从网络空间认知战到对俄大规模网络致瘫攻击

■ 文档编号	NSF-TR-RPM-204	■ 密级	公开
■ 版本编号	V1.0	■ 日期	2022 年 3 月

■ 版权声明

■ 文档版本变更记录

时间	版本	说明	修改人

■ 适用性声明

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

一、 背景介绍

认知是人们思维的工具。人们通常根据自己的所见所闻作出判断并付诸行动。处于互联网信息化高速发展的今天，人们获取信息和传播信息的速度是以往不能比拟的，通过互联网传播的舆论，发展速度快、传播范围广、控制难度大，任何一个互联网用户都有可能成为潜在目标。传统的“认知战”主要针对敌对方的军人和群众。但是在本次俄乌冲突，亲乌反俄势力，利用网络舆论对全世界的网民发动了“网络空间认知战”，大量利用互联网舆情操纵大众意识，影响大众对乌俄局势的判断，煽动了大量原本中立的互联网民众参与到针对俄罗斯的网络空间战争中来。

近日，绿盟科技天元实验室和威胁情报中心监测到一起从网络空间认知战发展为大规模对俄网络致瘫的攻击事件，战术手段和攻击发动方式历史鲜有，绿盟科技天元实验室对此次网络攻击进行了详细的技战术研判分析。

二、 情报分析

根据威胁情报监测，互联网注册域名为 stop-russian-desinformation.near.page 的网站作为攻击武器载体，在客户端浏览器进行访问时会向俄罗斯联邦相关网站发起大量攻击请求。攻击组织利用互联网时代信息的快速传播能力，致使网站被大量点击访问，而任何一个访问该网站的个人都被动加入到了此次攻击行动当中。

Russia MUST BE STOPPED! Help Ukraine WIN!

English version

The "official" news in the Russian Federation is mostly fake and we believe it is better to shut them down and let people switch to trustful news.

Please, just open this page and let it be open on your devices. It will flood the Russian propaganda websites and pose a huge load on their infrastructure.

Your browser will be slow. It's ok, don't worry and keep it run.

A small contribution from each of us will save Ukraine 🙏

Русская версия

«Официальные» новости в РФ полны пропаганды и транслируют лживую информацию о событиях на Украине. Мы считаем, что лучше их закрыть и позволить людям переключиться на достоверные новости.

Пожалуйста, откройте эту страницу на ваших устройствах. Это зальёт российские пропагандистские сайты запросами и создаст огромную нагрузку на их инфраструктуру.

Ваш браузер будет работать медленно. Все в порядке, не волнуйтесь и держите его открытым.

Небольшой вклад каждого из нас спасет Украину 🙏

Українська версія

«Офіційні» новини в РФ сповнені пропаганди та транслюють брехливу інформацію про події в Україні. Ми вважаємо, що краще їх закрити та дозволити людям переключитися на достовірні новини.

Будь ласка, відкрийте цю сторінку на вашому пристрої. Це закидає російські пропагандистські сайти запитами та створить величезне навантаження на їхню інфраструктуру.

Ваш браузер працюватиме повільно. Все гаразд, не хвилюйтеся та тримайте його відкритим.

Невеликий внесок кожного з нас врятує Україну 🙏

URL	Number of Requests	Number of Errors
https://lenta.ru/	1267	0
https://ria.ru/	266	0
https://ria.ru/lenta/	265	0
https://www.rbc.ru/	267	0
https://www.rt.com/	266	0
http://kremlin.ru/	281	281
http://en.kremlin.ru/	283	283
https://smotrim.ru/	266	0
https://tass.ru/	265	0
https://tvzvezda.ru/	267	0
https://vsoloviev.ru/	266	0
https://www.1tv.ru/	265	0
https://www.vesti.ru/	267	0
https://online.sberbank.ru/	266	0
https://sberbank.ru/	265	0
https://zakupki.gov.ru/	267	0
https://www.gosuslugi.ru/	266	0
https://er.ru/	265	0
https://www.rzd.ru/	265	0
https://rzdlog.ru/	266	0
https://vgtrk.ru/	265	0
https://www.interfax.ru/	265	0
https://www.mos.ru/uslugi/	266	0
http://government.ru/	281	281
https://mil.ru/	265	0
https://www.nalog.gov.ru/	266	0
https://customs.gov.ru/	265	0
https://pfr.gov.ru/	265	0
https://rkn.gov.ru/	266	0

