VECTRA_REPORT_1

Aug 25th, 2024 to Aug 26th, 2024 | Report Created On: Aug 26th, 2024

VECTRA

HOST SEVERITY SUMMARY

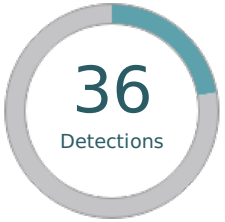
HIGH	CRITICAL
0 Hosts / 0	35 Hosts / 2

LOW	MEDIUM
0 Hosts / 0	0 Hosts / 0

KEY ASSETS

No Key Assets with Detections

DETECTION BREAKDOWN



- Threat Detections: 8 (22%)
- Fixed: 0 (0%)
- Filtered: 28 (78%)
- Whitelisted: 0 (0%)

WORST OFFENDERS

HOSTNAME	PEAK SCORE	
	THREAT	CERTAINTY
nac-buk-01.centenarybank.co.ug	100	81
BTD-CSA-001-LSS.centenarybank.co.ug	100	80
BTD-ISC-033.centenarybank.co.ug	100	74
IP-196.10.139.146	94	79
IP-196.10.138.151	93	75

DETECTIONS BY CATEGORY

Botnet	0
Command & Control	4
Reconnaissance	3
Lateral Movement	1
Exfiltration	0

BIGGEST MOVERS

HOSTNAME	START SCORE		END SCORE	
	THREAT	CERTAINTY	THREAT	CERTAINTY
BTD-CSA-001-LSS.centenarybank...	100	81	100	77
nkr-mbb-001-lss	80	74	80	70
IP-10.224.11.78	54	78	54	76
nac-buk-01.centenarybank.co.ug	100	82	100	79
CBPROFGWPRD01	79	76	79	74

DETECTIONS BY TYPE

Hidden HTTPS Tunnel	4
Port Sweep	2
Automated Replication	1
Internal Darknet Scan	1
Others	0

92 CAMPAIGNS, 2253 HOSTS, 177 DETECTIONS

Showing 30 of 92 total campaigns. This list was cut off because there were too many items.

epay.uneb.ac.ug-16

External Domain: epay.uneb.ac.ug Internal Hosts: 2 Detections: 3 Duration: 162 days 17 hours Last Activity: Aug. 25, 2024, 8:32 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.148	196.10.138.148	52	21		•					Mar 16th, 2024	Aug 25th, 2024
BILL-PAY	10.224.42.12	38	30		•					Mar 16th, 2024	Aug 25th, 2024

archive.ubuntu.com-181

External Domain: archive.ubuntu.com Internal Hosts: 74 Detections: 5 Duration: 92 days 19 hours Last Activity: July 25, 2024, 11:23 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25							Apr 24th, 2024	Jul 25th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Apr 24th, 2024	Jul 25th, 2024
IP-196.10.138.148	196.10.138.148	52	21		•					Apr 24th, 2024	Jul 25th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Apr 24th, 2024	Jul 25th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Apr 24th, 2024	Jul 25th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Apr 24th, 2024	Jul 25th, 2024
IP-196.10.138.149	196.10.138.149	38	24							May 8th, 2024	Jul 25th, 2024
AGENTBANKING-GW	10.224.30.183	38	31							Apr 25th, 2024	Jul 25th, 2024
dev.vendorappraisal.centenary...	10.222.225.64	0	0							Apr 24th, 2024	Jul 25th, 2024
tpsuat.centenarybank.co.ug	10.223.225.65	0	0							Apr 24th, 2024	Jul 25th, 2024
MIS-ARCHIVE-SVR	10.222.130.60	0	0							Apr 24th, 2024	Jul 25th, 2024
SAGE-BIO	10.222.206.35	0	0							Apr 24th, 2024	Jun 25th, 2024
ESB-PRD	10.224.52.82	19	13							Apr 24th, 2024	Jul 25th, 2024
SMS-GATEWAY-SVR	10.222.130.36	0	0							Apr 25th, 2024	Jul 25th, 2024
SWITCH-CBS-AP	10.224.225.66	0	0							Apr 24th, 2024	Jul 25th, 2024
SMS-GATEWAY-SVR-TEST	10.222.130.71	0	0							Apr 24th, 2024	Jul 25th, 2024
SMS-OMNI-GATEWAY	10.222.130.47	0	0							Apr 25th, 2024	Jul 25th, 2024
IP-10.222.130.16	10.222.130.16	0	0							Apr 24th, 2024	Jul 25th, 2024
WEB-REVAMP	10.222.218.20	0	0							Apr 24th, 2024	Jul 25th, 2024
APM-GATEWAY2	10.222.206.15	0	0							Apr 24th, 2024	Jul 25th, 2024
Cente-Website-New	10.222.218.3	0	0							Apr 24th, 2024	Jul 25th, 2024
IP-10.222.130.12	10.222.130.12	0	0							Apr 24th, 2024	Jun 3rd, 2024
new-esb-db-test	10.223.52.140	0	0							Apr 24th, 2024	Apr 29th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
esb-test-svr	10.223.50.68	0	0		Apr 24th, 2024	Apr 27th, 2024
IP-10.222.110.35	10.222.110.35	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Apr 24th, 2024	May 10th, 2024
DESKTOP CENTRAL-HQ	10.222.140.140	28	27	•	Apr 24th, 2024	Jul 25th, 2024
BTD-ISC-104.centenarybank.co....	10.90.20.14	0	0		Apr 25th, 2024	Apr 25th, 2024
IP-10.90.55.29	10.90.55.29	0	0		Apr 25th, 2024	Apr 25th, 2024
btd-alt-005-lss	10.90.18.40	0	0		Apr 29th, 2024	May 4th, 2024
IP-10.222.130.15	10.222.130.15	0	0		Apr 30th, 2024	Jun 19th, 2024

flixmate.net-20

External Domain: flixmate.net Internal Hosts: 8 Detections: 17 Duration: 60 days 10 hours Last Activity: July 1, 2024, 7 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jun 26th, 2024	Jul 1st, 2024
IP-196.10.138.146	196.10.138.146	38	25		May 13th, 2024	Jun 26th, 2024
IP-196.10.138.145	196.10.138.145	80	79		May 2nd, 2024	May 3rd, 2024
IP-196.10.138.148	196.10.138.148	52	21		May 15th, 2024	Jun 21st, 2024
IP-196.10.138.151	196.10.138.151	93	75		May 6th, 2024	May 13th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jun 7th, 2024	Jun 11th, 2024
fsproxy-04-wcg.centenarybank....	10.222.203.30	0	0		May 14th, 2024	May 14th, 2024
stg-sup-031-lss	10.90.43.125	0	0	•	May 2nd, 2024	Jul 1st, 2024

update2.vectranetworks.com-236

External Domain: update2.vectranetworks.com Internal Hosts: 2 Detections: 1 Duration: 30 days 14 hours Last Activity: July 3, 2024, 5 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.146	196.10.138.146	38	25		Jun 3rd, 2024	Jul 3rd, 2024
IP-10.222.199.34	10.222.199.34	38	35	•	Jun 3rd, 2024	Jul 3rd, 2024

detectportal.firefox.com-119

External Domain: detectportal.firefox.com Internal Hosts: 99 Detections: 9 Duration: 21 days 12 hours Last Activity: June 27, 2024, 3:30 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jun 6th, 2024	Jun 24th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jun 6th, 2024	Jun 26th, 2024
Proxy-New	10.222.140.19	52	28		Jun 6th, 2024	Jun 27th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jun 6th, 2024	Jun 26th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jun 6th, 2024	Jun 27th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jun 6th, 2024	Jun 27th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jun 7th, 2024	Jun 24th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jun 7th, 2024	Jun 24th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.147	196.10.138.147	52	33		Jun 6th, 2024	Jun 27th, 2024
PROXY-204	10.222.140.204	52	22		Jun 6th, 2024	Jun 27th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jun 6th, 2024	Jun 26th, 2024
crdbprd-em-sv01.centenarybank...	10.222.140.151	19	18		Jun 18th, 2024	Jun 18th, 2024
ForcePoint	10.222.199.21	19	19		Jun 9th, 2024	Jun 23rd, 2024
PROXY203-DR	10.222.140.203	52	29		Jun 6th, 2024	Jun 27th, 2024
IP-10.90.21.50	10.90.21.50	0	0		Jun 11th, 2024	Jun 11th, 2024
cbp-pc-150	10.90.27.88	0	0		Jun 9th, 2024	Jun 23rd, 2024
fsproxy	10.222.203.27	19	13		Jun 6th, 2024	Jun 27th, 2024
BTD-ITN-002.centenarybank.co....	10.90.34.54	19	6		Jun 6th, 2024	Jun 27th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jun 6th, 2024	Jun 26th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jun 6th, 2024	Jun 26th, 2024
SHAREDVD1.centenarybank.co.ug	10.222.130.104	19	13		Jun 8th, 2024	Jun 9th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jun 6th, 2024	Jun 27th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jun 6th, 2024	Jun 27th, 2024
IP-196.10.139.146	196.10.139.146	0	0		Jun 6th, 2024	Jun 18th, 2024
sec-gms-001-lss	10.90.241.91	0	0		Jun 6th, 2024	Jun 6th, 2024
rtl-sup-222-lss	10.90.50.25	19	13		Jun 6th, 2024	Jun 25th, 2024
strg-off-011	10.90.55.11	0	0		Jun 6th, 2024	Jun 8th, 2024
kml-amb-001-lss	10.76.0.37	19	11		Jun 6th, 2024	Jun 6th, 2024
lir-act-001-lss	10.93.0.57	0	0		Jun 6th, 2024	Jun 8th, 2024
btd-alt-020-lss	10.90.18.65	0	0		Jun 6th, 2024	Jun 27th, 2024

secure.jumia.ug-3

External Domain: secure.jumia.ug Internal Hosts: 12 Detections: 1 Duration: 18 days 04 hours Last Activity: June 24, 2024, 1:19 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28		Jun 21st, 2024	Jun 21st, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jun 20th, 2024	Jun 20th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jun 6th, 2024	Jun 22nd, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jun 6th, 2024	Jun 11th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jun 6th, 2024	Jun 24th, 2024
PROXY-204	10.222.140.204	52	22		Jun 6th, 2024	Jun 24th, 2024
PROXY203-DR	10.222.140.203	52	29		Jun 6th, 2024	Jun 24th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jun 22nd, 2024	Jun 22nd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jun 10th, 2024	Jun 19th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.139.146	196.10.139.146	0	0		Jun 10th, 2024	Jun 10th, 2024
IP-196.10.139.146	196.10.139.146	52	34	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jun 19th, 2024	Jun 19th, 2024
lir-lno-024-lse	10.11.240.96	0	0	•	Jun 19th, 2024	Jun 19th, 2024

172.16.15.2-181

External Domain: 172.16.15.2 Internal Hosts: 2 Detections: 1 Duration: 39 days 15 hours Last Activity: July 16, 2024, 6 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-10.222.0.2	10.222.0.2	0	0		Jun 19th, 2024	Jul 11th, 2024
IP-10.222.1.13	10.222.1.13	35	36	•	Jun 7th, 2024	Jul 16th, 2024

quay.io-123

External Domain: quay.io Internal Hosts: 16 Detections: 1 Duration: 24 days 11 hours Last Activity: July 1, 2024, 2:38 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jun 7th, 2024	Jul 1st, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jun 7th, 2024	Jun 8th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jun 8th, 2024	Jun 10th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jun 7th, 2024	Jul 1st, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jun 7th, 2024	Jul 1st, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jun 27th, 2024	Jun 27th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jun 7th, 2024	Jun 28th, 2024
masterprodhq02	10.224.225.25	0	0		Jun 8th, 2024	Jun 10th, 2024
masterproddr01.crdbproddrcls....	10.224.225.124	0	0		Jun 28th, 2024	Jul 1st, 2024
masterproddr02.crdbproddrcls....	10.224.225.125	0	0	•	Jun 7th, 2024	Jun 28th, 2024
wrkprodhq01	10.224.225.27	0	0		Jun 27th, 2024	Jun 27th, 2024
wrkprodhq02	10.224.225.28	0	0		Jun 26th, 2024	Jun 26th, 2024
masterprodhq01	10.224.225.24	0	0		Jun 7th, 2024	Jul 1st, 2024
masterprodhq03	10.224.225.26	0	0		Jun 7th, 2024	Jun 8th, 2024
OPENSHIFT-DEV-VM	10.222.225.22	0	0		Jun 7th, 2024	Jul 1st, 2024
OPENSHIFT-UAT-VM	10.223.225.20	0	0		Jun 7th, 2024	Jul 1st, 2024

f.vimeocdn.com-21

External Domain: f.vimeocdn.com Internal Hosts: 23 Detections: 1 Duration: 19 days 19 hours Last Activity: June 28, 2024, 2:22 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25		Jun 17th, 2024	Jun 17th, 2024
Proxy-New	10.222.140.19	52	28		Jun 21st, 2024	Jun 21st, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jun 11th, 2024	Jun 25th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jun 15th, 2024	Jun 25th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.148	196.10.138.148	52	21		Jun 11th, 2024	Jun 27th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jun 10th, 2024	Jun 27th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jun 12th, 2024	Jun 21st, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jun 10th, 2024	Jun 28th, 2024
PROXY-204	10.222.140.204	52	22		Jun 8th, 2024	Jun 25th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jun 8th, 2024	Jun 24th, 2024
PROXY203-DR	10.222.140.203	52	29		Jun 18th, 2024	Jun 24th, 2024
fsproxy	10.222.203.27	19	13		Jun 11th, 2024	Jun 28th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jun 8th, 2024	Jun 13th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jun 11th, 2024	Jun 24th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jun 11th, 2024	Jun 27th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jun 12th, 2024	Jun 27th, 2024
IP-196.10.139.146	196.10.139.146	0	0		Jun 12th, 2024	Jun 12th, 2024
btd-isc-099	10.90.20.27	28	11		Jun 10th, 2024	Jun 10th, 2024
IP-10.90.46.79	10.90.46.79	0	0		Jun 17th, 2024	Jun 17th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jun 19th, 2024	Jun 27th, 2024
mgr-cbo-001-lss	10.90.50.138	0	0		Jun 21st, 2024	Jun 21st, 2024
BTD-ISC-033.centenarybank.co....	10.90.20.29	100	71		Jun 22nd, 2024	Jun 24th, 2024
IP-10.90.46.25	10.90.46.25	0	0		Jun 25th, 2024	Jun 25th, 2024

media.swncdn.com-11

External Domain: media.swncdn.com Internal Hosts: 18 Detections: 1 Duration: 20 days 03 hours Last Activity: June 28, 2024, noon

