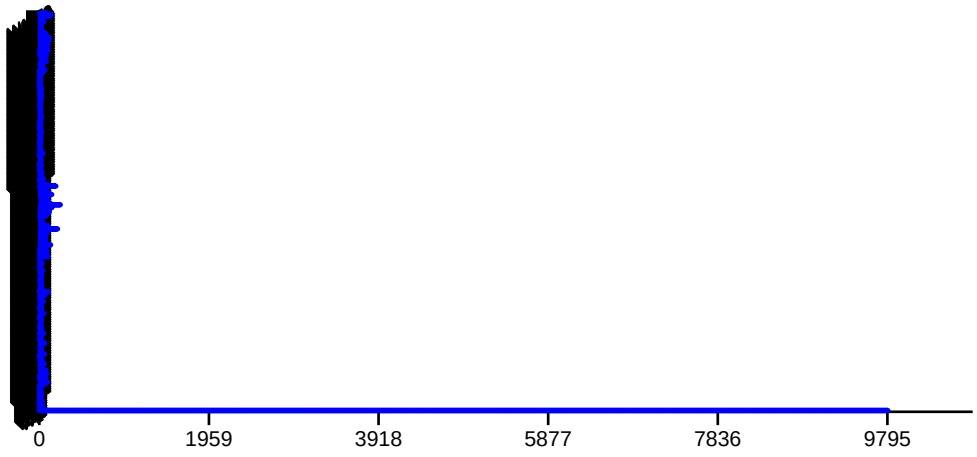
Z-Shark Network Analysis Report

1. Executive Summary

Metric	Value
File Analyzed	botnet-capture-20110810-neris
Analysis Start Time	2011-08-10 05:01:40
Analysis End Time	2011-08-10 09:49:33
Total Duration	17272.99 seconds
Total Packets	323,154
Total Bytes	50.64 MB
Incidents Detected	157

2. Packet Rate Over Time (PPS)



3. Network Flow Statistics

Top 5 Source IPs

Source IP	Packets	Bytes
147.32.84.165	238,622	28151.13 KB
213.246.53.125	17,566	1082.70 KB
184.154.132.106	15,594	980.04 KB

212.117.171.138	7,431	2697.71 KB
147.32.80.9	7,421	1035.00 KB

Top 5 Destination Ports

Dest Port	Packets	Bytes
53	58,428	4179.71 KB
25	50,794	3075.42 KB
5296	35,018	2051.86 KB
9541	31,090	1821.69 KB
80	17,710	2143.64 KB

4. Detected Incidents

Time	Severity	Label	Model	Justification
05:06:21	**HIGH**	High Volume Anomaly (DDoS Suspect)	DDoSDetector	PPS Z-score 1472.09 exceeds threshold. Spike: 9799.8 PPS (Avg: 15.4)
05:06:43	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'w.nucleardiscover.com' (Label: nucleardiscover) has high entropy (3.51).
08:59:20	**MEDIUM**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 147.32.84.165 accessed 16 unique ports over time.
05:15:19	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 74.222.3.26 accessed 10 unique ports over time.
07:23:49	**LOW**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 212.117.171.138 accessed 12 unique ports over time.
09:15:03	**LOW**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 174.133.57.141 accessed 11 unique ports over time.
05:22:44	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 222.88.205.195 accessed 10 unique ports over time.
05:25:16	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 31.192.109.167 accessed 10 unique ports over time.
09:16:14	**LOW**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 173.192.170.88 accessed 11 unique ports over time.
05:32:38	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 173.236.81.226 accessed 10 unique ports over time.
05:32:38	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 69.175.10.98 accessed 10 unique ports over time.

