com
btcc-xt.com
btcc-xy.com
btcc-yt.com
btcex-crypto.top
btcex-cryptoddwo03.top
btcex-cryptopy.com
bullishko3.top
buxjuns.top
buxmatt.com
bybithdrt.top
capitaltreade.net
cbgerned.com
cbi-banetyik.top
cbkgnfdter.com
cbkuent.com
cbldyoipiwedr.top
cbngdkegwt.com
cboedlo.com
cboekpg.top
cbotcrypthgd.com
cbpurtnfger.com
cbselnu.com
cbsleverage-vip.com
cbsperut.com
cbspmucer.com
cbswallkh.com
cbtodresn.com
cbuodytebg.com
cepzfe.top
cexlbit.com
cexlbited.com
cexlbitzf.top
cexlhdrt.top
cexljedlet.com
cexlmelti.top
cfhkddwo03.top
chicmecrypt.com
ciobsehtfzp.top
cloudtradeice.com
cloudtradeice.top
cloud-treadqydv.com
cloutradeing.com
cmegroupbrup.top
cmegroupecf.top
cmegroupgfe.top
cmegrouphkpd.info
cmegroupmhyo.com
cobwaltbvd.com
coibohupyu.com
coibseing.com
coim-baqysebct.com
coim-batqsebdc.top
coin-bacryptoet.com
coinbase-mpred.com
coinbasepromxs.com
coinbase-qaz.com
coinbase-rafekxt.com
coinbase-shortterm.com
coinbase-sm.com
coinbase-ssd.com
coinbase-ujm.com
coinbasewalletty.com
coinbase-wsx.com
coinbaseyy-ne.com
coinbd-defibnp.top
coin-btcreg.com
coinmatecrytodfk9.top
coinmetroddfk9.top
coinmetrodfk9.top
coinmetrogent.top
coinmetrotaloe.com
coinmetrotsdr.com
coinmetrowent.com

For a full list of domain names identified utilizing Funnull infrastructure click this link.

Recommended Mitigations:

The FBI recommends the following:

1. Domain name system (DNS) providers, Internet service providers, web browser manufacturers, and safe browsing aggregators should take note of the Funnull infrastructure and increase the risk metric for domains hosted on this infrastructure. If the provider has a mechanism to return a risk warning to the end user, it is recommended that they do so.

2. End users should be aware that a HTTPS or green lock icon does not indicate a specific website is trustworthy. End users should also be aware that scam websites often imitate legitimate websites.

3. Potential investors should be aware that there is increased scam risk for investment companies who are not members of self-regulatory organizations such as the National Futures Association (NFA) or Financial Industry Regulatory Authority (FINRA).

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. With regards to specific information that appears in this communication; the context, individual indicators, particularly those of a non-deterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise. Indicators should always be evaluated in light of your complete information security situation.

Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:CLEAR**. Subject to standard copyright rules, the information in this product may be shared without restriction.