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28		Jun 10th, 2024	Jun 25th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jun 19th, 2024	Jun 27th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jun 11th, 2024	Jun 24th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jun 10th, 2024	Jun 27th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jun 25th, 2024	Jun 25th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jun 10th, 2024	Jun 10th, 2024
PROXY-204	10.222.140.204	52	22		Jun 8th, 2024	Jun 26th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jun 17th, 2024	Jun 27th, 2024
PROXY203-DR	10.222.140.203	52	29		Jun 8th, 2024	Jun 8th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jun 17th, 2024	Jun 27th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jun 19th, 2024	Jun 27th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jun 10th, 2024	Jun 27th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jun 8th, 2024	Jun 28th, 2024
IP-196.10.139.146	196.10.139.146	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jun 8th, 2024	Jun 14th, 2024
stg-sup-031-lss	10.90.43.125	0	0		Jun 10th, 2024	Jun 10th, 2024
btd-inf-003-lss	10.90.240.251	29	6		Jun 10th, 2024	Jun 10th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jun 20th, 2024	Jun 28th, 2024
KRK-TEL-024-LSE.centenarybank...	10.75.0.157	0	0	•	Jun 21st, 2024	Jun 21st, 2024

d8c14d4960ca.853c74aa.me-south-1.token.awswaf.com-12

External Domain: d8c14d4960ca.853c74aa.me-south-1.token.awswaf.com Internal Hosts: 17 Detections: 1 Duration: 18 days 10 hours Last Activity: June 28, 2024, 7 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jun 21st, 2024	Jun 21st, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jun 11th, 2024	Jun 11th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jun 10th, 2024	Jun 28th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jun 10th, 2024	Jun 28th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jun 11th, 2024	Jun 11th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jun 11th, 2024	Jun 25th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jun 10th, 2024	Jun 26th, 2024
fsproxy	10.222.203.27	19	13		Jun 11th, 2024	Jun 20th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jun 10th, 2024	Jun 26th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jun 10th, 2024	Jun 28th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jun 10th, 2024	Jun 28th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jun 10th, 2024	Jun 27th, 2024
IP-196.10.139.146	196.10.139.146	0	0		Jun 10th, 2024	Jun 15th, 2024
btd-off-001-lss	10.90.33.68	38	13		Jun 11th, 2024	Jun 11th, 2024
cbo-chf-020-lss	10.90.13.24	0	0		Jun 11th, 2024	Jun 11th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jun 21st, 2024	Jun 27th, 2024
aud-sup-223-lss	10.90.53.89	30	65	•	Jun 22nd, 2024	Jun 22nd, 2024

centenarybank-co-ug.mail.protection.outlook.com-56

External Domain: centenarybank-co-ug.mail.protection.outlook.com Internal Hosts: 2 Detections: 1 Duration: 20 days 14 hours Last Activity: July 2, 2024, 5 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.144	196.10.138.144	38	29		Jun 12th, 2024	Jun 12th, 2024
SMTP-COREBANKING	10.222.140.233	29	49	•	Jun 12th, 2024	Jul 2nd, 2024

dstv.stream

External Domain: dstv.stream Internal Hosts: 11 Detections: 1 Duration: 16 days 11 hours Last Activity: June 30, 2024, 8:26 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-196.10.138.145	196.10.138.145	80	79							Jun 19th, 2024	Jun 27th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jun 17th, 2024	Jun 23rd, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jun 17th, 2024	Jun 19th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jun 14th, 2024	Jun 22nd, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jun 17th, 2024	Jun 25th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 17th, 2024	Jun 25th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 19th, 2024	Jun 27th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jun 17th, 2024	Jun 23rd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jun 20th, 2024	Jun 30th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jun 20th, 2024	Jun 30th, 2024
aud-sup-123-lss	10.90.241.106	19	14		•					Jun 25th, 2024	Jun 25th, 2024

subscriptions.nation.africa

External Domain: subscriptions.nation.africa Internal Hosts: 19 Detections: 1 Duration: 20 days 03 hours Last Activity: July 4, 2024, 2:53 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28							Jul 3rd, 2024	Jul 4th, 2024
Proxy-New	10.222.140.19	52	28							Jun 19th, 2024	Jun 19th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jun 14th, 2024	Jun 19th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Jun 22nd, 2024	Jun 28th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jun 14th, 2024	Jul 2nd, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 2nd, 2024	Jul 2nd, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jun 17th, 2024	Jul 4th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jun 19th, 2024	Jul 4th, 2024
PROXY-204	10.222.140.204	52	22							Jun 19th, 2024	Jun 28th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jun 17th, 2024	Jul 1st, 2024
PROXY203-DR	10.222.140.203	52	29							Jul 4th, 2024	Jul 4th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 17th, 2024	Jul 1st, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 14th, 2024	Jun 19th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jun 14th, 2024	Jul 2nd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jun 19th, 2024	Jul 3rd, 2024
cent-tech-003	10.170.46.62	0	0							Jun 17th, 2024	Jul 4th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jun 19th, 2024	Jul 3rd, 2024
kml-mgr-002	10.76.0.35	0	0		•					Jun 27th, 2024	Jun 27th, 2024
eba-off-002	10.90.243.170	19	8							Jul 2nd, 2024	Jul 2nd, 2024

api.vectranetworks.com-233

External Domain: api.vectranetworks.com Internal Hosts: 2 Detections: 1 Duration: 29 days 01 hours Last Activity: July 14, 2024, 4 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES: BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-196.10.138.146	196.10.138.146	38	25							Jun 15th, 2024	Jul 14th, 2024	
IP-10.222.199.34	10.222.199.34	38	35		•					Jun 15th, 2024	Jul 14th, 2024	

biblehub.com

External Domain: biblehub.com Internal Hosts: 20 Detections: 1 Duration: 18 days 06 hours Last Activity: July 5, 2024, 4:47 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES: BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-196.10.138.150	196.10.138.150	52	28							Jun 29th, 2024	Jun 29th, 2024	
Proxy-New	10.222.140.19	52	28							Jun 29th, 2024	Jun 29th, 2024	
IP-196.10.138.145	196.10.138.145	80	79							Jun 19th, 2024	Jun 24th, 2024	
PROXY-DR-NEW	10.222.140.20	61	19							Jun 21st, 2024	Jun 21st, 2024	
IP-196.10.138.148	196.10.138.148	52	21							Jun 17th, 2024	Jul 5th, 2024	
IP-196.10.138.147	196.10.138.147	52	33							Jun 21st, 2024	Jul 4th, 2024	
PROXY-204	10.222.140.204	52	22							Jun 21st, 2024	Jun 21st, 2024	
IP-196.10.138.149	196.10.138.149	38	24							Jun 18th, 2024	Jul 1st, 2024	
IP-10.222.219.11	10.222.219.11	29	39							Jun 24th, 2024	Jul 4th, 2024	
IP-196.10.139.10	196.10.139.10	29	39							Jun 24th, 2024	Jul 4th, 2024	
DNS1	10.222.219.10	38	28							Jun 17th, 2024	Jul 1st, 2024	
IP-196.10.138.10	196.10.138.10	38	28							Jun 17th, 2024	Jul 1st, 2024	
PROXY203-DR	10.222.140.203	52	29							Jun 29th, 2024	Jun 29th, 2024	
fsproxy	10.222.203.27	19	13							Jun 21st, 2024	Jul 4th, 2024	
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 18th, 2024	Jul 1st, 2024	
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 19th, 2024	Jun 24th, 2024	
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jun 17th, 2024	Jul 5th, 2024	
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jun 20th, 2024	Jul 2nd, 2024	
IP-196.10.139.146	196.10.139.146	52	34							Jun 20th, 2024	Jul 2nd, 2024	
kbh-tel-003-lse	10.97.0.173	0	0		•					Jun 29th, 2024	Jun 29th, 2024	

api.sofascore.app-6

External Domain: api.sofascore.app Internal Hosts: 9 Detections: 1 Duration: 15 days 23 hours Last Activity: July 5, 2024, 7:10 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES: BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-196.10.138.145	196.10.138.145	80	79							Jun 19th, 2024	Jul 1st, 2024	
IP-196.10.138.148	196.10.138.148	52	21							Jun 26th, 2024	Jul 5th, 2024	
IP-196.10.138.149	196.10.138.149	38	24							Jun 29th, 2024	Jul 5th, 2024	
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 29th, 2024	Jul 5th, 2024	

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 19th, 2024	Jul 1st, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jun 26th, 2024	Jul 5th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 1st, 2024	Jul 5th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 1st, 2024	Jul 5th, 2024
kbl-tel-011-lse	10.7.0.119	0	0		•					Jul 1st, 2024	Jul 1st, 2024

services.interswitchug.com

External Domain: services.interswitchug.com Internal Hosts: 18 Detections: 1 Duration: 20 days 06 hours Last Activity: July 8, 2024, 2:35 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Jun 18th, 2024	Jul 8th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jun 18th, 2024	Jul 3rd, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jun 22nd, 2024	Jul 4th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jun 19th, 2024	Jun 27th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jun 20th, 2024	Jul 8th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 28th, 2024	Jul 8th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 19th, 2024	Jul 4th, 2024
SHAREDVD1.centenarybank.co.ug	10.222.130.104	19	13							Jun 22nd, 2024	Jun 29th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jun 18th, 2024	Jul 3rd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jun 26th, 2024	Jul 5th, 2024
rtl-sup-222-lss	10.90.50.25	19	13							Jun 18th, 2024	Jul 8th, 2024
INT-SUP-028.centenarybank.co....	10.90.242.195	0	0							Jun 18th, 2024	Jul 8th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jun 26th, 2024	Jul 5th, 2024
OPS-OFF-097-LSS	10.90.50.109	29	23							Jun 19th, 2024	Jul 5th, 2024
ops-off-014-lss	10.90.50.97	0	0							Jun 20th, 2024	Jul 5th, 2024
fin-rec-001-lss	10.90.26.127	19	6		•					Jul 1st, 2024	Jul 1st, 2024
ops-off-222-lss	10.90.50.65	0	0							Jul 3rd, 2024	Jul 3rd, 2024
OPS-OFF-013-LSS.centenarybank...	10.90.50.97	0	0							Jul 8th, 2024	Jul 8th, 2024

resolver4.chkp.ctmail.com-42

External Domain: resolver4.chkp.ctmail.com Internal Hosts: 2 Detections: 1 Duration: 20 days 16 hours Last Activity: July 8, 2024, 7:08 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.132	196.10.138.132	38	24		•					Jun 18th, 2024	Jul 8th, 2024
IP-196.10.138.134	196.10.138.134	38	12							Jun 18th, 2024	Jul 8th, 2024

www.radiosimba.ug

External Domain: www.radiosimba.ug Internal Hosts: 9 Detections: 1 Duration: 5 days 08 hours Last Activity: July 9, 2024, 5:15 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES: BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	FIRST SEEN	LAST SEEN
IP-196.10.138.150	196.10.138.150	52	28							Jul 4th, 2024	Jul 4th, 2024	
IP-196.10.138.146	196.10.138.146	38	25							Jul 4th, 2024	Jul 4th, 2024	
IP-196.10.138.145	196.10.138.145	80	79							Jul 4th, 2024	Jul 4th, 2024	
IP-196.10.138.148	196.10.138.148	52	21							Jul 4th, 2024	Jul 4th, 2024	
IP-196.10.138.144	196.10.138.144	38	29							Jul 4th, 2024	Jul 4th, 2024	
IP-196.10.138.149	196.10.138.149	38	24							Jul 9th, 2024	Jul 9th, 2024	
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 9th, 2024	Jul 9th, 2024	
IP-10.90.46.25	10.90.46.25	0	0							Jul 4th, 2024	Jul 4th, 2024	
cent-tech-003	10.170.46.62	0	0		•					Jul 4th, 2024	Jul 4th, 2024	

x.com-13

External Domain: x.com Internal Hosts: 42 Detections: 2 Duration: 20 days 05 hours Last Activity: July 13, 2024, 1 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES: BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	FIRST SEEN	LAST SEEN
IP-196.10.138.150	196.10.138.150	52	28							Jun 23rd, 2024	Jul 12th, 2024	
IP-196.10.138.146	196.10.138.146	38	25							Jun 24th, 2024	Jul 10th, 2024	
Proxy-New	10.222.140.19	52	28							Jun 24th, 2024	Jul 11th, 2024	
IP-196.10.138.145	196.10.138.145	80	79							Jun 24th, 2024	Jul 12th, 2024	
PROXY-DR-NEW	10.222.140.20	61	19							Jun 25th, 2024	Jul 9th, 2024	
IP-196.10.138.148	196.10.138.148	52	21							Jun 23rd, 2024	Jul 13th, 2024	
IP-196.10.138.151	196.10.138.151	93	75							Jun 24th, 2024	Jul 12th, 2024	
IP-196.10.138.144	196.10.138.144	38	29							Jun 24th, 2024	Jul 12th, 2024	
IP-196.10.138.147	196.10.138.147	52	33							Jun 23rd, 2024	Jul 12th, 2024	
PROXY-204	10.222.140.204	52	22							Jun 24th, 2024	Jul 12th, 2024	
IP-196.10.138.149	196.10.138.149	38	24							Jun 23rd, 2024	Jul 13th, 2024	
PROXY203-DR	10.222.140.203	52	29							Jul 3rd, 2024	Jul 12th, 2024	
fsproxy	10.222.203.27	19	13		•					Jun 23rd, 2024	Jul 12th, 2024	
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 23rd, 2024	Jul 13th, 2024	
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 24th, 2024	Jul 12th, 2024	
SHAREDVD1.centenarybank.co.ug	10.222.130.104	19	13							Jun 24th, 2024	Jun 25th, 2024	
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jun 23rd, 2024	Jul 13th, 2024	
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jun 23rd, 2024	Jul 13th, 2024	
IP-196.10.139.146	196.10.139.146	52	34							Jun 23rd, 2024	Jul 13th, 2024	

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
CCC-OFF-222-LSS.centenarybank...	10.90.47.34	0	0		Jun 23rd, 2024	Jul 12th, 2024
ccm-mgr-058	10.90.14.33	29	27	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jun 24th, 2024	Jul 12th, 2024
IP-10.90.46.25	10.90.46.25	0	0		Jun 24th, 2024	Jun 24th, 2024
IP-10.90.46.20	10.90.46.20	0	0		Jun 24th, 2024	Jun 24th, 2024
cent-tech-003	10.170.46.62	0	0		Jun 24th, 2024	Jul 11th, 2024
CCM-CCC-002-LSS.centenarybank...	10.90.47.15	0	0		Jun 24th, 2024	Jun 24th, 2024
ops-off-103-lss	10.90.47.58	19	11		Jun 25th, 2024	Jun 25th, 2024
IP-10.90.46.20	10.90.46.20	0	0		Jun 26th, 2024	Jun 26th, 2024
btd-its-063	10.90.20.11	0	0		Jun 26th, 2024	Jun 26th, 2024
cent-tech-005	10.170.46.38	30	65		Jun 28th, 2024	Jul 12th, 2024
IP-10.90.46.25	10.90.46.25	0	0		Jun 28th, 2024	Jun 28th, 2024

172.21.75.2-59

External Domain: 172.21.75.2 Internal Hosts: 2 Detections: 1 Duration: 20 days 03 hours Last Activity: July 10, 2024, 7 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-10.222.0.2	10.222.0.2	0	0		Jul 8th, 2024	Jul 8th, 2024
IP-10.222.1.13	10.222.1.13	35	36	•	Jun 20th, 2024	Jul 10th, 2024

mirrors.128technology.com-16

External Domain: mirrors.128technology.com Internal Hosts: 7 Detections: 1 Duration: 20 days 01 hours Last Activity: July 16, 2024, 6:17 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jun 26th, 2024	Jul 15th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jun 26th, 2024	Jul 16th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jun 26th, 2024	Jul 15th, 2024
REMEDIATION.centenarybank.co....	10.222.204.15	0	0	•	Jun 26th, 2024	Jul 16th, 2024
IP-10.222.199.45	10.222.199.45	0	0		Jun 26th, 2024	Jul 15th, 2024
IP-10.222.199.47	10.222.199.47	0	0		Jun 26th, 2024	Jul 15th, 2024
IP-10.222.199.46	10.222.199.46	0	0		Jun 26th, 2024	Jul 15th, 2024

172.16.2.2-138

External Domain: 172.16.2.2 Internal Hosts: 2 Detections: 1 Duration: 43 days 06 hours Last Activity: Aug. 8, 2024, 9 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-10.222.1.13	10.222.1.13	35	36	•	Jun 26th, 2024	Aug 8th, 2024
btd-bita-003-ls	10.90.34.66	0	0		Jul 8th, 2024	Jul 8th, 2024

update2.vectranetworks.com-249

External Domain: update2.vectranetworks.com Internal Hosts: 2 Detections: 2 Duration: 20 days 08 hours Last Activity: July 16, 2024, 11 a.m.