Z-Shark Network Analysis Report

05:44:56	**HIGH**	Source IP Entropy Collapse	DDoSDetector	Entropy dropped to 0.56 (Normal: 1.26). Possible flood.
05:45:38	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 67.214.158.5 accessed 10 unique ports over time.
05:45:38	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 50.22.198.84 accessed 10 unique ports over time.
07:43:09	**HIGH**	C2 Beaconing Suspect (FFT)	BeaconingDetector	Periodic signal in 147.32.84.165-213.246.53.125:2343-5296:6. Peak: 0.599
06:29:05	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'metalproduct-s.ru' (Label: metalproduct-s) has high entropy (3.66).
06:29:05	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'megevanie-kostroma.ru' (Label: megevanie-kostroma) has high entropy (3.57).
06:29:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns2.dynamicnetworkservices.net' (Label: dynamicnetworkservices) has high entropy (3.79).
06:31:19	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'kvartirny-wopros.ru' (Label: kvartirny-wopros) has high entropy (3.58).
06:31:19	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'kurortgelendzhik.ru' (Label: kurortgelendzhik) has high entropy (3.62).
06:31:19	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'kupi-nedvijimost.ru' (Label: kupi-nedvijimost) has high entropy (3.70).
06:31:19	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'kubanperevozki.ru' (Label: kubanperevozki) has high entropy (3.52).
06:31:19	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns2.unitedplatform.com' (Label: unitedplatform) has high entropy (3.66).
06:50:26	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns2.friendhosting-1-1.biz' (Label: friendhosting-1-1) has high entropy (3.62).
06:51:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'bizneskvadrat.ru' (Label: bizneskvadrat) has high entropy (3.55).
06:53:29	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'birchwoodcasey.ru' (Label: birchwoodcasey) has high entropy (3.52).
06:53:29	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'axfordstanley.ru' (Label: axfordstanley) has high entropy (3.55).
06:56:11	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'loveplanet-znakomstva.ru' (Label: loveplanet-znakomstva) has high entropy (3.59).
06:56:11	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ccd-s5.capitalcitydevelopments.co.uk' (Label: capitalcitydevelopments) has high entropy (3.68).
06:57:12	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'luchshie-oteli-moskvy.ru' (Label: luchshie-oteli-moskvy) has high entropy (3.73).

Z-Shark Network Analysis Report

06:57:12	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'lymanproducts.ru' (Label: lymanproducts) has high entropy (3.70).
06:58:13	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'marykay-lipetsk.ru' (Label: marykay-lipetsk) has high entropy (3.51).
06:59:14	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ifdk-insurance.ru' (Label: ifdk-insurance) has high entropy (3.52).
07:00:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'promtech-ufa.ru' (Label: promtech-ufa) has high entropy (3.58).
07:00:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'prominvestuk.ru' (Label: prominvestuk) has high entropy (3.58).
07:00:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'robert-maksimov.ru' (Label: robert-maksimov) has high entropy (3.51).
07:00:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'moscowlindyexchange.ru' (Label: moscowlindyexchange) has high entropy (3.83).
07:01:16	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'skadi-telecom.ru' (Label: skadi-telecom) has high entropy (3.55).
07:01:26	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'klimov-sergey.ru' (Label: klimov-sergey) has high entropy (3.55).
07:01:26	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'letushov-kalachanov.ru' (Label: letushov-kalachanov) has high entropy (3.58).
09:33:28	**HIGH**	C2 Beaconing Suspect (FFT)	BeaconingDetector	Periodic signal in 147.32.80.9-147.32.84.165:53-2077:17. Peak: 0.523
07:03:17	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'vipiska-iz-egrul.ru' (Label: vipiska-iz-egrul) has high entropy (3.58).
07:03:27	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'radiocomplekt.ru' (Label: radiocomplekt) has high entropy (3.55).
07:03:27	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'radiodetali-nsk.ru' (Label: radiodetali-nsk) has high entropy (3.51).
07:04:17	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'world-of-pirates.ru' (Label: world-of-pirates) has high entropy (3.62).
07:04:17	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'world-company.ru' (Label: world-company) has high entropy (3.55).
07:04:17	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'woodmaster-nsk.ru' (Label: woodmaster-nsk) has high entropy (3.52).
07:04:17	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'womanwrestling.ru' (Label: womanwrestling) has high entropy (3.52).
07:04:27	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'lampy-svetodiodnye.ru' (Label: lampy-svetodiodnye) has high entropy (3.73).
07:04:27	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'russian-hockey.ru' (Label: russian-hockey) has high entropy (3.66).