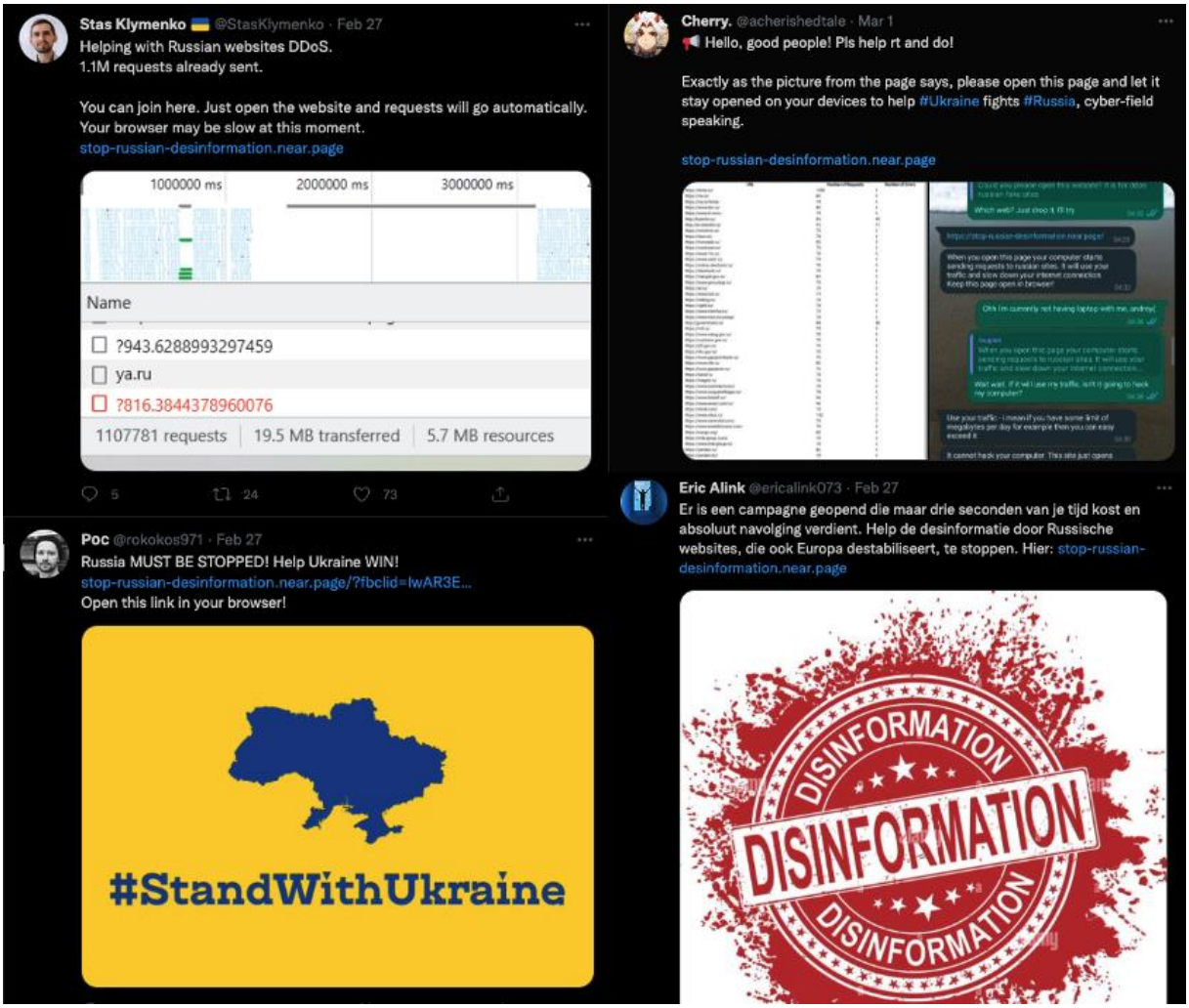
页面用英语，俄语，乌克兰语三种语言分别写下了以下内容：

> 俄罗斯联邦的“官方”新闻大多是假的，我们认为最好关闭它们，让人们转向可信的新闻。
>
> 请打开这个页面，让它在您的设备上打开。它将淹没俄罗斯的宣传网站，并对其基础设施造成巨大的负担。
>
> 你的浏览器会很慢。没关系，别担心，继续运行。
>
> 我们每个人的一点点贡献将拯救乌克兰。