				DETECTION CATEGORIES	FIRST SEEN	LAST SEEN

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
HOSTNAME	LAST IP	THREAT	CERTAINTY	BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25	BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	Jun 26th, 2024	Jul 16th, 2024
IP-10.222.199.34	10.222.199.34	38	35		•				•	Jun 26th, 2024	Jul 16th, 2024

flixmate.net-22

External Domain: flixmate.net Internal Hosts: 2 Detections: 1 Duration: 20 days 06 hours Last Activity: July 17, 2024, 3 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Jun 27th, 2024	Jul 17th, 2024
stg-sup-031-lss	10.90.43.125	0	0		•					Jun 27th, 2024	Jul 17th, 2024

plausible.zinlab.com-41

External Domain: plausible.zinlab.com Internal Hosts: 9 Detections: 17 Duration: 58 days 12 hours Last Activity: Aug. 25, 2024, 9 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Jun 28th, 2024	Aug 16th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 14th, 2024	Aug 25th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 29th, 2024	Aug 9th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 9th, 2024	Aug 12th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Aug 16th, 2024	Aug 16th, 2024
BI-REPORTING	10.222.206.20	29	41			•				Aug 14th, 2024	Aug 25th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 19th, 2024	Jul 19th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 19th, 2024	Jul 19th, 2024
stg-sup-031-lss	10.90.43.125	0	0			•			•	Jun 28th, 2024	Aug 16th, 2024

data.tradingview.com-20

External Domain: data.tradingview.com Internal Hosts: 13 Detections: 1 Duration: 19 days 15 hours Last Activity: July 18, 2024, 9:02 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28							Jul 11th, 2024	Jul 11th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 2nd, 2024	Jul 17th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 9th, 2024	Jul 17th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 8th, 2024	Jul 11th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 11th, 2024	Jul 11th, 2024
PROXY-204	10.222.140.204	52	22							Jul 11th, 2024	Jul 11th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jun 28th, 2024	Jul 17th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 28th, 2024	Jul 17th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 2nd, 2024	Jul 17th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 9th, 2024	Jul 17th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 3rd, 2024	Jul 18th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 3rd, 2024	Jul 18th, 2024
mrt-fin-001	10.77.0.36	0	0		•					Jul 11th, 2024	Jul 11th, 2024

api.x.com-10

External Domain: api.x.com Internal Hosts: 34 Detections: 1 Duration: 20 days 04 hours Last Activity: July 19, 2024, 10:20 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28							Jul 1st, 2024	Jul 19th, 2024
IP-196.10.138.146	196.10.138.146	38	25							Jun 29th, 2024	Jul 19th, 2024
Proxy-New	10.222.140.19	52	28							Jun 29th, 2024	Jul 11th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jun 29th, 2024	Jul 19th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Jun 29th, 2024	Jul 3rd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jun 29th, 2024	Jul 19th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jun 29th, 2024	Jul 19th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jun 29th, 2024	Jul 19th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jun 29th, 2024	Jul 18th, 2024
PROXY-204	10.222.140.204	52	22							Jun 29th, 2024	Jul 16th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jun 29th, 2024	Jul 19th, 2024
PROXY203-DR	10.222.140.203	52	29							Jul 3rd, 2024	Jul 12th, 2024
fsproxy	10.222.203.27	19	13							Jun 29th, 2024	Jul 18th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jun 29th, 2024	Jul 19th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jun 29th, 2024	Jul 19th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		•					Jun 29th, 2024	Jul 19th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jun 29th, 2024	Jul 19th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jun 29th, 2024	Jul 19th, 2024
BTD-OFF-321-LSS	10.90.27.28	19	17							Jun 29th, 2024	Jun 29th, 2024
btd-csa-009-lss	10.90.21.12	0	0							Jul 1st, 2024	Jul 1st, 2024
btd-0ff-021-lss	10.90.18.43	38	22							Jul 1st, 2024	Jul 1st, 2024
cent-tech-003	10.170.46.62	0	0							Jul 1st, 2024	Jul 16th, 2024
ops-off-102-lss	10.90.243.35	0	0							Jul 2nd, 2024	Jul 17th, 2024
cent-tech-004	10.170.46.42	0	0							Jul 3rd, 2024	Jul 3rd, 2024
mpi-mgr-001-lss	10.55.0.89	29	6							Jul 5th, 2024	Jul 5th, 2024
CCC-OFF-222-LSS.centenarybank...	10.90.47.34	0	0							Jul 6th, 2024	Jul 6th, 2024
ccm-mgr-058	10.90.14.33	29	27							Jul 8th, 2024	Jul 10th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-10.90.10.207	10.90.10.207	0	0		Jul 8th, 2024	Jul 8th, 2024
fin-grp-001	10.90.46.14	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 11th, 2024	Jul 11th, 2024
cent-tech-005	10.170.46.38	30	65		Jul 12th, 2024	Jul 12th, 2024

cf.bstatic.com-21

External Domain: cf.bstatic.com Internal Hosts: 16 Detections: 2 Duration: 21 days 01 hours Last Activity: July 22, 2024, 6:08 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jul 4th, 2024	Jul 10th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 2nd, 2024	Jul 20th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jul 10th, 2024	Jul 19th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 2nd, 2024	Jul 20th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 16th, 2024	Jul 16th, 2024
PROXY-204	10.222.140.204	52	22		Jul 10th, 2024	Jul 19th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 4th, 2024	Jul 22nd, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 4th, 2024	Jul 22nd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 2nd, 2024	Jul 20th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 2nd, 2024	Jul 20th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 1st, 2024	Jul 17th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 1st, 2024	Jul 17th, 2024
krk-bs-002-lse	10.75.0.158	0	0	•	Jul 13th, 2024	Jul 13th, 2024
grp-stg-001	10.170.46.51	39	70		Jul 16th, 2024	Jul 16th, 2024
ebb-ba-06-lse	10.57.240.160	0	0	•	Jul 16th, 2024	Jul 16th, 2024
ops-off-104-lss	10.90.241.252	19	9		Jul 19th, 2024	Jul 19th, 2024

inetcallhome.stratus.com-13

External Domain: inetcallhome.stratus.com Internal Hosts: 4 Detections: 1 Duration: 21 days 04 hours Last Activity: July 23, 2024, 8:58 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.145	196.10.138.145	80	79	•	Jul 2nd, 2024	Jul 23rd, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 2nd, 2024	Jul 23rd, 2024
IP-10.222.180.201	10.222.180.201	0	0		Jul 2nd, 2024	Jul 23rd, 2024
IP-10.222.180.204	10.222.180.204	0	0		Jul 2nd, 2024	Jul 23rd, 2024

efristest.ura.go.ug-66

External Domain: efristest.ura.go.ug Internal Hosts: 9 Detections: 2 Duration: 21 days 05 hours Last Activity: July 23, 2024, 9:56 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28	•	Jul 16th, 2024	Jul 16th, 2024
IP-196.10.138.146	196.10.138.146	38	25	•	Jul 2nd, 2024	Jul 19th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Jul 15th, 2024	Jul 23rd, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 4th, 2024	Jul 23rd, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 2nd, 2024	Jul 12th, 2024
FIN-REQUISITION	10.222.110.26	0	0							Jul 2nd, 2024	Jul 19th, 2024
LEASING-APP-TST.centenarybank...	10.222.110.230	0	0							Jul 2nd, 2024	Jul 23rd, 2024
EFRIS.centenarybank.co.ug	10.222.110.16	0	0							Jul 4th, 2024	Jul 23rd, 2024
IP-10.90.27.138	10.90.27.138	0	0							Jul 15th, 2024	Jul 15th, 2024

81.19.104.167-14

External Domain: 81.19.104.167 Internal Hosts: 187 Detections: 2 Duration: 20 days 06 hours Last Activity: July 22, 2024, 9:59 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		•					Jul 3rd, 2024	Jul 19th, 2024
IP-196.10.138.146	196.10.138.146	38	25							Jul 2nd, 2024	Jul 19th, 2024
Proxy-New	10.222.140.19	52	28							Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 2nd, 2024	Jul 19th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 2nd, 2024	Jul 22nd, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 2nd, 2024	Jul 20th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 2nd, 2024	Jul 22nd, 2024
PROXY-204	10.222.140.204	52	22							Jul 2nd, 2024	Jul 22nd, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 4th, 2024	Jul 20th, 2024
SCCM-HQ	10.222.140.111	30	73							Jul 2nd, 2024	Jul 22nd, 2024
PROXY203-DR	10.222.140.203	52	29							Jul 3rd, 2024	Jul 22nd, 2024
MERC-BANK-DB	10.222.110.41	19	14							Jul 4th, 2024	Jul 22nd, 2024
KAVNEW-HQ	10.222.140.43	22	17							Jul 2nd, 2024	Jul 21st, 2024
SOLARWINDSAPP	10.222.110.210	39	70							Jul 7th, 2024	Jul 7th, 2024
LEASING-DB-TST.centenarybank....	10.222.110.231	0	0							Jul 6th, 2024	Jul 22nd, 2024
LEASING-APP-TST.centenarybank...	10.222.110.230	0	0							Jul 2nd, 2024	Jul 21st, 2024
FINSUNAPP.centenarybank.co.ug	10.222.110.30	0	0							Jul 3rd, 2024	Jul 21st, 2024
iam-job-uat	10.222.140.205	0	0							Jul 13th, 2024	Jul 20th, 2024
SERVICEDESK-UAT.centenarybank...	10.222.140.17	0	0							Jul 5th, 2024	Jul 22nd, 2024
risk-jump.centenarybank.co.ug	10.222.206.31	0	0							Jul 7th, 2024	Jul 7th, 2024
TEAMMATE-TST-DB.centenarybank...	10.222.110.108	0	0							Jul 2nd, 2024	Jul 20th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
cbo-off-070-lss	10.90.50.22	0	0		Jul 2nd, 2024	Jul 4th, 2024
btd-mis-016	10.90.33.55	19	6	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 2nd, 2024	Jul 16th, 2024
BT-BOF-217	10.90.242.101	19	13		Jul 2nd, 2024	Jul 19th, 2024
fin-chf-004-lss	10.90.26.51	0	0		Jul 2nd, 2024	Jul 2nd, 2024
aud-mgr-004-lss	10.90.40.26	29	12		Jul 2nd, 2024	Jul 2nd, 2024
btd-mgr-010-lss	10.90.33.69	19	13		Jul 2nd, 2024	Jul 22nd, 2024
btd-off-201-lss	10.90.240.157	19	13		Jul 2nd, 2024	Jul 10th, 2024

time.samsungcloudsolution.com-36

External Domain: time.samsungcloudsolution.com Internal Hosts: 20 Detections: 1 Duration: 19 days 06 hours Last Activity: July 22, 2024, 1:04 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 22nd, 2024	Jul 22nd, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 4th, 2024	Jul 10th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 14th, 2024	Jul 15th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 10th, 2024	Jul 12th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 3rd, 2024	Jul 19th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 8th, 2024	Jul 22nd, 2024
IP-10.90.34.57	10.90.34.57	0	0		Jul 4th, 2024	Jul 4th, 2024
IP-10.90.34.89	10.90.34.89	0	0		Jul 5th, 2024	Jul 5th, 2024
IP-10.90.34.89	10.90.34.89	0	0		Jul 8th, 2024	Jul 8th, 2024
IP-10.90.34.89	10.90.34.89	0	0		Jul 9th, 2024	Jul 9th, 2024
IP-10.90.34.89	10.90.34.89	0	0		Jul 10th, 2024	Jul 10th, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 12th, 2024	Jul 12th, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 15th, 2024	Jul 15th, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 15th, 2024	Jul 15th, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 16th, 2024	Jul 18th, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 19th, 2024	Jul 19th, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 22nd, 2024	Jul 22nd, 2024
IP-10.90.34.93	10.90.34.93	0	0		Jul 22nd, 2024	Jul 22nd, 2024

cdn-api.syteapi.com

External Domain: cdn-api.syteapi.com Internal Hosts: 8 Detections: 1 Duration: 5 days 15 hours Last Activity: July 16, 2024, 7:13 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79		Jul 16th, 2024	Jul 16th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
IP-196.10.138.148	196.10.138.148	52	21		Jul 10th, 2024	Jul 10th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 10th, 2024	Jul 10th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 16th, 2024	Jul 16th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 10th, 2024	Jul 10th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 11th, 2024	Jul 11th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 11th, 2024	Jul 11th, 2024
STG-OFF-001-LSS.centenarybank...	10.90.43.13	0	0	•	Jul 16th, 2024	Jul 16th, 2024

analytics.avcdn.net-5

External Domain: analytics.avcdn.net Internal Hosts: 9 Detections: 1 Duration: 20 days 01 hours Last Activity: July 23, 2024, 7:53 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 3rd, 2024	Jul 17th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 4th, 2024	Jul 5th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 3rd, 2024	Jul 22nd, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jul 6th, 2024	Jul 14th, 2024
IP-196.10.138.144	196.10.138.144	38	29	•	Jul 12th, 2024	Jul 18th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 11th, 2024	Jul 22nd, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 3rd, 2024	Jul 23rd, 2024
mbl-btl-001-lss	10.90.10.52	19	9		Jul 3rd, 2024	Jul 19th, 2024

api.ahagamecenter.com

External Domain: api.ahagamecenter.com Internal Hosts: 18 Detections: 1 Duration: 21 days 04 hours Last Activity: July 24, 2024, 1:59 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 4th, 2024	Jul 24th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 3rd, 2024	Jul 24th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 3rd, 2024	Jul 24th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 3rd, 2024	Jul 24th, 2024
IP-196.10.138.151	196.10.138.151	93	75	•	Jul 3rd, 2024	Jul 20th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 3rd, 2024	Jul 24th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 5th, 2024	Jul 23rd, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 6th, 2024	Jul 24th, 2024
IP-10.253.164.180	10.253.164.180	0	0		Jul 4th, 2024	Jul 4th, 2024
IP-10.253.164.187	10.253.164.187	0	0		Jul 6th, 2024	Jul 6th, 2024
IP-10.253.194.223	10.253.194.223	0	0		Jul 10th, 2024	Jul 10th, 2024
IP-10.253.194.143	10.253.194.143	0	0		Jul 15th, 2024	Jul 15th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-10.253.165.119	10.253.165.119	0	0		Jul 15th, 2024	Jul 15th, 2024
IP-10.253.194.182	10.253.194.182	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 15th, 2024	Jul 15th, 2024
IP-10.253.194.211	10.253.194.211	0	0		Jul 16th, 2024	Jul 16th, 2024
IP-10.253.195.90	10.253.195.90	0	0		Jul 19th, 2024	Jul 19th, 2024
IP-10.253.164.217	10.253.164.217	0	0		Jul 22nd, 2024	Jul 22nd, 2024
btd-sdt-001-lse	10.90.19.88	0	0		Jul 23rd, 2024	Jul 23rd, 2024

news-af.feednews.com-32

External Domain: news-af.feednews.com Internal Hosts: 14 Detections: 1 Duration: 20 days 08 hours Last Activity: July 24, 2024, 4:14 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 11th, 2024	Jul 24th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 4th, 2024	Jul 23rd, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 4th, 2024	Jul 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 9th, 2024	Jul 24th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jul 8th, 2024	Jul 24th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 4th, 2024	Jul 24th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 4th, 2024	Jul 24th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 8th, 2024	Jul 24th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 15th, 2024	Jul 15th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 15th, 2024	Jul 15th, 2024
IP-10.253.194.143	10.253.194.143	0	0		Jul 15th, 2024	Jul 15th, 2024
IP-10.253.164.217	10.253.164.217	0	0		Jul 22nd, 2024	Jul 22nd, 2024
IP-10.253.230.192	10.253.230.192	0	0		Jul 24th, 2024	Jul 24th, 2024
IP-10.90.46.20	10.90.46.20	0	0		Jul 24th, 2024	Jul 24th, 2024

x.com-17

External Domain: x.com Internal Hosts: 61 Detections: 5 Duration: 27 days 14 hours Last Activity: July 31, 2024, 5:04 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 4th, 2024	Jul 31st, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 4th, 2024	Jul 31st, 2024
Proxy-New	10.222.140.19	52	28		Jul 5th, 2024	Jul 23rd, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 4th, 2024	Jul 31st, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jul 9th, 2024	Jul 27th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 4th, 2024	Jul 31st, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jul 5th, 2024	Jul 31st, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 4th, 2024	Jul 30th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 5th, 2024	Jul 31st, 2024
PROXY-204	10.222.140.204	52	22		Jul 9th, 2024	Jul 22nd, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 4th, 2024	Jul 31st, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
PROXY203-DR	10.222.140.203	52	29	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 5th, 2024	Jul 22nd, 2024
fsproxy	10.222.203.27	19	13		Jul 5th, 2024	Jul 31st, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 4th, 2024	Jul 31st, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40	•	Jul 4th, 2024	Jul 31st, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33	•	Jul 4th, 2024	Jul 31st, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25	•	Jul 4th, 2024	Jul 31st, 2024
IP-196.10.139.146	196.10.139.146	52	34	•	Jul 4th, 2024	Jul 31st, 2024
ops-off-102-lss	10.90.243.35	0	0		Jul 4th, 2024	Jul 19th, 2024
cent-tech-003	10.170.46.62	0	0		Jul 4th, 2024	Jul 24th, 2024
ccm-mgr-058	10.90.14.33	29	27	•	Jul 5th, 2024	Jul 12th, 2024
mpi-mgr-001-lss	10.55.0.89	29	6		Jul 5th, 2024	Jul 5th, 2024
CCC-OFF-222-LSS.centenarybank...	10.90.47.34	0	0		Jul 6th, 2024	Jul 30th, 2024
aud-sup-006	10.90.10.29	0	0		Jul 8th, 2024	Jul 8th, 2024
ccm-off-020-lss	10.90.47.54	19	4		Jul 9th, 2024	Jul 30th, 2024
fin-grp-001	10.90.46.14	0	0		Jul 11th, 2024	Jul 11th, 2024
cent-tech-004	10.170.46.42	0	0		Jul 11th, 2024	Jul 11th, 2024
FMK-GM-002	10.90.26.163	0	0		Jul 12th, 2024	Jul 12th, 2024
cent-tech-005	10.170.46.38	30	65		Jul 12th, 2024	Jul 12th, 2024
btd-its-063	10.90.20.11	0	0		Jul 15th, 2024	Jul 15th, 2024