Z-Shark Network Analysis Report

07:04:27	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'kingcoal-group.ru' (Label: kingcoal-group) has high entropy (3.52).
09:29:46	**HIGH**	C2 Beaconing Suspect (FFT)	BeaconingDetector	Periodic signal in 147.32.80.9-147.32.84.165:53-2079:17. Peak: 1.321
07:05:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'lampschandelierslighting.ru' (Label: lampschandelierslighting) has high entropy (3.69).
07:05:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'stavropolmagazin.ru' (Label: stavropolmagazin) has high entropy (3.58).
07:06:29	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'kamenniyostrov.ru' (Label: kamenniyostrov) has high entropy (3.52).
07:07:30	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'purchase-lenovo.ru' (Label: purchase-lenovo) has high entropy (3.64).
07:07:30	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'pulse-fashion.ru' (Label: pulse-fashion) has high entropy (3.55).
07:08:31	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'voronezh-market.ru' (Label: voronezh-market) has high entropy (3.51).
07:08:31	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'vokrugsveta-95.ru' (Label: vokrugsveta-95) has high entropy (3.66).
07:08:31	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'yellowbrickroad.ru' (Label: yellowbrickroad) has high entropy (3.51).
07:09:32	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'zdravkomplekt.ru' (Label: zdravkomplekt) has high entropy (3.55).
07:10:33	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'gymnasium1306.ru' (Label: gymnasium1306) has high entropy (3.55).
07:10:33	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'guide-paris-france.ru' (Label: guide-paris-france) has high entropy (3.61).
07:10:33	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'gruzotaksi24.ru' (Label: gruzotaksi24) has high entropy (3.58).
07:11:33	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns135.webhostingworld.net' (Label: webhostingworld) has high entropy (3.64).
07:12:33	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'wellness-hotelhungary.ru' (Label: wellness-hotelhungary) has high entropy (3.65).
07:13:34	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'e-shopfixtures.ru' (Label: e-shopfixtures) has high entropy (3.52).
07:14:35	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favorit-opalubka.ru' (Label: favorit-opalubka) has high entropy (3.58).
07:14:35	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favorit-product.ru' (Label: favorit-product) has high entropy (3.51).
07:14:35	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favorit-wedding.ru' (Label: favorit-wedding) has high entropy (3.64).

Z-Shark Network Analysis Report

07:14:35	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favorite-spb.ru' (Label: favorite-spb) has high entropy (3.58).
07:14:35	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favoritjob2010.ru' (Label: favoritjob2010) has high entropy (3.52).
07:14:35	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favourite-games.ru' (Label: favourite-games) has high entropy (3.64).
07:14:35	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favouritemp3.ru' (Label: favouritemp3) has high entropy (3.58).
07:14:35	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'favouritetechno.ru' (Label: favouritetechno) has high entropy (3.51).
07:14:35	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'fc-dinamo-barnaul.ru' (Label: fc-dinamo-barnaul) has high entropy (3.57).
07:15:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'chlebokombinat1.ru' (Label: chlebokombinat1) has high entropy (3.64).
07:15:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'farmprodvizhenie.ru' (Label: farmprodvizhenie) has high entropy (3.62).
07:15:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'videotrainclub.ru' (Label: videotrainclub) has high entropy (3.66).
07:16:36	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'auto-chelyabinsk.ru' (Label: auto-chelyabinsk) has high entropy (3.88).
07:16:36	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'authors-community.ru' (Label: authors-community) has high entropy (3.62).
07:16:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'votkinsk-liceum.ru' (Label: votkinsk-liceum) has high entropy (3.64).
07:16:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'pogoda-novosibirsk.ru' (Label: pogoda-novosibirsk) has high entropy (3.50).
07:16:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns2.exclusivehosting.net' (Label: exclusivehosting) has high entropy (3.62).
07:17:36	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'bronirovanie-gostinicy-moskva.ru' (Label: bronirovanie-gostinicy-moskva) has high entropy (3.80).
07:17:36	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'vip-znakomstvo.ru' (Label: vip-znakomstvo) has high entropy (3.52).
07:17:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'infoaustriablog.ru' (Label: infoaustriablog) has high entropy (3.51).
07:17:46	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'mx0.stahlbaupichler.com' (Label: stahlbaupichler) has high entropy (3.51).
07:25:40	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'parquet-discount.ru' (Label: parquet-discount) has high entropy (3.75).
07:26:51	HIGH	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'italianedvizhimost.ru' (Label: italianedvizhimost) has high entropy (3.50).