music-201.boomplaymusic.com-3

External Domain: music-201.boomplaymusic.com Internal Hosts: 26 Detections: 1 Duration: 13 days 22 hours Last Activity: July 25, 2024, 8:31 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 13th, 2024	Jul 25th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 18th, 2024	Jul 24th, 2024
Proxy-New	10.222.140.19	52	28		Jul 18th, 2024	Jul 18th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 11th, 2024	Jul 13th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 11th, 2024	Jul 22nd, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 13th, 2024	Jul 22nd, 2024
PROXY-204	10.222.140.204	52	22		Jul 18th, 2024	Jul 18th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 13th, 2024	Jul 24th, 2024
PROXY203-DR	10.222.140.203	52	29		Jul 17th, 2024	Jul 17th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 24th, 2024	Jul 24th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 11th, 2024	Jul 11th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 11th, 2024	Jul 22nd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 13th, 2024	Jul 23rd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
igg-dc1	10.71.0.3	0	0		Jul 22nd, 2024	Jul 22nd, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 13th, 2024	Jul 23rd, 2024
msk-wu-002-lse	10.3.0.35	0	0		Jul 13th, 2024	Jul 13th, 2024
krk-qms-001	10.75.0.30	0	0		Jul 13th, 2024	Jul 13th, 2024
PDH-LNO-007-LSE	10.82.240.24	0	0		Jul 13th, 2024	Jul 13th, 2024
kum-off-004-lse	10.46.0.71	19	17		Jul 13th, 2024	Jul 13th, 2024
krk-fin-009-lse	10.75.0.33	0	0		Jul 13th, 2024	Jul 13th, 2024
mtn-tel-008	10.17.0.44	0	0		Jul 18th, 2024	Jul 18th, 2024
kbg-amb-001-lss	10.23.0.53	0	0	•	Jul 18th, 2024	Jul 18th, 2024
kwk-ast-011-lss	10.87.0.37	0	0		Jul 18th, 2024	Jul 18th, 2024
IP-10.90.55.16	10.90.55.16	0	0		Jul 18th, 2024	Jul 18th, 2024
nak-fof-023-lss	10.18.240.42	0	0		Jul 18th, 2024	Jul 18th, 2024
KSR-QMS-001	10.72.0.30	0	0		Jul 25th, 2024	Jul 25th, 2024

update2.vectranetworks.com-250

External Domain: update2.vectranetworks.com Internal Hosts: 2 Detections: 2 Duration: 27 days 01 hours Last Activity: Aug. 1, 2024, 5 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25	•	Jul 5th, 2024	Aug 1st, 2024
IP-10.222.199.34	10.222.199.34	38	35	•	Jul 5th, 2024	Aug 1st, 2024

audio11.mixcloud.com-46

External Domain: audio11.mixcloud.com Internal Hosts: 8 Detections: 1 Duration: 11 days 03 hours Last Activity: July 19, 2024, 4:38 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79		Jul 8th, 2024	Jul 19th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jul 10th, 2024	Jul 10th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 10th, 2024	Jul 10th, 2024
PROXY203-DR	10.222.140.203	52	29		Jul 10th, 2024	Jul 10th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 19th, 2024	Jul 19th, 2024
fmk-off-013-lss	10.90.240.135	19	11		Jul 8th, 2024	Jul 13th, 2024
cent-tech-003	10.170.46.62	0	0		Jul 10th, 2024	Jul 10th, 2024
btd-0ff-021-lss	10.90.18.43	38	22	•	Jul 19th, 2024	Jul 19th, 2024

quay.io-125

External Domain: quay.io Internal Hosts: 24 Detections: 1 Duration: 25 days 09 hours Last Activity: Aug. 1, 2024, 12:51 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 7th, 2024	Aug 1st, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 7th, 2024	Aug 1st, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Jul 8th, 2024	Jul 17th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 7th, 2024	Aug 1st, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 12th, 2024	Jul 12th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 7th, 2024	Jul 30th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 9th, 2024	Jul 30th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 7th, 2024	Jul 28th, 2024
masterprodhq02	10.224.225.25	0	0							Jul 8th, 2024	Jul 17th, 2024
masterproddr01.crdbproddrcls....	10.224.225.124	0	0							Jul 12th, 2024	Jul 12th, 2024
masterproddr02.crdbproddrcls....	10.224.225.125	0	0		•					Jul 7th, 2024	Jul 28th, 2024
masterproddr03.crdbproddrcls....	10.224.225.126	29	35							Jul 12th, 2024	Aug 1st, 2024
wrkproddr01.crdbproddrcls.cen...	10.224.225.127	0	0							Jul 12th, 2024	Jul 12th, 2024
wrkproddr03.crdbproddrcls.cen...	10.224.225.129	0	0							Jul 12th, 2024	Jul 12th, 2024
wrkprodhq01	10.224.225.27	0	0							Jul 9th, 2024	Jul 26th, 2024
wrkprodhq03.crdbprodhqcls.cen...	10.224.225.29	0	0							Jul 9th, 2024	Jul 15th, 2024
wrkprodhq02	10.224.225.28	0	0							Jul 9th, 2024	Jul 26th, 2024
masterprodhq01	10.224.225.24	0	0							Jul 7th, 2024	Jul 30th, 2024
masterprodhq03	10.224.225.26	0	0							Jul 7th, 2024	Aug 1st, 2024
OPENSHIFT-DEV-VM	10.222.225.22	0	0							Jul 7th, 2024	Aug 1st, 2024
OPENSHIFT-UAT-VM	10.223.225.20	0	0							Jul 7th, 2024	Aug 1st, 2024
wrkproddr02.crdbproddrcls.cen...	10.224.225.128	0	0							Jul 12th, 2024	Jul 12th, 2024
wrkprodhq04.crdbprodhqcls.cen...	10.224.225.35	0	0							Jul 29th, 2024	Jul 30th, 2024
wrkprodhq05.crdbprodhqcls.cen...	10.224.225.36	0	0							Jul 29th, 2024	Jul 30th, 2024

software.128technology.com-296

External Domain: software.128technology.com Internal Hosts: 9 Detections: 2 Duration: 21 days 10 hours Last Activity: July 30, 2024, 4:01 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Jul 9th, 2024	Jul 30th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 11th, 2024	Jul 11th, 2024
IP-196.10.138.151	196.10.138.151	93	75		•					Jul 9th, 2024	Jul 30th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 9th, 2024	Jul 30th, 2024
REMEDIATION.centenarybank.co....	10.222.204.15	0	0		•					Jul 9th, 2024	Jul 30th, 2024
IP-10.222.199.45	10.222.199.45	0	0							Jul 9th, 2024	Jul 30th, 2024
IP-10.222.199.47	10.222.199.47	0	0							Jul 9th, 2024	Jul 30th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 16th, 2024	Jul 24th, 2024
IP-10.222.199.46	10.222.199.46	0	0							Jul 9th, 2024	Jul 30th, 2024

stream.hydeinnovations.com-134

External Domain: stream.hydeinnovations.com Internal Hosts: 17 Detections: 2 Duration: 22 days 04 hours Last Activity: Aug. 2, 2024, 1:58 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Jul 11th, 2024	Jul 22nd, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 11th, 2024	Aug 2nd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 11th, 2024	Jul 31st, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 11th, 2024	Jul 24th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 22nd, 2024	Jul 23rd, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 15th, 2024	Jul 25th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 15th, 2024	Jul 31st, 2024
fsproxy	10.222.203.27	19	13							Jul 15th, 2024	Jul 25th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 15th, 2024	Jul 31st, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 11th, 2024	Aug 2nd, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 11th, 2024	Jul 31st, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 11th, 2024	Aug 2nd, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 11th, 2024	Aug 2nd, 2024
grp-stg-001	10.170.46.51	39	70							Jul 22nd, 2024	Jul 23rd, 2024
cb-sup-001-lss	10.90.242.184	19	11							Jul 22nd, 2024	Jul 22nd, 2024
ktd-fof-001-lss	10.78.0.90	0	0		•					Jul 24th, 2024	Jul 24th, 2024
mbd-lno-004-lss	10.56.240.34	0	0		•					Jul 26th, 2024	Jul 26th, 2024

app.usercentrics.eu

External Domain: app.usercentrics.eu Internal Hosts: 11 Detections: 1 Duration: 19 days 04 hours Last Activity: July 31, 2024, 6:56 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25							Jul 16th, 2024	Jul 24th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 16th, 2024	Jul 30th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 12th, 2024	Jul 30th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 19th, 2024	Jul 29th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 12th, 2024	Jul 31st, 2024
fsproxy	10.222.203.27	19	13							Jul 19th, 2024	Jul 29th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 13th, 2024	Jul 31st, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 12th, 2024	Jul 29th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 17th, 2024	Jul 31st, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 17th, 2024	Jul 31st, 2024
kwp-tel-055-lsd	10.32.240.164	0	0		•					Jul 25th, 2024	Jul 25th, 2024

music-201.boomplaymusic.com-4

External Domain: music-201.boomplaymusic.com Internal Hosts: 49 Detections: 2 Duration: 17 days 05 hours Last Activity: July 30, 2024, 5:12 p.m.

				DETECTION CATEGORIES	FIRST SEEN	LAST SEEN

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
HOSTNAME	LAST IP	THREAT	CERTAINTY	BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 13th, 2024	Jul 25th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 18th, 2024	Jul 30th, 2024
Proxy-New	10.222.140.19	52	28		Jul 18th, 2024	Jul 27th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 13th, 2024	Jul 30th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jul 26th, 2024	Jul 26th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 18th, 2024	Jul 30th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jul 25th, 2024	Jul 30th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 26th, 2024	Jul 30th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 13th, 2024	Jul 27th, 2024
PROXY-204	10.222.140.204	52	22		Jul 18th, 2024	Jul 25th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 13th, 2024	Jul 30th, 2024
PROXY203-DR	10.222.140.203	52	29		Jul 17th, 2024	Jul 27th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 24th, 2024	Jul 30th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 27th, 2024	Jul 30th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 22nd, 2024	Jul 22nd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 13th, 2024	Jul 23rd, 2024
igg-dc1	10.71.0.3	0	0		Jul 22nd, 2024	Jul 22nd, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 13th, 2024	Jul 23rd, 2024
msk-wu-002-lse	10.3.0.35	0	0		Jul 13th, 2024	Jul 26th, 2024
krk-qms-001	10.75.0.30	0	0		Jul 13th, 2024	Jul 13th, 2024
PDH-LNO-007-LSE	10.82.240.24	0	0		Jul 13th, 2024	Jul 13th, 2024
kum-off-004-lse	10.46.0.71	19	17		Jul 13th, 2024	Jul 13th, 2024
krk-fin-009-lse	10.75.0.33	0	0		Jul 13th, 2024	Jul 13th, 2024
mtn-tel-008	10.17.0.44	0	0		Jul 18th, 2024	Jul 18th, 2024
kwk-ast-011-lss	10.87.0.37	0	0		Jul 18th, 2024	Jul 18th, 2024
IP-10.90.55.16	10.90.55.16	0	0		Jul 18th, 2024	Jul 18th, 2024
nak-fof-023-lss	10.18.240.42	0	0		Jul 18th, 2024	Jul 18th, 2024
btd-dca-015-lss	10.90.27.20	19	19		Jul 25th, 2024	Jul 25th, 2024
mkn-tel-303-lse	10.25.0.147	0	0		Jul 25th, 2024	Jul 25th, 2024
amo-act-001-lss	10.93.0.55	0	0		Jul 25th, 2024	Jul 25th, 2024

ws.qualified.com-2

External Domain: ws.qualified.com Internal Hosts: 19 Detections: 1 Duration: 18 days 06 hours Last Activity: Aug. 2, 2024, 6:11 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 24th, 2024	Jul 24th, 2024
Proxy-New	10.222.140.19	52	28		Jul 25th, 2024	Jul 25th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Jul 15th, 2024	Aug 2nd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 16th, 2024	Aug 1st, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 18th, 2024	Jul 27th, 2024
PROXY-204	10.222.140.204	52	22							Jul 25th, 2024	Jul 25th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 18th, 2024	Aug 2nd, 2024
PROXY203-DR	10.222.140.203	52	29							Jul 27th, 2024	Jul 27th, 2024
fsproxy	10.222.203.27	19	13							Jul 18th, 2024	Jul 24th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 18th, 2024	Aug 2nd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 15th, 2024	Aug 2nd, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 16th, 2024	Jul 31st, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 23rd, 2024	Aug 2nd, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 23rd, 2024	Aug 2nd, 2024
cdp-sup-014	10.90.50.88	0	0							Jul 23rd, 2024	Jul 23rd, 2024
IP-10.90.46.41	10.90.46.41	0	0							Jul 26th, 2024	Jul 26th, 2024
kwp-tel-055-lsd	10.32.240.164	0	0		•					Jul 27th, 2024	Jul 27th, 2024
IP-10.90.55.27	10.90.55.27	0	0							Jul 29th, 2024	Jul 29th, 2024
IP-10.170.35.116	10.170.35.116	0	0							Aug 1st, 2024	Aug 1st, 2024

pebed.dm-event.net-47

External Domain: pebed.dm-event.net Internal Hosts: 21 Detections: 1 Duration: 19 days 23 hours Last Activity: Aug. 5, 2024, 12:03 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28							Jul 17th, 2024	Aug 2nd, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 16th, 2024	Aug 5th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Jul 23rd, 2024	Jul 23rd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 16th, 2024	Aug 5th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 25th, 2024	Jul 26th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 17th, 2024	Aug 2nd, 2024
PROXY-204	10.222.140.204	52	22							Jul 22nd, 2024	Jul 22nd, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 17th, 2024	Aug 5th, 2024
PROXY203-DR	10.222.140.203	52	29							Jul 17th, 2024	Aug 2nd, 2024
fsproxy	10.222.203.27	19	13							Jul 20th, 2024	Jul 30th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 17th, 2024	Aug 5th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 16th, 2024	Aug 5th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		•					Jul 16th, 2024	Aug 5th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 17th, 2024	Aug 5th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 17th, 2024	Aug 5th, 2024
IP-10.90.59.13	10.90.59.13	0	0							Jul 29th, 2024	Jul 29th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
fmk-off-013-lss	10.90.240.135	19	11							Jul 30th, 2024	Jul 30th, 2024
IP-10.90.59.13	10.90.59.13	0	0							Jul 30th, 2024	Jul 30th, 2024
IP-10.90.59.13	10.90.59.13	0	0							Jul 30th, 2024	Jul 30th, 2024
IP-10.170.35.52	10.170.35.52	0	0							Aug 1st, 2024	Aug 1st, 2024
IP-10.90.59.13	10.90.59.13	0	0							Aug 3rd, 2024	Aug 3rd, 2024

downloads.hpdaas.com-52

External Domain: downloads.hpdaas.com Internal Hosts: 146 Detections: 7 Duration: 26 days Last Activity: Aug. 12, 2024, 6:54 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Jul 22nd, 2024	Aug 10th, 2024
IP-196.10.138.146	196.10.138.146	38	25							Jul 18th, 2024	Aug 10th, 2024
Proxy-New	10.222.140.19	52	28							Jul 18th, 2024	Aug 11th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 17th, 2024	Aug 12th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Jul 17th, 2024	Aug 11th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 17th, 2024	Aug 11th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 17th, 2024	Aug 12th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 17th, 2024	Aug 10th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 17th, 2024	Aug 11th, 2024
PROXY-204	10.222.140.204	52	22							Jul 18th, 2024	Aug 11th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 17th, 2024	Aug 12th, 2024
PROXY203-DR	10.222.140.203	52	29							Jul 17th, 2024	Aug 11th, 2024
fsproxy	10.222.203.27	19	13							Jul 30th, 2024	Aug 8th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 17th, 2024	Aug 12th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 17th, 2024	Aug 12th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 17th, 2024	Aug 11th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 17th, 2024	Aug 12th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 17th, 2024	Aug 12th, 2024
BTD-ALT-021-LSS.centenarybank...	10.90.240.255	0	0							Jul 17th, 2024	Jul 18th, 2024
btd-dca-007-lss	10.90.27.14	19	5						•	Jul 17th, 2024	Aug 1st, 2024
str-mgr-033-lss	10.90.43.20	0	0							Jul 17th, 2024	Jul 18th, 2024
CRD-MGR-111-LSS.centenarybank...	10.90.242.117	19	11							Jul 17th, 2024	Jul 17th, 2024
bt-hlp-002-lss	10.90.19.63	38	32							Jul 17th, 2024	Aug 12th, 2024
DESKTOP-5K4HIJR	10.90.50.86	19	3							Jul 17th, 2024	Jul 19th, 2024
bt-dca-004-lss	10.90.27.26	19	13							Jul 17th, 2024	Jul 29th, 2024
btd-alt-099-lss	10.90.241.117	0	0							Jul 17th, 2024	Jul 17th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN
fin-sup-123-lss	10.90.26.109	0	0		Jul 18th, 2024	Jul 24th, 2024
crd-off-005-lss	10.90.10.192	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 18th, 2024	Aug 9th, 2024
fmk-off-011-lss	10.90.26.145	0	0		Jul 18th, 2024	Jul 24th, 2024
bloomberg-01	10.90.26.55	0	0		Jul 20th, 2024	Jul 26th, 2024

flixmate.net-27

External Domain: flixmate.net Internal Hosts: 7 Detections: 6 Duration: 38 days 13 hours Last Activity: Aug. 25, 2024, 10 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jul 18th, 2024	Aug 16th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Aug 14th, 2024	Aug 25th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 29th, 2024	Aug 9th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 9th, 2024	Aug 12th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 16th, 2024	Aug 16th, 2024
BI-REPORTING	10.222.206.20	29	41	•	Aug 14th, 2024	Aug 25th, 2024
stg-sup-031-lss	10.90.43.125	0	0	• •	Jul 18th, 2024	Aug 16th, 2024

c.whatsapp.net

External Domain: c.whatsapp.net Internal Hosts: 156 Detections: 1 Duration: 20 days 05 hours Last Activity: Aug. 7, 2024, 12:55 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Jul 18th, 2024	Aug 7th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 18th, 2024	Aug 6th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 18th, 2024	Aug 7th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 18th, 2024	Aug 7th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Jul 18th, 2024	Aug 7th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 18th, 2024	Aug 7th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 18th, 2024	Aug 7th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 18th, 2024	Aug 7th, 2024
btd-bit-96-lss	10.90.18.59	0	0		Jul 20th, 2024	Jul 20th, 2024
rtl-off-111-lss	10.90.50.110	19	7		Jul 18th, 2024	Aug 2nd, 2024
stg-sup-031-lss	10.90.43.125	0	0		Jul 18th, 2024	Aug 2nd, 2024
rtl-off-040-lss	10.90.242.182	0	0		Jul 18th, 2024	Jul 30th, 2024
IP-10.90.55.23	10.90.55.23	0	0		Jul 18th, 2024	Jul 18th, 2024
btd-alt-004-lss	10.90.18.76	19	14		Jul 18th, 2024	Aug 1st, 2024
IP-10.90.27.146	10.90.27.146	0	0		Jul 18th, 2024	Jul 18th, 2024
PRO-SUP-001-LSS.centenarybank...	10.90.18.62	39	85		Jul 18th, 2024	Aug 2nd, 2024
SEC-MGR-009-LSS.centenarybank...	10.90.30.19	38	27	•	Jul 18th, 2024	Aug 2nd, 2024
fin-project-lss	10.90.26.139	19	5		Jul 19th, 2024	Jul 25th, 2024
STG-MNG-050.centenarybank.co....	10.90.240.191	19	6		Jul 19th, 2024	Jul 19th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-10.90.27.141	10.90.27.141	0	0		Jul 19th, 2024	Jul 19th, 2024
IP-10.77.0.66	10.77.0.66	0	0		Jul 21st, 2024	Jul 21st, 2024
tech-1	10.170.46.41	0	0		Jul 22nd, 2024	Aug 5th, 2024
pdh-lno-001-lse	10.82.0.32	0	0		Jul 22nd, 2024	Jul 22nd, 2024
aud-mgr-004-lss	10.90.40.26	29	12		Jul 22nd, 2024	Jul 25th, 2024
IP-10.90.55.23	10.90.55.23	0	0		Jul 22nd, 2024	Jul 22nd, 2024
IP-10.90.55.16	10.90.55.16	0	0		Jul 22nd, 2024	Jul 22nd, 2024
IP-10.90.30.74	10.90.30.74	0	0		Jul 23rd, 2024	Jul 23rd, 2024
btd-sdt-001-lse	10.90.19.88	0	0		Jul 23rd, 2024	Jul 23rd, 2024
rtl-off-099-lss	10.90.50.111	38	6		Jul 23rd, 2024	Jul 23rd, 2024
IP-10.90.55.23	10.90.55.23	0	0		Jul 23rd, 2024	Jul 23rd, 2024

flerap.com

External Domain: flerap.com Internal Hosts: 11 Detections: 2 Duration: 18 days 10 hours Last Activity: Aug. 6, 2024, 8:15 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
Proxy-New	10.222.140.19	52	28		Jul 22nd, 2024	Jul 22nd, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 22nd, 2024	Aug 6th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jul 22nd, 2024	Jul 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 19th, 2024	Aug 3rd, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 22nd, 2024	Aug 6th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 22nd, 2024	Aug 6th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 22nd, 2024	Aug 6th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 19th, 2024	Aug 3rd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 26th, 2024	Aug 5th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 26th, 2024	Aug 5th, 2024
FMK-GM-002	10.90.26.163	0	0		Jul 31st, 2024	Jul 31st, 2024

yum.oracle.com-7

External Domain: yum.oracle.com Internal Hosts: 33 Detections: 1 Duration: 21 days 20 hours Last Activity: Aug. 9, 2024, 11:58 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Jul 19th, 2024	Aug 8th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Jul 19th, 2024	Aug 9th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 19th, 2024	Aug 7th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 19th, 2024	Aug 9th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-196.10.138.151	196.10.138.151	93	75		Jul 19th, 2024	Aug 9th, 2024	
IP-196.10.138.144	196.10.138.144	38	29		Jul 19th, 2024	Aug 7th, 2024	
IP-196.10.138.147	196.10.138.147	52	33		Jul 19th, 2024	Aug 9th, 2024	
IP-10.222.81.136	10.222.81.136	0	0		Jul 19th, 2024	Aug 7th, 2024	
IP-10.222.219.11	10.222.219.11	29	39		Jul 19th, 2024	Aug 9th, 2024	
IP-196.10.139.10	196.10.139.10	29	39		Jul 19th, 2024	Aug 9th, 2024	
IP-10.224.225.130	10.224.225.130	0	0		Jul 19th, 2024	Aug 9th, 2024	
OPENSHIFT-JUMP-UAT	10.223.225.22	0	0		Jul 19th, 2024	Aug 9th, 2024	
crdbhq-kvm-node2.centenaryban...	10.222.81.32	0	0		Jul 19th, 2024	Aug 9th, 2024	
crdbhq-kvm-node1.centenaryban...	10.222.81.31	0	0		Jul 19th, 2024	Aug 9th, 2024	
DNS1	10.222.219.10	38	28		Jul 19th, 2024	Aug 9th, 2024	
IP-196.10.138.10	196.10.138.10	38	28		Jul 19th, 2024	Aug 9th, 2024	
IP-10.222.81.137	10.222.81.137	0	0		Jul 19th, 2024	Aug 7th, 2024	
IP-10.222.81.135	10.222.81.135	0	0		Jul 19th, 2024	Aug 7th, 2024	
IP-10.224.225.31	10.224.225.31	0	0		Jul 19th, 2024	Aug 9th, 2024	
DESKTOP CENTRAL-HQ	10.222.140.140	28	27		Jul 19th, 2024	Aug 9th, 2024	
IP-10.223.60.11	10.223.60.11	0	0		Jul 19th, 2024	Aug 9th, 2024	
IP-10.223.60.10	10.223.60.10	0	0		Jul 19th, 2024	Aug 9th, 2024	
IP-10.223.60.12	10.223.60.12	0	0		Jul 19th, 2024	Aug 9th, 2024	
crdb-el-repo.centenarybank.co...	10.222.140.76	0	0		Jul 19th, 2024	Aug 9th, 2024	
calypso-ds-dev	10.225.60.10	0	0		Jul 19th, 2024	Aug 9th, 2024	
calypso-eng-dev	10.225.60.11	31	72		Jul 19th, 2024	Aug 9th, 2024	
None	10.225.60.12	0	0		Jul 19th, 2024	Aug 9th, 2024	
IP-10.225.61.9	10.225.61.9	0	0		Jul 19th, 2024	Aug 3rd, 2024	
drclsbastion.crdbproddrcls.ce...	10.224.225.131	0	0		Jul 19th, 2024	Aug 6th, 2024	
IP-10.224.225.131	10.224.225.131	0	0		Aug 7th, 2024	Aug 7th, 2024	

i.ebayimg.com-8

External Domain: i.ebayimg.com Internal Hosts: 17 Detections: 1 Duration: 16 days 23 hours Last Activity: Aug. 8, 2024, 7:41 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
Proxy-New	10.222.140.19	52	28		Jul 26th, 2024	Aug 3rd, 2024	
IP-196.10.138.145	196.10.138.145	80	79		Jul 22nd, 2024	Aug 8th, 2024	
PROXY-DR-NEW	10.222.140.20	61	19		Jul 26th, 2024	Aug 1st, 2024	
IP-196.10.138.148	196.10.138.148	52	21		Jul 24th, 2024	Aug 1st, 2024	
IP-196.10.138.147	196.10.138.147	52	33		Jul 26th, 2024	Aug 6th, 2024	
PROXY-204	10.222.140.204	52	22		Jul 25th, 2024	Aug 1st, 2024	
IP-196.10.138.149	196.10.138.149	38	24		Jul 23rd, 2024	Aug 2nd, 2024	
PROXY203-DR	10.222.140.203	52	29		Jul 31st, 2024	Aug 3rd, 2024	
fsproxy	10.222.203.27	19	13		Aug 2nd, 2024	Aug 6th, 2024	

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 23rd, 2024	Aug 2nd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 23rd, 2024	Aug 8th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 24th, 2024	Aug 1st, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 23rd, 2024	Aug 7th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 23rd, 2024	Aug 7th, 2024
aud-mgr-004-lss	10.90.40.26	29	12							Jul 22nd, 2024	Jul 22nd, 2024
IP-10.170.35.57	10.170.35.57	0	0							Jul 31st, 2024	Jul 31st, 2024
isg-fof-006-lse	10.59.0.72	19	12		•					Aug 2nd, 2024	Aug 2nd, 2024

172.27.56.2

External Domain: 172.27.56.2 Internal Hosts: 2 Detections: 1 Duration: 20 days 08 hours Last Activity: Aug. 9, 2024, noon

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-10.222.1.5	10.222.1.5	38	29		•					Jul 20th, 2024	Aug 9th, 2024
BTD-ITN-002.centenarybank.co....	10.90.34.54	19	6							Aug 1st, 2024	Aug 8th, 2024

api.sofascore.app-9

External Domain: api.sofascore.app Internal Hosts: 10 Detections: 2 Duration: 20 days 01 hours Last Activity: Aug. 12, 2024, 2:38 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Aug 3rd, 2024	Aug 12th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 24th, 2024	Aug 7th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 30th, 2024	Jul 30th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 31st, 2024	Aug 12th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 31st, 2024	Aug 12th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 3rd, 2024	Aug 12th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 24th, 2024	Aug 7th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 23rd, 2024	Aug 1st, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 23rd, 2024	Aug 1st, 2024
bt-hlp-002-lss	10.90.19.63	38	32		•					Aug 3rd, 2024	Aug 5th, 2024

dispatcher.cdp.us-east-1.prod.data.typeform.com

External Domain: dispatcher.cdp.us-east-1.prod.data.typeform.com Internal Hosts: 8 Detections: 2 Duration: 16 days 06 hours Last Activity: Aug. 14, 2024, 4 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Aug 6th, 2024	Aug 8th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 1st, 2024	Aug 8th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Aug 12th, 2024	Aug 12th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.149	196.10.138.149	38	24							Jul 29th, 2024	Aug 14th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 29th, 2024	Aug 14th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 6th, 2024	Aug 8th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Aug 1st, 2024	Aug 8th, 2024
stg-mgr-048-lss	10.90.43.120	0	0		•				•	Aug 6th, 2024	Aug 8th, 2024

g.ezoic.net-4

External Domain: g.ezoic.net Internal Hosts: 21 Detections: 1 Duration: 19 days 05 hours Last Activity: Aug. 13, 2024, 3:37 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Jul 26th, 2024	Jul 26th, 2024
IP-196.10.138.146	196.10.138.146	38	25							Aug 9th, 2024	Aug 9th, 2024
Proxy-New	10.222.140.19	52	28							Jul 31st, 2024	Jul 31st, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 1st, 2024	Aug 9th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 30th, 2024	Aug 9th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Jul 31st, 2024	Jul 31st, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 2nd, 2024	Aug 2nd, 2024
PROXY-204	10.222.140.204	52	22							Jul 31st, 2024	Jul 31st, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 25th, 2024	Aug 13th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 25th, 2024	Aug 13th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 1st, 2024	Aug 1st, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 30th, 2024	Aug 7th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Jul 25th, 2024	Jul 25th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Jul 25th, 2024	Jul 25th, 2024
IP-10.170.35.55	10.170.35.55	0	0							Jul 31st, 2024	Jul 31st, 2024
crd-off-025-lss	10.90.31.185	19	11		•					Aug 7th, 2024	Aug 7th, 2024
IP-10.90.55.25	10.90.55.25	0	0							Aug 8th, 2024	Aug 8th, 2024
IP-10.90.55.27	10.90.55.27	0	0							Aug 8th, 2024	Aug 8th, 2024
IP-10.90.59.12	10.90.59.12	0	0							Aug 9th, 2024	Aug 9th, 2024
IP-10.90.55.27	10.90.55.27	0	0							Aug 9th, 2024	Aug 9th, 2024
IP-10.90.55.25	10.90.55.25	0	0							Aug 9th, 2024	Aug 9th, 2024

52.114.112.182-2

External Domain: 52.114.112.182 Internal Hosts: 24 Detections: 3 Duration: 11 days 03 hours Last Activity: Aug. 13, 2024, 4 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28		•					Aug 8th, 2024	Aug 13th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 2nd, 2024	Aug 2nd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
PROXY-DR-NEW	10.222.140.20	61	19							Aug 2nd, 2024	Aug 13th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 2nd, 2024	Aug 13th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Aug 2nd, 2024	Aug 2nd, 2024
IP-196.10.138.144	196.10.138.144	38	29							Aug 2nd, 2024	Aug 2nd, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 2nd, 2024	Aug 13th, 2024
PROXY-204	10.222.140.204	52	22		•					Aug 8th, 2024	Aug 8th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Aug 2nd, 2024	Aug 2nd, 2024
PROXY203-DR	10.222.140.203	52	29		•					Aug 6th, 2024	Aug 8th, 2024
btd-mis-001	10.90.240.87	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-off-099-lss	10.90.33.52	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-off-211-lss	10.90.33.50	0	0							Aug 2nd, 2024	Aug 2nd, 2024
knu-tel-002-lse	10.63.0.40	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-mis-014-lss	10.90.33.54	29	21							Aug 2nd, 2024	Aug 2nd, 2024
btd-mis-004-lss	10.90.33.73	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-mis-103-lss	10.90.33.59	0	0							Aug 2nd, 2024	Aug 2nd, 2024
FIN-OFF-021-LSS.centenarybank...	10.90.33.73	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-mis-099	10.90.243.51	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-hlp-003	10.90.19.41	0	0							Aug 2nd, 2024	Aug 2nd, 2024
btd-alt-012-lse	10.90.242.13	0	0							Aug 6th, 2024	Aug 6th, 2024
DESKTOP-4I1VV4R	10.90.243.244	0	0							Aug 12th, 2024	Aug 12th, 2024
ebb-amb-003-lse	10.52.0.84	0	0							Aug 13th, 2024	Aug 13th, 2024
mgr-cbo-001-lss	10.90.50.138	0	0							Aug 13th, 2024	Aug 13th, 2024

onlineradiobox.com-3

External Domain: onlineradiobox.com Internal Hosts: 23 Detections: 2 Duration: 21 days 02 hours Last Activity: Aug. 16, 2024, 9:01 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Aug 2nd, 2024	Aug 2nd, 2024
IP-196.10.138.146	196.10.138.146	38	25							Aug 14th, 2024	Aug 14th, 2024
Proxy-New	10.222.140.19	52	28							Aug 5th, 2024	Aug 13th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 27th, 2024	Aug 12th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Aug 7th, 2024	Aug 16th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 26th, 2024	Aug 16th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Aug 2nd, 2024	Aug 2nd, 2024
IP-196.10.138.147	196.10.138.147	52	33							Jul 26th, 2024	Aug 16th, 2024
PROXY-204	10.222.140.204	52	22							Aug 7th, 2024	Aug 13th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 27th, 2024	Aug 15th, 2024
PROXY203-DR	10.222.140.203	52	29							Aug 5th, 2024	Aug 12th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
fsproxy	10.222.203.27	19	13	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 26th, 2024	Aug 16th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 27th, 2024	Aug 15th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 29th, 2024	Aug 12th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 26th, 2024	Aug 16th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Aug 1st, 2024	Aug 16th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Aug 1st, 2024	Aug 16th, 2024
IP-10.253.129.201	10.253.129.201	0	0		Jul 27th, 2024	Jul 27th, 2024
KRK-TEL-024-LSE.centenarybank...	10.75.0.157	0	0		Aug 2nd, 2024	Aug 2nd, 2024
kyj-ba-001-lss	10.22.0.120	0	0		Aug 2nd, 2024	Aug 2nd, 2024
crd-off-009-lse	10.90.31.40	0	0	•	Aug 8th, 2024	Aug 9th, 2024
IP-10.170.35.109	10.170.35.109	0	0		Aug 9th, 2024	Aug 9th, 2024
crd-off-429-lss	10.90.242.220	22	8		Aug 14th, 2024	Aug 14th, 2024