Z-Shark Network Analysis Report

07:26:51	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ostrovok-rukodeliya.ru' (Label: ostrovok-rukodeliya) has high entropy (3.62).
07:27:41	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'photonaildesign.ru' (Label: photonaildesign) has high entropy (3.51).
07:27:51	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns24.ferngullygraphics.com' (Label: ferngullygraphics) has high entropy (3.73).
07:28:42	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'nlp-marketing.ru' (Label: nlp-marketing) has high entropy (3.55).
07:28:52	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'realtimeconsulting.se' (Label: realtimeconsulting) has high entropy (3.61).
07:29:42	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'present-with-love.ru' (Label: present-with-love) has high entropy (3.57).
07:29:42	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'megnarod-turism.ru' (Label: megnarod-turism) has high entropy (3.64).
07:30:43	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'russianopen2007.ru' (Label: russianopen2007) has high entropy (3.51).
07:30:43	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'russianlawyergroup.ru' (Label: russianlawyergroup) has high entropy (3.57).
07:31:44	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'opentravelcms.ru' (Label: opentravelcms) has high entropy (3.55).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ryazantsev-mig25.ru' (Label: ryazantsev-mig25) has high entropy (3.88).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'rybinsk-zemlya.ru' (Label: rybinsk-zemlya) has high entropy (3.66).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns1.siteground281.com' (Label: siteground281) has high entropy (3.70).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'petro-canada-omsk.ru' (Label: petro-canada-omsk) has high entropy (3.57).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'junglecambodia.ru' (Label: junglecambodia) has high entropy (3.66).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'sochiarenda23.ru' (Label: sochiarenda23) has high entropy (3.55).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'snowbirdgames.ru' (Label: snowbirdgames) has high entropy (3.55).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'snowbird-games.ru' (Label: snowbird-games) has high entropy (3.66).
07:32:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'katalog-suvenirov.ru' (Label: katalog-suvenirov) has high entropy (3.73).
07:34:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'romantikclub.ru' (Label: romantikclub) has high entropy (3.58).
07:34:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'prague-hotels.ru' (Label: prague-hotels) has high entropy (3.55).

Z-Shark Network Analysis Report

07:34:45	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'softservice-tula.ru' (Label: softservice-tula) has high entropy (3.62).
07:36:56	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'fotosuvenir39.ru' (Label: fotosuvenir39) has high entropy (3.55).
07:36:56	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'foundation-courses.ru' (Label: foundation-courses) has high entropy (3.57).
07:36:56	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'hrambagrationovsk.ru' (Label: hrambagrationovsk) has high entropy (3.57).
07:36:56	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'forex-consultant.ru' (Label: forex-consultant) has high entropy (3.62).
07:37:56	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'constellation-vertu.ru' (Label: constellation-vertu) has high entropy (3.58).
07:38:57	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'cns3.my-hosting-panel.com' (Label: my-hosting-panel) has high entropy (3.75).
07:39:57	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'diversant-club.ru' (Label: diversant-club) has high entropy (3.81).
07:39:57	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'establishingabroad.ru' (Label: establishingabroad) has high entropy (3.57).
07:40:58	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'aukettfitzroyrobinson.ru' (Label: aukettfitzroyrobinson) has high entropy (3.65).
07:40:58	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ufsin-vologda.ru' (Label: ufsin-vologda) has high entropy (3.55).
07:42:59	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'axima-consult.ru' (Label: axima-consult) has high entropy (3.55).
07:42:59	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'array2.theemaillaundry.net' (Label: theemaillaundry) has high entropy (3.51).
07:45:52	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'chernogorsk-auto.ru' (Label: chernogorsk-auto) has high entropy (3.58).
07:45:52	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'barnaul-kredit.ru' (Label: barnaul-kredit) has high entropy (3.52).
07:45:52	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'baltschug-kempinski.ru' (Label: baltschug-kempinski) has high entropy (3.93).
07:46:52	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'fusioncabaret.ru' (Label: fusioncabaret) has high entropy (3.55).
07:46:52	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'heruvim-clan.ru' (Label: heruvim-clan) has high entropy (3.58).
07:48:13	**HIGH**	C2 Beaconing Suspect (FFT)	BeaconingDetector	Periodic signal in 147.32.84.165-184.154.132.106:1398-9541:6. Peak: 0.513
09:17:25	**INFO**	Port Scan Suspect (Stateful)	PortScanDetector	Source IP 174.36.246.56 accessed 10 unique ports over time.