analytics-ingress-global.bitmovin.com-4

External Domain: analytics-ingress-global.bitmovin.com Internal Hosts: 9 Detections: 1 Duration: 17 days 03 hours Last Activity: Aug. 15, 2024, 9 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.146	196.10.138.146	38	25		Aug 10th, 2024	Aug 11th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 31st, 2024	Aug 15th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 30th, 2024	Aug 14th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Jul 31st, 2024	Jul 31st, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 29th, 2024	Aug 15th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 29th, 2024	Aug 15th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Jul 31st, 2024	Aug 15th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 30th, 2024	Aug 14th, 2024
aud-mgr-020-lss	10.90.241.45	29	29	•	Aug 9th, 2024	Aug 9th, 2024

j1le6kzmv7.execute-api.eu-west-1.amazonaws.com-3

External Domain: j1le6kzmv7.execute-api.eu-west-1.amazonaws.com Internal Hosts: 15 Detections: 2 Duration: 23 days 04 hours Last Activity: Aug. 19, 2024, 5:40 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Aug 5th, 2024	Aug 13th, 2024
Proxy-New	10.222.140.19	52	28		Aug 9th, 2024	Aug 9th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 29th, 2024	Aug 17th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Aug 9th, 2024	Aug 9th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 27th, 2024	Aug 19th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 7th, 2024	Aug 13th, 2024
PROXY-204	10.222.140.204	52	22		Aug 13th, 2024	Aug 13th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 30th, 2024	Aug 7th, 2024
fsproxy	10.222.203.27	19	13		Aug 7th, 2024	Aug 13th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM			
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 30th, 2024	Aug 7th, 2024	
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 29th, 2024	Aug 17th, 2024	
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Jul 27th, 2024	Aug 19th, 2024	
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Aug 5th, 2024	Aug 13th, 2024	
IP-196.10.139.146	196.10.139.146	52	34							Aug 5th, 2024	Aug 13th, 2024	
bt-sup-010-lse	10.90.27.38	37	8				•			Aug 5th, 2024	Aug 13th, 2024	

www.kucoin.com-10

External Domain: www.kucoin.com Internal Hosts: 12 Detections: 1 Duration: 17 days 16 hours Last Activity: Aug. 18, 2024, 5 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM			
IP-196.10.138.145	196.10.138.145	80	79							Jul 31st, 2024	Aug 17th, 2024	
PROXY-DR-NEW	10.222.140.20	61	19							Aug 8th, 2024	Aug 16th, 2024	
IP-196.10.138.148	196.10.138.148	52	21							Aug 3rd, 2024	Aug 17th, 2024	
IP-196.10.138.147	196.10.138.147	52	33							Aug 8th, 2024	Aug 16th, 2024	
IP-196.10.138.149	196.10.138.149	38	24							Aug 4th, 2024	Aug 18th, 2024	
fsproxy	10.222.203.27	19	13							Aug 8th, 2024	Aug 16th, 2024	
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Aug 4th, 2024	Aug 18th, 2024	
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Jul 31st, 2024	Aug 17th, 2024	
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Aug 3rd, 2024	Aug 17th, 2024	
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Aug 5th, 2024	Aug 16th, 2024	
IP-196.10.139.146	196.10.139.146	52	34							Aug 5th, 2024	Aug 16th, 2024	
btd-cba-001-lss	10.90.27.22	0	0				•			Aug 11th, 2024	Aug 11th, 2024	

ruxit-synth-screencap.s3-accelerate.amazonaws.com-16

External Domain: ruxit-synth-screencap.s3-accelerate.amazonaws.com Internal Hosts: 2 Detections: 1 Duration: 25 days 01 hours Last Activity: Aug. 23, 2024, 6:02 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM			
IP-196.10.138.151	196.10.138.151	93	75		•					Jul 29th, 2024	Aug 23rd, 2024	
APM-GATEWAY2	10.222.206.15	0	0							Jul 29th, 2024	Aug 23rd, 2024	

52.114.113.137

External Domain: 52.114.113.137 Internal Hosts: 40 Detections: 1 Duration: 14 days 18 hours Last Activity: Aug. 16, 2024, 1:40 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM			
IP-196.10.138.150	196.10.138.150	52	28							Aug 2nd, 2024	Aug 2nd, 2024	
Proxy-New	10.222.140.19	52	28							Aug 2nd, 2024	Aug 16th, 2024	
IP-196.10.138.145	196.10.138.145	80	79							Aug 2nd, 2024	Aug 16th, 2024	
PROXY-DR-NEW	10.222.140.20	61	19				•			Aug 12th, 2024	Aug 16th, 2024	

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.148	196.10.138.148	52	21	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 16th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Aug 1st, 2024	Aug 16th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Aug 16th, 2024	Aug 16th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 2nd, 2024	Aug 16th, 2024
PROXY-204	10.222.140.204	52	22		Aug 2nd, 2024	Aug 16th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 2nd, 2024	Aug 16th, 2024
PROXY203-DR	10.222.140.203	52	29		Aug 3rd, 2024	Aug 3rd, 2024
bloomberg-01	10.90.26.55	0	0		Aug 1st, 2024	Aug 1st, 2024
ops-rsm-001-lss	10.90.50.139	0	0		Aug 2nd, 2024	Aug 2nd, 2024
reg-mgr-011-lss	10.90.10.184	0	0		Aug 2nd, 2024	Aug 2nd, 2024
ops-rse-004-lss	10.64.240.11	38	24		Aug 2nd, 2024	Aug 2nd, 2024
ops-rmw-002-lss	10.56.0.33	0	0		Aug 2nd, 2024	Aug 2nd, 2024
fin-off-033	10.90.10.230	19	11		Aug 2nd, 2024	Aug 2nd, 2024
ops-rmg-012	10.83.0.50	29	21		Aug 2nd, 2024	Aug 2nd, 2024
rtl-sup-040-lss	10.90.50.210	0	0		Aug 2nd, 2024	Aug 2nd, 2024
rmf-off-072-lss	10.90.10.28	19	3		Aug 2nd, 2024	Aug 2nd, 2024
kpl-visa-002	10.35.240.48	0	0		Aug 3rd, 2024	Aug 3rd, 2024
btd-mis-006-lss	10.90.18.48	29	32		Aug 3rd, 2024	Aug 3rd, 2024
btd-mis-012-lss	10.90.18.27	19	2		Aug 7th, 2024	Aug 7th, 2024
mpr-bof-002-lse	10.37.240.12	0	0		Aug 12th, 2024	Aug 12th, 2024
HRD-OFF-002-LSS.centenarybank...	10.90.22.60	0	0		Aug 12th, 2024	Aug 12th, 2024
hr-mgr-099-lss	10.90.22.57	29	11		Aug 12th, 2024	Aug 12th, 2024
kbg-lno-004-lse	10.23.240.2	0	0		Aug 12th, 2024	Aug 12th, 2024
adj-tel-001-lse	10.85.0.33	0	0		Aug 12th, 2024	Aug 12th, 2024
bb-mcs-001-lss	10.52.240.35	28	29		Aug 15th, 2024	Aug 15th, 2024
rtl-off-300-lss	10.90.50.87	19	11		Aug 15th, 2024	Aug 15th, 2024

flag.lab.amplitude.com-3

External Domain: flag.lab.amplitude.com Internal Hosts: 40 Detections: 1 Duration: 20 days 07 hours Last Activity: Aug. 19, 2024, 5:09 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 14th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Aug 9th, 2024	Aug 16th, 2024
Proxy-New	10.222.140.19	52	28		Jul 31st, 2024	Aug 14th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Aug 3rd, 2024	Aug 19th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Jul 30th, 2024	Aug 19th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 31st, 2024	Aug 19th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Aug 15th, 2024	Aug 19th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 30th, 2024	Aug 19th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.147	196.10.138.147	52	33							Aug 1st, 2024	Aug 13th, 2024
PROXY-204	10.222.140.204	52	22							Aug 1st, 2024	Aug 1st, 2024
IP-196.10.138.149	196.10.138.149	38	24							Jul 30th, 2024	Aug 19th, 2024
PROXY203-DR	10.222.140.203	52	29							Aug 1st, 2024	Aug 19th, 2024
fsproxy	10.222.203.27	19	13							Aug 13th, 2024	Aug 13th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Jul 30th, 2024	Aug 19th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 3rd, 2024	Aug 19th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Aug 2nd, 2024	Aug 19th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Aug 5th, 2024	Aug 9th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Aug 5th, 2024	Aug 9th, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 1st, 2024	Aug 1st, 2024
IP-10.170.35.78	10.170.35.78	0	0							Aug 2nd, 2024	Aug 2nd, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 6th, 2024	Aug 6th, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 8th, 2024	Aug 8th, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 12th, 2024	Aug 12th, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 12th, 2024	Aug 12th, 2024
IP-10.170.46.57	10.170.46.57	0	0							Aug 13th, 2024	Aug 13th, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 13th, 2024	Aug 13th, 2024
IP-10.90.59.14	10.90.59.14	0	0							Aug 14th, 2024	Aug 14th, 2024
IP-10.90.33.26	10.90.33.26	0	0							Aug 14th, 2024	Aug 14th, 2024
IP-10.90.59.16	10.90.59.16	0	0							Aug 14th, 2024	Aug 14th, 2024
IP-10.170.35.247	10.170.35.247	0	0							Aug 15th, 2024	Aug 15th, 2024

cdn.samsungcloudsolution.com-35

External Domain: cdn.samsungcloudsolution.com Internal Hosts: 241 Detections: 2 Duration: 25 days 16 hours Last Activity: Aug. 25, 2024, 10:33 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		•					Jul 30th, 2024	Aug 23rd, 2024
IP-196.10.138.146	196.10.138.146	38	25							Jul 31st, 2024	Aug 19th, 2024
Proxy-New	10.222.140.19	52	28							Aug 5th, 2024	Aug 8th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Jul 30th, 2024	Aug 22nd, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Aug 5th, 2024	Aug 7th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Jul 31st, 2024	Aug 23rd, 2024
IP-196.10.138.151	196.10.138.151	93	75							Aug 2nd, 2024	Aug 25th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Jul 31st, 2024	Aug 25th, 2024
IP-196.10.138.147	196.10.138.147	52	33		•					Jul 31st, 2024	Aug 22nd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
PROXY-204	10.222.140.204	52	22		Aug 5th, 2024	Aug 13th, 2024
IP-196.10.138.149	196.10.138.149	38	24	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 31st, 2024	Aug 22nd, 2024
PROXY203-DR	10.222.140.203	52	29		Aug 5th, 2024	Aug 7th, 2024
IP-10.8.0.235	10.8.0.235	19	19		Aug 12th, 2024	Aug 19th, 2024
krk-dc	10.75.0.2	0	0		Aug 8th, 2024	Aug 8th, 2024
INFRA-EXMBX4-HQ	10.222.140.56	39	85		Aug 6th, 2024	Aug 23rd, 2024
IP-10.9.0.235	10.9.0.235	19	19		Aug 14th, 2024	Aug 14th, 2024
risk-jump.centenarybank.co.ug	10.222.206.31	0	0		Aug 9th, 2024	Aug 19th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Aug 3rd, 2024	Aug 22nd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Aug 5th, 2024	Aug 13th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Aug 6th, 2024	Aug 22nd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Aug 5th, 2024	Aug 7th, 2024
KYOTERA-DC1	10.13.0.2	0	0		Aug 9th, 2024	Aug 9th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Aug 5th, 2024	Aug 7th, 2024
REUTERZ-PC.centenarybank.co.ug	10.90.26.150	0	0		Aug 6th, 2024	Aug 6th, 2024
FMKT-OFF-011.centenarybank.co...	10.90.26.237	22	15		Aug 8th, 2024	Aug 8th, 2024
crd-off-113-lss	10.90.31.17	19	11		Jul 31st, 2024	Jul 31st, 2024
ARU-QMS-001-LSE.centenarybank...	10.15.0.169	19	14		Jul 31st, 2024	Aug 20th, 2024
fin-gmf-002	10.90.26.177	19	6		Jul 31st, 2024	Jul 31st, 2024
ksr-qms-001-lss	10.72.0.30	0	0		Jul 31st, 2024	Jul 31st, 2024
hma-vis-003	10.16.240.57	0	0		Jul 31st, 2024	Jul 31st, 2024

wdm-r.wbx2.com-5

External Domain: wdm-r.wbx2.com Internal Hosts: 37 Detections: 1 Duration: 23 days Last Activity: Aug. 22, 2024, 9:39 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28		Aug 1st, 2024	Aug 9th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Aug 2nd, 2024	Aug 2nd, 2024
Proxy-New	10.222.140.19	52	28		Aug 15th, 2024	Aug 15th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Jul 30th, 2024	Aug 20th, 2024
PROXY-DR-NEW	10.222.140.20	61	19		Aug 13th, 2024	Aug 13th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Jul 30th, 2024	Aug 19th, 2024
IP-196.10.138.151	196.10.138.151	93	75		Aug 16th, 2024	Aug 16th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Jul 30th, 2024	Aug 5th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 1st, 2024	Aug 20th, 2024
PROXY-204	10.222.140.204	52	22		Aug 11th, 2024	Aug 16th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Jul 30th, 2024	Aug 22nd, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Aug 1st, 2024	Aug 22nd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Jul 30th, 2024	Aug 20th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 30th, 2024	Aug 19th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 30th, 2024	Aug 9th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 30th, 2024	Aug 9th, 2024
IP-10.90.59.13	10.90.59.13	0	0		Jul 30th, 2024	Jul 30th, 2024
IP-10.90.59.13	10.90.59.13	0	0		Jul 30th, 2024	Jul 30th, 2024
IP-10.90.40.22	10.90.40.22	34	8		Jul 30th, 2024	Jul 30th, 2024
IP-10.90.59.13	10.90.59.13	0	0		Jul 31st, 2024	Jul 31st, 2024
IP-10.90.40.22	10.90.40.22	52	9		Jul 31st, 2024	Jul 31st, 2024
IP-10.90.40.22	10.90.40.22	0	0		Jul 31st, 2024	Jul 31st, 2024
IP-10.90.59.13	10.90.59.13	0	0		Aug 1st, 2024	Aug 1st, 2024
IP-10.90.40.11	10.90.40.11	28	10		Aug 1st, 2024	Aug 1st, 2024
IP-10.90.43.29	10.90.43.29	0	0		Aug 1st, 2024	Aug 1st, 2024
IP-10.90.59.13	10.90.59.13	0	0		Aug 1st, 2024	Aug 1st, 2024
IP-10.90.43.29	10.90.43.29	0	0		Aug 2nd, 2024	Aug 2nd, 2024
IP-10.90.43.29	10.90.43.29	0	0		Aug 2nd, 2024	Aug 2nd, 2024
IP-10.90.59.13	10.90.59.13	0	0		Aug 2nd, 2024	Aug 2nd, 2024
IP-10.90.59.13	10.90.59.13	0	0		Aug 3rd, 2024	Aug 3rd, 2024

accounts.opera.com-6

External Domain: accounts.opera.com Internal Hosts: 10 Detections: 1 Duration: 21 days 14 hours Last Activity: Aug. 20, 2024, 5:27 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.148	196.10.138.148	52	21		Jul 30th, 2024	Aug 20th, 2024
IP-196.10.138.144	196.10.138.144	38	29	•	Jul 30th, 2024	Aug 20th, 2024
PROXY-204	10.222.140.204	52	22		Aug 12th, 2024	Aug 12th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 13th, 2024	Aug 20th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Jul 30th, 2024	Aug 20th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Aug 9th, 2024	Aug 12th, 2024
SHAREDVD1.centenarybank.co.ug	10.222.130.104	19	13		Jul 30th, 2024	Aug 19th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Jul 30th, 2024	Aug 20th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Jul 30th, 2024	Aug 20th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Jul 30th, 2024	Aug 19th, 2024

inetcallhome.stratus.com-27

External Domain: inetcallhome.stratus.com Internal Hosts: 4 Detections: 1 Duration: 20 days 13 hours Last Activity: Aug. 22, 2024, 6:33 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79	•	Aug 2nd, 2024	Aug 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21		Aug 2nd, 2024	Aug 22nd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-10.222.180.201	10.222.180.201	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 22nd, 2024	
IP-10.222.180.204	10.222.180.204	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 22nd, 2024	

data.tradingview.com-23

External Domain: data.tradingview.com Internal Hosts: 9 Detections: 1 Duration: 20 days Last Activity: Aug. 22, 2024, 8:41 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-196.10.138.145	196.10.138.145	80	79	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 9th, 2024	Aug 19th, 2024	
IP-196.10.138.148	196.10.138.148	52	21	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 22nd, 2024	
IP-196.10.138.149	196.10.138.149	38	24	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 6th, 2024	Aug 22nd, 2024	
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 6th, 2024	Aug 22nd, 2024	
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 9th, 2024	Aug 19th, 2024	
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 22nd, 2024	
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 6th, 2024	Aug 18th, 2024	
IP-196.10.139.146	196.10.139.146	52	34	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 6th, 2024	Aug 18th, 2024	
mrt-fin-001	10.77.0.36	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 15th, 2024	Aug 15th, 2024	

4.sophosxl.net-7

External Domain: 4.sophosxl.net Internal Hosts: 58 Detections: 1 Duration: 20 days 01 hours Last Activity: Aug. 22, 2024, 10:02 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	IN CAMPAIGN	FIRST SEEN IN CAMPAIGN	LAST SEEN
IP-196.10.138.150	196.10.138.150	52	28	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 14th, 2024	Aug 15th, 2024	
IP-196.10.138.146	196.10.138.146	38	25	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 2nd, 2024	
IP-196.10.138.148	196.10.138.148	52	21	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 22nd, 2024	
IP-196.10.138.144	196.10.138.144	38	29	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 8th, 2024	Aug 22nd, 2024	
IP-196.10.138.147	196.10.138.147	52	33	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 5th, 2024	Aug 22nd, 2024	
IP-196.10.138.149	196.10.138.149	38	24	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 5th, 2024	Aug 15th, 2024	
IP-10.90.59.12	10.90.59.12	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 2nd, 2024	
IP-10.90.43.34	10.90.43.34	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 2nd, 2024	
IP-10.90.10.204	10.90.10.204	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 2nd, 2024	Aug 2nd, 2024	
IP-10.90.59.12	10.90.59.12	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 3rd, 2024	Aug 3rd, 2024	
IP-10.90.59.12	10.90.59.12	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 5th, 2024	Aug 5th, 2024	
IP-10.90.59.11	10.90.59.11	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 5th, 2024	Aug 5th, 2024	
IP-10.90.59.13	10.90.59.13	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 5th, 2024	Aug 5th, 2024	
IP-10.90.59.11	10.90.59.11	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 5th, 2024	Aug 5th, 2024	
IP-10.90.59.12	10.90.59.12	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 6th, 2024	Aug 6th, 2024	
IP-10.90.59.11	10.90.59.11	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 6th, 2024	Aug 6th, 2024	
IP-10.90.59.12	10.90.59.12	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 7th, 2024	Aug 7th, 2024	

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-10.90.59.13	10.90.59.13	0	0		Aug 7th, 2024	Aug 7th, 2024
IP-10.90.59.11	10.90.59.11	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 7th, 2024	Aug 7th, 2024
IP-10.90.59.12	10.90.59.12	0	0		Aug 8th, 2024	Aug 8th, 2024
IP-10.90.59.13	10.90.59.13	0	0		Aug 8th, 2024	Aug 8th, 2024
IP-10.90.59.11	10.90.59.11	0	0		Aug 8th, 2024	Aug 8th, 2024
IP-10.90.59.16	10.90.59.16	0	0		Aug 8th, 2024	Aug 8th, 2024
IP-10.90.59.11	10.90.59.11	0	0		Aug 9th, 2024	Aug 9th, 2024
IP-10.90.59.12	10.90.59.12	0	0		Aug 9th, 2024	Aug 9th, 2024
IP-10.90.59.13	10.90.59.13	0	0		Aug 9th, 2024	Aug 9th, 2024
IP-10.90.59.12	10.90.59.12	0	0		Aug 10th, 2024	Aug 10th, 2024
IP-10.90.59.12	10.90.59.12	0	0		Aug 12th, 2024	Aug 12th, 2024
IP-10.90.59.11	10.90.59.11	29	28		Aug 12th, 2024	Aug 12th, 2024
IP-10.90.59.12	10.90.59.12	0	0		Aug 13th, 2024	Aug 13th, 2024

cdn-header-bidding.snack-media.com-35

External Domain: cdn-header-bidding.snack-media.com Internal Hosts: 16 Detections: 1 Duration: 20 days 06 hours Last Activity: Aug. 22, 2024, 2:49 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
Proxy-New	10.222.140.19	52	28		Aug 12th, 2024	Aug 20th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Aug 6th, 2024	Aug 21st, 2024
IP-196.10.138.148	196.10.138.148	52	21		Aug 2nd, 2024	Aug 21st, 2024
IP-196.10.138.151	196.10.138.151	93	75		Aug 12th, 2024	Aug 12th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 12th, 2024	Aug 20th, 2024
PROXY-204	10.222.140.204	52	22		Aug 12th, 2024	Aug 12th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 2nd, 2024	Aug 22nd, 2024
PROXY203-DR	10.222.140.203	52	29		Aug 19th, 2024	Aug 20th, 2024
fsproxy	10.222.203.27	19	13		Aug 17th, 2024	Aug 17th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Aug 2nd, 2024	Aug 22nd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Aug 6th, 2024	Aug 21st, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Aug 2nd, 2024	Aug 21st, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Aug 2nd, 2024	Aug 5th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Aug 2nd, 2024	Aug 5th, 2024
IP-10.90.59.15	10.90.59.15	29	28		Aug 12th, 2024	Aug 12th, 2024
naj-amc-001-lss	10.62.0.61	0	0		Aug 15th, 2024	Aug 15th, 2024

ds.kaspersky.com-3

External Domain: ds.kaspersky.com Internal Hosts: 55 Detections: 5 Duration: 23 days 19 hours Last Activity: Aug. 25, 2024, 10:39 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Aug 2nd, 2024	Aug 22nd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25		•					Aug 2nd, 2024	Aug 25th, 2024
Proxy-New	10.222.140.19	52	28							Aug 10th, 2024	Aug 10th, 2024
IP-196.10.138.145	196.10.138.145	80	79		•					Aug 4th, 2024	Aug 25th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Aug 3rd, 2024	Aug 11th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 4th, 2024	Aug 25th, 2024
IP-196.10.138.151	196.10.138.151	93	75		•					Aug 16th, 2024	Aug 20th, 2024
IP-196.10.138.144	196.10.138.144	38	29		•					Aug 6th, 2024	Aug 25th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 2nd, 2024	Aug 25th, 2024
PROXY-204	10.222.140.204	52	22							Aug 3rd, 2024	Aug 10th, 2024
IP-196.10.138.149	196.10.138.149	38	24		•					Aug 2nd, 2024	Aug 25th, 2024
crdb-omni-hq-uat-appsvr-dotnet	10.223.225.14	0	0							Aug 2nd, 2024	Aug 21st, 2024
PROXY203-DR	10.222.140.203	52	29							Aug 4th, 2024	Aug 11th, 2024
DT-EDGE	10.222.120.18	0	0							Aug 2nd, 2024	Aug 15th, 2024
KAVNEW-HQ	10.222.140.43	22	17							Aug 2nd, 2024	Aug 25th, 2024
SOLARWINDSAPP	10.222.110.210	39	70							Aug 2nd, 2024	Aug 25th, 2024
risk-jump.centenarybank.co.ug	10.222.206.31	0	0							Aug 2nd, 2024	Aug 25th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Aug 3rd, 2024	Aug 17th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 4th, 2024	Aug 19th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Aug 2nd, 2024	Aug 23rd, 2024
ADS_QMS-v2-	10.222.110.202	0	0							Aug 2nd, 2024	Aug 25th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Aug 2nd, 2024	Aug 25th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Aug 3rd, 2024	Aug 25th, 2024
REUTERZ-PC.centenarybank.co.ug	10.90.26.150	0	0							Aug 2nd, 2024	Aug 22nd, 2024
FMKT-OFF-011.centenarybank.co...	10.90.26.237	22	15							Aug 2nd, 2024	Aug 25th, 2024
btd-isc-099	10.90.20.27	28	11							Aug 2nd, 2024	Aug 24th, 2024
BTD-ISC-034	10.90.20.21	19	6							Aug 2nd, 2024	Aug 24th, 2024
BTD-ISC-033.centenarybank.co....	10.90.20.29	100	71							Aug 2nd, 2024	Aug 24th, 2024
bloomberg-01	10.90.26.55	0	0							Aug 5th, 2024	Aug 23rd, 2024
EBA-OFF-179.centenarybank.co....	10.90.51.250	0	0							Aug 24th, 2024	Aug 25th, 2024

archive.ubuntu.com-194

External Domain: archive.ubuntu.com Internal Hosts: 60 Detections: 1 Duration: 21 days 10 hours Last Activity: Aug. 23, 2024, 1:46 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Aug 4th, 2024	Aug 23rd, 2024
IP-196.10.138.146	196.10.138.146	38	25							Aug 2nd, 2024	Aug 22nd, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 2nd, 2024	Aug 23rd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 2nd, 2024	Aug 23rd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.151	196.10.138.151	93	75		Aug 2nd, 2024	Aug 23rd, 2024
IP-196.10.138.144	196.10.138.144	38	29		Aug 2nd, 2024	Aug 23rd, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 2nd, 2024	Aug 23rd, 2024
AGENTBANKING-GW	10.224.30.183	38	31		Aug 2nd, 2024	Aug 23rd, 2024
dev.vendorappraisal.centenary...	10.222.225.64	0	0		Aug 2nd, 2024	Aug 23rd, 2024
tpsuat.centenarybank.co.ug	10.223.225.65	0	0		Aug 2nd, 2024	Aug 23rd, 2024
MIS-ARCHIVE-SVR	10.222.130.60	0	0		Aug 2nd, 2024	Aug 23rd, 2024
SCCM-HQ	10.222.140.111	30	73		Aug 12th, 2024	Aug 12th, 2024
ESB-PRD	10.224.52.82	19	13		Aug 2nd, 2024	Aug 23rd, 2024
SMS-GATEWAY-SVR	10.222.130.36	0	0		Aug 2nd, 2024	Aug 23rd, 2024
SWITCH-CBS-AP	10.224.225.66	0	0		Aug 2nd, 2024	Aug 22nd, 2024
SMS-GATEWAY-SVR-TEST	10.222.130.71	0	0		Aug 2nd, 2024	Aug 22nd, 2024
SMS-OMNI-GATEWAY	10.222.130.47	0	0		Aug 2nd, 2024	Aug 23rd, 2024
IP-10.222.130.16	10.222.130.16	0	0		Aug 2nd, 2024	Aug 23rd, 2024
WEB-REVAMP	10.222.218.20	0	0		Aug 2nd, 2024	Aug 23rd, 2024
APM-GATEWAY2	10.222.206.15	0	0		Aug 2nd, 2024	Aug 14th, 2024
Cente-Website-New	10.222.218.3	0	0		Aug 2nd, 2024	Aug 22nd, 2024
IP-10.222.110.35	10.222.110.35	0	0		Aug 3rd, 2024	Aug 23rd, 2024
DESKTOP CENTRAL-HQ	10.222.140.140	28	27	•	Aug 2nd, 2024	Aug 23rd, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Aug 7th, 2024	Aug 7th, 2024
CBCRMPRPAPDB01.centenarybank....	10.222.130.69	0	0		Aug 2nd, 2024	Aug 23rd, 2024
esb-test-svr	10.223.50.68	0	0		Aug 2nd, 2024	Aug 23rd, 2024
new-esb-db-test	10.223.52.140	0	0		Aug 2nd, 2024	Aug 23rd, 2024
IP-10.222.206.35	10.222.206.35	0	0		Aug 2nd, 2024	Aug 23rd, 2024
IP-10.222.130.145	10.222.130.145	0	0		Aug 2nd, 2024	Aug 3rd, 2024
IP-10.222.130.145	10.222.130.145	0	0		Aug 4th, 2024	Aug 5th, 2024

time.samsungcloudsolution.com-41

External Domain: time.samsungcloudsolution.com Internal Hosts: 21 Detections: 1 Duration: 22 days 03 hours Last Activity: Aug. 25, 2024, 10:33 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28	•	Aug 12th, 2024	Aug 23rd, 2024
IP-196.10.138.146	196.10.138.146	38	25		Aug 6th, 2024	Aug 6th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Aug 3rd, 2024	Aug 19th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Aug 12th, 2024	Aug 23rd, 2024
IP-196.10.138.151	196.10.138.151	93	75		Aug 5th, 2024	Aug 25th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Aug 9th, 2024	Aug 25th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 5th, 2024	Aug 19th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.149	196.10.138.149	38	24							Aug 12th, 2024	Aug 12th, 2024
IP-10.90.34.11	10.90.34.11	0	0							Aug 5th, 2024	Aug 5th, 2024
IP-10.90.34.11	10.90.34.11	0	0							Aug 6th, 2024	Aug 6th, 2024
IP-10.90.34.11	10.90.34.11	0	0							Aug 7th, 2024	Aug 7th, 2024
IP-10.90.34.11	10.90.34.11	0	0							Aug 8th, 2024	Aug 8th, 2024
IP-10.90.34.11	10.90.34.11	0	0							Aug 9th, 2024	Aug 9th, 2024
IP-10.90.34.11	10.90.34.11	0	0							Aug 12th, 2024	Aug 12th, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 12th, 2024	Aug 12th, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 13th, 2024	Aug 13th, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 14th, 2024	Aug 15th, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 16th, 2024	Aug 16th, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 19th, 2024	Aug 21st, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 22nd, 2024	Aug 22nd, 2024
IP-10.90.34.14	10.90.34.14	0	0							Aug 23rd, 2024	Aug 23rd, 2024

img-c.udemycdn.com-5

External Domain: img-c.udemycdn.com Internal Hosts: 24 Detections: 1 Duration: 19 days 23 hours Last Activity: Aug. 23, 2024, 10:53 a.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28							Aug 13th, 2024	Aug 13th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 5th, 2024	Aug 22nd, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Aug 6th, 2024	Aug 20th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 3rd, 2024	Aug 23rd, 2024
IP-196.10.138.151	196.10.138.151	93	75							Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Aug 19th, 2024	Aug 21st, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 8th, 2024	Aug 19th, 2024
PROXY-204	10.222.140.204	52	22							Aug 5th, 2024	Aug 23rd, 2024
IP-196.10.138.149	196.10.138.149	38	24							Aug 3rd, 2024	Aug 23rd, 2024
PROXY203-DR	10.222.140.203	52	29							Aug 5th, 2024	Aug 20th, 2024
fsproxy	10.222.203.27	19	13							Aug 8th, 2024	Aug 19th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Aug 3rd, 2024	Aug 23rd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 5th, 2024	Aug 22nd, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Aug 3rd, 2024	Aug 23rd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Aug 3rd, 2024	Aug 5th, 2024
IP-196.10.139.146	196.10.139.146	52	34							Aug 3rd, 2024	Aug 5th, 2024
IP-10.170.35.173	10.170.35.173	0	0							Aug 5th, 2024	Aug 5th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-10.170.35.189	10.170.35.189	0	0		Aug 7th, 2024	Aug 7th, 2024
IP-10.170.35.172	10.170.35.172	0	0	BOTNET C&C RECON LATERAL EXFIL CUSTOM	Aug 14th, 2024	Aug 14th, 2024
adj-act-001-lss	10.85.240.20	19	9	•	Aug 16th, 2024	Aug 16th, 2024
IP-10.170.35.248	10.170.35.248	19	3		Aug 19th, 2024	Aug 19th, 2024
btd-bitab-020	10.90.19.85	0	0		Aug 20th, 2024	Aug 20th, 2024
IP-10.90.59.16	10.90.59.16	0	0		Aug 21st, 2024	Aug 21st, 2024
btd-sup-501-lss	10.90.33.74	29	29		Aug 23rd, 2024	Aug 23rd, 2024

www.eafinder.com-4

External Domain: www.eafinder.com Internal Hosts: 7 Detections: 1 Duration: 13 days 02 hours Last Activity: Aug. 16, 2024, 3:47 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.148	196.10.138.148	52	21		Aug 14th, 2024	Aug 16th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 8th, 2024	Aug 15th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Aug 8th, 2024	Aug 15th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Aug 14th, 2024	Aug 16th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Aug 3rd, 2024	Aug 3rd, 2024
IP-196.10.139.146	196.10.139.146	52	34		Aug 3rd, 2024	Aug 3rd, 2024
ops-off-099-lss	10.90.240.227	19	2	•	Aug 16th, 2024	Aug 16th, 2024

www.scribd.com-3

External Domain: www.scribd.com Internal Hosts: 18 Detections: 1 Duration: 19 days 23 hours Last Activity: Aug. 23, 2024, 2:38 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
Proxy-New	10.222.140.19	52	28		Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Aug 5th, 2024	Aug 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21		Aug 4th, 2024	Aug 23rd, 2024
IP-196.10.138.151	196.10.138.151	93	75		Aug 19th, 2024	Aug 19th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 3rd, 2024	Aug 20th, 2024
PROXY-204	10.222.140.204	52	22		Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 8th, 2024	Aug 19th, 2024
PROXY203-DR	10.222.140.203	52	29		Aug 20th, 2024	Aug 20th, 2024
fsproxy	10.222.203.27	19	13		Aug 3rd, 2024	Aug 13th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Aug 8th, 2024	Aug 19th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Aug 5th, 2024	Aug 22nd, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Aug 4th, 2024	Aug 23rd, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Aug 20th, 2024	Aug 23rd, 2024
IP-196.10.139.146	196.10.139.146	52	34		Aug 20th, 2024	Aug 23rd, 2024
kcc-off-011	10.90.50.196	0	0		Aug 14th, 2024	Aug 14th, 2024
btd-sup-030-lss	10.90.24.20	0	0	•	Aug 16th, 2024	Aug 16th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-10.90.59.15	10.90.59.15	0	0							Aug 19th, 2024	Aug 19th, 2024
IP-10.90.59.12	10.90.59.12	0	0							Aug 19th, 2024	Aug 19th, 2024