Z-Shark Network Analysis Report

09:24:13	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'magicland-spb.ru' (Label: magicland-spb) has high entropy (3.55).
09:24:13	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'magic-patterns.ru' (Label: magic-patterns) has high entropy (3.52).
09:24:13	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'magic-of-numbers.ru' (Label: magic-of-numbers) has high entropy (3.75).
09:24:13	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'magazinchik-online.ru' (Label: magazinchik-online) has high entropy (3.53).
09:25:13	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'matyukhin-stile.ru' (Label: matyukhin-stile) has high entropy (3.64).
09:26:14	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'ns2.siteground293.com' (Label: siteground293) has high entropy (3.70).
09:26:34	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'work4bandwidth.ch' (Label: work4bandwidth) has high entropy (3.52).
09:27:35	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'uralstroytechnika.ru' (Label: uralstroytechnika) has high entropy (3.73).
09:28:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'mysterious-game.ru' (Label: mysterious-game) has high entropy (3.51).
09:28:35	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'build-your-home.ru' (Label: build-your-home) has high entropy (3.51).
09:29:15	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'germanshutenko.ru' (Label: germanshutenko) has high entropy (3.52).
09:31:16	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'art-techcompany.ru' (Label: art-techcompany) has high entropy (3.51).
09:31:16	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'art-linestudio.ru' (Label: art-linestudio) has high entropy (3.52).
09:31:16	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'art-investgroup.ru' (Label: art-investgroup) has high entropy (3.64).
09:31:16	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'art-gold-fishes.ru' (Label: art-gold-fishes) has high entropy (3.64).
09:35:39	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'folkwang-hochschule.de' (Label: folkwang-hochschule) has high entropy (3.68).
09:35:39	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'lazerclinicarostov.ru' (Label: lazerclinicarostov) has high entropy (3.50).
09:41:33	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'sdesign-parquet.ru' (Label: sdesign-parquet) has high entropy (3.64).
09:46:36	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'timesquareband.ru' (Label: timesquareband) has high entropy (3.52).
09:47:27	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'projector-lamps.ru' (Label: projector-lamps) has high entropy (3.51).
09:47:37	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'tvoykaliningrad.ru' (Label: tvoykaliningrad) has high entropy (3.51).

09:48:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'pornomaloletkilesbianki.ru' (Label: pornomaloletkilesbianki) has high entropy (3.56).
09:48:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'professional-penza.ru' (Label: professional-penza) has high entropy (3.50).
09:48:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'profkonsalting.ru' (Label: profkonsalting) has high entropy (3.52).
09:48:28	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'psychoanalystcenter.ru' (Label: psychoanalystcenter) has high entropy (3.51).
09:48:38	**HIGH**	DNS High Entropy (DGA Suspect)	DNSAnomalyDetector	Domain 'soft-magazine-list.ru' (Label: soft-magazine-list) has high entropy (3.61).

5. Mitigation Recommendations

- Isolate the source IP addresses identified in HIGH severity incidents immediately.
- Review firewall and IDS/IPS logs for correlation with the detected events.
- Implement rate-limiting policies on network devices to mitigate future volumetric attacks (e.g., DDoS).
- Update network device firmware and security patches.
- Conduct a full forensic analysis on any hosts identified in ARP Spoofing incidents.