172.21.56.2-164

External Domain: 172.21.56.2 Internal Hosts: 2 Detections: 1 Duration: 19 days 18 hours Last Activity: Aug. 25, 2024, 10 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-10.222.1.13	10.222.1.13	35	36		•					Aug 6th, 2024	Aug 25th, 2024
BTD-ITN-002.centenarybank.co....	10.90.34.54	19	6							Aug 8th, 2024	Aug 8th, 2024

perr.l-err.biz-91

External Domain: perr.l-err.biz Internal Hosts: 3 Detections: 2 Duration: 6 days 07 hours Last Activity: Aug. 25, 2024, 3:01 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-196.10.138.145	196.10.138.145	80	79		•					Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.147	196.10.138.147	52	33		•					Aug 19th, 2024	Aug 25th, 2024
btd-csa-011-lss	10.90.21.27	19	2							Aug 19th, 2024	Aug 25th, 2024

perr.l-agent.me-7

External Domain: perr.l-agent.me Internal Hosts: 3 Detections: 2 Duration: 6 days 07 hours Last Activity: Aug. 25, 2024, 3 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-196.10.138.145	196.10.138.145	80	79		•					Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.147	196.10.138.147	52	33		•					Aug 19th, 2024	Aug 25th, 2024
btd-csa-011-lss	10.90.21.27	19	2							Aug 19th, 2024	Aug 25th, 2024

shop.app-2

External Domain: shop.app Internal Hosts: 18 Detections: 1 Duration: 18 days 05 hours Last Activity: Aug. 25, 2024, 1:46 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM		
IP-196.10.138.150	196.10.138.150	52	28							Aug 21st, 2024	Aug 22nd, 2024
IP-196.10.138.146	196.10.138.146	38	25							Aug 16th, 2024	Aug 21st, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 13th, 2024	Aug 24th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 7th, 2024	Aug 25th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 15th, 2024	Aug 22nd, 2024
IP-196.10.138.149	196.10.138.149	38	24							Aug 8th, 2024	Aug 24th, 2024

fsproxy	10.222.203.27	19	13							Aug 15th, 2024	Aug 22nd, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28		Aug 8th, 2024	Aug 24th, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40		Aug 13th, 2024	Aug 24th, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33		Aug 7th, 2024	Aug 25th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25		Aug 7th, 2024	Aug 24th, 2024
IP-196.10.139.146	196.10.139.146	52	34		Aug 7th, 2024	Aug 24th, 2024
grp-stg-001	10.170.46.51	39	70		Aug 15th, 2024	Aug 15th, 2024
IP-10.170.35.101	10.170.35.101	29	5		Aug 19th, 2024	Aug 19th, 2024
aud-mgr-004-lss	10.90.40.26	29	12	•	Aug 20th, 2024	Aug 20th, 2024
IP-10.170.35.145	10.170.35.145	0	0		Aug 20th, 2024	Aug 20th, 2024
IP-10.170.46.46	10.170.46.46	0	0		Aug 21st, 2024	Aug 21st, 2024
IP-10.170.35.145	10.170.35.145	29	18		Aug 21st, 2024	Aug 21st, 2024

clientsdk.bright-sdk.com-2

External Domain: clientsdk.bright-sdk.com Internal Hosts: 3 Detections: 2 Duration: 6 days 05 hours Last Activity: Aug. 25, 2024, 3:35 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79	•	Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.147	196.10.138.147	52	33	•	Aug 23rd, 2024	Aug 23rd, 2024
btd-csa-011-lss	10.90.21.27	19	2		Aug 19th, 2024	Aug 25th, 2024

quay.io-129

External Domain: quay.io Internal Hosts: 17 Detections: 1 Duration: 18 days 18 hours Last Activity: Aug. 25, 2024, 9:47 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN	LAST SEEN
				BOTNET C&C RECON LATERAL EXFIL CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28		Aug 7th, 2024	Aug 25th, 2024
IP-196.10.138.146	196.10.138.146	38	25		Aug 7th, 2024	Aug 18th, 2024
IP-196.10.138.145	196.10.138.145	80	79		Aug 18th, 2024	Aug 25th, 2024
IP-196.10.138.148	196.10.138.148	52	21		Aug 7th, 2024	Aug 25th, 2024
IP-196.10.138.144	196.10.138.144	38	29		Aug 18th, 2024	Aug 18th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 9th, 2024	Aug 18th, 2024
masterprodhq02	10.224.225.25	0	0		Aug 18th, 2024	Aug 25th, 2024
masterproddr01.crdbproddrcls....	10.224.225.124	0	0		Aug 7th, 2024	Aug 20th, 2024
masterproddr03.crdbproddrcls....	10.224.225.126	29	35	•	Aug 20th, 2024	Aug 25th, 2024
wrkprodhq01	10.224.225.27	0	0		Aug 9th, 2024	Aug 9th, 2024
wrkprodhq02	10.224.225.28	0	0		Aug 18th, 2024	Aug 22nd, 2024
masterprodhq01	10.224.225.24	0	0		Aug 18th, 2024	Aug 18th, 2024
masterprodhq03	10.224.225.26	0	0		Aug 7th, 2024	Aug 18th, 2024
OPENSHIFT-DEV-VM	10.222.225.22	0	0		Aug 7th, 2024	Aug 25th, 2024
OPENSHIFT-UAT-VM	10.223.225.20	0	0		Aug 7th, 2024	Aug 25th, 2024
wrkprodhq05.crdbprodhqcls.cen...	10.224.225.36	0	0		Aug 7th, 2024	Aug 7th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-10.224.225.27	10.224.225.27	0	0							Aug 18th, 2024	Aug 18th, 2024

data.metaxplay.com-53

External Domain: data.metaxplay.com Internal Hosts: 15 Detections: 1 Duration: 17 days 07 hours Last Activity: Aug. 25, 2024, 2:43 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.150	196.10.138.150	52	28							Aug 8th, 2024	Aug 12th, 2024
IP-196.10.138.146	196.10.138.146	38	25							Aug 8th, 2024	Aug 12th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 13th, 2024	Aug 22nd, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 13th, 2024	Aug 25th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Aug 8th, 2024	Aug 12th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Aug 13th, 2024	Aug 24th, 2024
IP-196.10.138.147	196.10.138.147	52	33		•					Aug 13th, 2024	Aug 23rd, 2024
IP-196.10.138.149	196.10.138.149	38	24							Aug 8th, 2024	Aug 12th, 2024
IP-10.90.17.11	10.90.17.11	0	0							Aug 17th, 2024	Aug 17th, 2024
IP-10.90.17.11	10.90.17.11	0	0							Aug 19th, 2024	Aug 19th, 2024
IP-10.90.17.11	10.90.17.11	0	0							Aug 20th, 2024	Aug 20th, 2024
IP-10.90.17.11	10.90.17.11	29	16							Aug 21st, 2024	Aug 21st, 2024
IP-10.90.17.11	10.90.17.11	0	0							Aug 22nd, 2024	Aug 22nd, 2024
IP-10.90.17.11	10.90.17.11	0	0							Aug 23rd, 2024	Aug 23rd, 2024
IP-10.90.17.11	10.90.17.11	0	0							Aug 24th, 2024	Aug 24th, 2024

update2.vectranetworks.com-267

External Domain: update2.vectranetworks.com Internal Hosts: 2 Detections: 1 Duration: 17 days 19 hours Last Activity: Aug. 25, 2024, 10 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25							Aug 8th, 2024	Aug 25th, 2024
IP-10.222.199.34	10.222.199.34	38	35		•					Aug 8th, 2024	Aug 25th, 2024

perr.bright-sdk.com-21

External Domain: perr.bright-sdk.com Internal Hosts: 3 Detections: 1 Duration: 6 days 07 hours Last Activity: Aug. 25, 2024, 3 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.145	196.10.138.145	80	79							Aug 20th, 2024	Aug 20th, 2024
IP-196.10.138.147	196.10.138.147	52	33		•					Aug 19th, 2024	Aug 25th, 2024
btd-csa-011-lss	10.90.21.27	19	2							Aug 19th, 2024	Aug 25th, 2024

www.netflix.com-72

External Domain: www.netflix.com Internal Hosts: 20 Detections: 1 Duration: 15 days 05 hours Last Activity: Aug. 25, 2024, 4 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.146	196.10.138.146	38	25							Aug 10th, 2024	Aug 12th, 2024
Proxy-New	10.222.140.19	52	28							Aug 13th, 2024	Aug 13th, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 12th, 2024	Aug 21st, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Aug 14th, 2024	Aug 14th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 12th, 2024	Aug 24th, 2024
IP-196.10.138.151	196.10.138.151	93	75							Aug 10th, 2024	Aug 12th, 2024
IP-196.10.138.144	196.10.138.144	38	29							Aug 13th, 2024	Aug 14th, 2024
IP-196.10.138.147	196.10.138.147	52	33							Aug 13th, 2024	Aug 15th, 2024
PROXY-204	10.222.140.204	52	22							Aug 14th, 2024	Aug 14th, 2024
IP-196.10.138.149	196.10.138.149	38	24							Aug 10th, 2024	Aug 23rd, 2024
PROXY203-DR	10.222.140.203	52	29							Aug 13th, 2024	Aug 13th, 2024
fsproxy	10.222.203.27	19	13							Aug 14th, 2024	Aug 15th, 2024
fsproxy-05-wcg.centenarybank....	10.222.203.29	52	28							Aug 12th, 2024	Aug 23rd, 2024
fsproxy-02-wcg.centenarybank....	10.222.203.25	38	40							Aug 12th, 2024	Aug 21st, 2024
fsproxy-01-wcg.centenarybank....	10.222.203.28	52	33							Aug 12th, 2024	Aug 24th, 2024
FSProxy-03-wcg.centenarybank....	10.222.203.19	38	25							Aug 20th, 2024	Aug 22nd, 2024
IP-196.10.139.146	196.10.139.146	52	34							Aug 20th, 2024	Aug 22nd, 2024
fmk-off-013-lss	10.90.240.135	19	11							Aug 19th, 2024	Aug 19th, 2024
aud-mgr-020-lss	10.90.241.45	29	29		•					Aug 23rd, 2024	Aug 23rd, 2024
IP-10.90.59.12	10.90.59.12	0	0							Aug 25th, 2024	Aug 25th, 2024

nsstats.nimblestorage.com-73

External Domain: nsstats.nimblestorage.com Internal Hosts: 2 Detections: 1 Duration: 13 days 17 hours Last Activity: Aug. 25, 2024, 8:29 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
IP-196.10.138.151	196.10.138.151	93	75		•					Aug 12th, 2024	Aug 25th, 2024
IP-10.222.71.87	10.222.71.87	0	0							Aug 12th, 2024	Aug 25th, 2024

52.114.214.40

External Domain: 52.114.214.40 Internal Hosts: 19 Detections: 1 Duration: 13 days 06 hours Last Activity: Aug. 25, 2024, 6 p.m.

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES						FIRST SEEN	LAST SEEN
				BOTNET	C&C	RECON	LATERAL	EXFIL	CUSTOM	IN CAMPAIGN	IN CAMPAIGN
Proxy-New	10.222.140.19	52	28							Aug 12th, 2024	Aug 21st, 2024
IP-196.10.138.145	196.10.138.145	80	79							Aug 14th, 2024	Aug 25th, 2024
PROXY-DR-NEW	10.222.140.20	61	19							Aug 12th, 2024	Aug 16th, 2024
IP-196.10.138.148	196.10.138.148	52	21							Aug 12th, 2024	Aug 19th, 2024

HOSTNAME	LAST IP	THREAT	CERTAINTY	DETECTION CATEGORIES	FIRST SEEN IN CAMPAIGN	LAST SEEN IN CAMPAIGN
IP-196.10.138.151	196.10.138.151	93	75		Aug 16th, 2024	Aug 19th, 2024
IP-196.10.138.147	196.10.138.147	52	33		Aug 12th, 2024	Aug 23rd, 2024
PROXY-204	10.222.140.204	52	22		Aug 12th, 2024	Aug 19th, 2024
IP-196.10.138.149	196.10.138.149	38	24		Aug 23rd, 2024	Aug 23rd, 2024
PROXY203-DR	10.222.140.203	52	29		Aug 12th, 2024	Aug 20th, 2024
kyj-tel-001-lse	10.22.0.121	0	0		Aug 14th, 2024	Aug 14th, 2024
FIN-OFF-012-LSS.centenarybank...	10.90.240.147	19	9		Aug 16th, 2024	Aug 16th, 2024
IP-10.90.55.23	10.90.55.23	0	0		Aug 16th, 2024	Aug 16th, 2024
rmf-gm-070-lss	10.90.240.137	29	38		Aug 19th, 2024	Aug 19th, 2024
rsk-mgr-030-lss	10.90.53.47	19	9		Aug 19th, 2024	Aug 19th, 2024
cbo-sup-237-lss	10.90.50.141	0	0		Aug 19th, 2024	Aug 19th, 2024
rtl-sup-007-lss	10.70.0.32	0	0		Aug 21st, 2024	Aug 21st, 2024
btd-dba-004-lse	10.90.24.13	38	33		Aug 23rd, 2024	Aug 23rd, 2024
ccm-off-220-ls	10.90.47.69	0	0		Aug 23rd, 2024	Aug 23rd, 2024
btd-csd-200	10.90.240.184	38	39	•	Aug 25th, 2024	Aug 25th, 2024

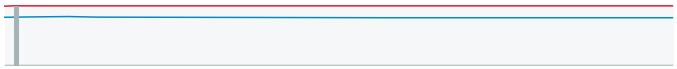
Showing 30 of 92 total campaigns. This list was cut off because there were too many items.

3 HOSTS, 0 KEY ASSETS WITH DETECTIONS, 0 TARGETING KEY ASSET

nac-buk-01.centenarybank.co.ug

Last Seen IP: 10.222.204.11

DETECTIONS	THREAT	CERTAINTY	LAST ACTIVITY
Exfil Cognito - VSA - Unencrypted FTP and Telnet	90	90	Aug 25th, 2024
Lateral Brute-Force	30	57	Aug 25th, 2024



Peak Certainty / Threat: 81 / 100 on Aug 25th, 2024

End Certainty / Threat: 80 / 100 on Aug 25th, 2024

IP-196.10.138.151

Last Seen IP: 196.10.138.151

DETECTIONS	THREAT	CERTAINTY	LAST ACTIVITY
Recon Cognito - PUP - HTTP - Potentially Harmful File Download	90	90	Aug 25th, 2024
C&C Hidden HTTPS Tunnel	50	72	Aug 25th, 2024

Peak Certainty / Threat: 71 / 93 on Aug 24th, 2024

End Certainty / Threat: 70 / 93 on Aug 25th, 2024

IP-196.10.138.145

Last Seen IP: 196.10.138.145

DETECTIONS	THREAT	CERTAINTY	LAST ACTIVITY
Recon Cognito - PUP - HTTP - Potentially Harmful File Download	90	90	Aug 25th, 2024

Peak Certainty / Threat: 81 / 80 on Aug 24th, 2024

End Certainty / Threat: 80 / 80 on Aug 25th, 2024

4 DETECTIONS, 1 TARGETING KEY ASSET

C&C Hidden HTTPS Tunnel

IP-196.10.138.150

THREAT	CERTAINTY	LAST ACTIVITY
70	80	Aug. 25, 2024, 11:47 p.m.

Sent & Received

Aug 25th, 2024 Aug 26th, 2024

Lateral Automated Replication

INFRA-EXMBX4-HQ

Targeting Key Assets: AD-10 , AD-199

THREAT	CERTAINTY	LAST ACTIVITY
62	72	Aug. 25, 2024, 11:49 a.m.

Sent & Received

Aug 25th, 2024 Aug 26th, 2024

Recon Port Sweep

KAV-43

THREAT	CERTAINTY	LAST ACTIVITY
60	80	Aug. 25, 2024, 11:49 p.m.

Scans

Aug 25th, 2024 Aug 26th, 2024

IP-10.224.11.80

THREAT	CERTAINTY	LAST ACTIVITY
60	80	Aug. 25, 2024, 9:01 p.m.

Scans

Aug 25th, 2024 Aug 26th, 2024

KEY ASSETS

No Key Assets with Detections

FILTER CRITERIA FOR HOSTS

Threat > 50
Certainty > 50
Host type: All
Source: All

FILTER CRITERIA FOR DETECTIONS

Threat > 50
Certainty > 50
Detection types: 104 types
Custom models: 0 models