其中被攻击的俄罗斯相关网站服务共计 66 个，主要涉及新闻媒体、政府、金融、工业、航天等行业单位，具体列表如下。

地址	种类	名称
https://lenta.ru/	新闻媒体	Lenta Ru
https://ria.ru/	新闻媒体	俄罗斯国际新闻通讯社
https://ria.ru/lenta	新闻媒体	俄罗斯国际新闻通讯社
https://www.rbc.ru	新闻媒体	RBK Group
https://www.rt.com	新闻媒体	RT电视台
http://kremlin.ru	新闻媒体	俄罗斯联邦总统官方网站
http://en.kremlin.ru	新闻媒体	俄罗斯联邦总统官方网站
https://smotrim.ru	视频平台	观看
https://tass.ru	新闻媒体	俄通社-塔斯社
https://tvzvezda.ru	新闻媒体	红星电视台
https://vsoloviev.ru	新闻媒体	索洛维科夫媒体
https://www.1tv.ru	新闻媒体	俄罗斯第一频道
https://www.vesti.ru	新闻媒体	Vesti.ru
https://online.sberbank.ru	银行金融	俄罗斯联邦储蓄银行
https://sberbank.ru	银行金融	俄罗斯联邦储蓄银行
https://zakupki.gov.ru	政府	统一采购信息系统
https://www.gosuslugi.ru	政府	俄罗斯联邦公共服务门户网站
https://er.ru	政党	统一俄罗斯政党官网
https://www.rzd.ru	铁路	俄罗斯铁路
https://rzdlog.ru	铁路	俄罗斯铁路物流
https://vgtrk.ru	俄罗斯媒体	全俄国家电视广播公司
https://www.interfax.ru	俄罗斯通信社	国际文传电讯社
https://www.mos.ru/uslugi	政府	莫斯科市长门户网站
http://government.ru	政府	俄罗斯联邦政府官网
https://mil.ru	政府	俄罗斯联邦国防部
https://www.nalog.gov.ru	政府税务	联邦税务局
https://customs.gov.ru	政府海关	俄罗斯联邦海关总署
https://pfr.gov.ru	政府联邦养老基金	俄罗斯联邦养恤基金
https://rkn.gov.ru	政府通信监测	俄罗斯联邦通信、信息技术和大众传媒监督局
https://www.gazprombank.ru	银行金融	天然气工业银行
https://www.vtb.ru	银行金融	俄罗斯外贸银行
https://www.gazprom.ru	国有能源	俄罗斯天然气工业股份公司
https://lukoil.ru	石油能源	卢克石油
https://magnit.ru	食物供应	Magnit 零售
https://www.nornickel.com	矿业冶金	诺里尔斯克镍公司
https://www.surgutneftegas.ru	石油天然气	苏尔古特内夫特加斯公司
https://www.tatneft.ru	石油	塔特内夫特公司
https://www.evraz.com/ru	钢铁矿石	耶弗拉兹公司
https://nlmk.com	钢铁	新波利佩茨克钢铁
https://www.sibur.ru	石油化工	西伯公司
https://www.severstal.com	钢铁矿石	北方钢铁
https://www.metalloinvest.com	开采冶金	Metalloinvest 公司
https://nangs.org	石油天然气	国家石油和天然气服务协会
https://rmk-group.ru/ru	冶金	俄罗斯铜业股份有限公司
https://www.tmk-group.ru	钢铁	OAO TMK管道冶金公司
https://yandex.ru	互联网搜索引擎	燕基科斯
https://yandex.by	互联网搜索引擎	燕基科斯
https://www.polymetalinternational.com/ru	金属矿业	国际聚金属公司
https://www.uralkali.com/ru	化学工业	乌拉尔钾肥公司
https://www.eurosib.ru	能源	EuroSibEnergo公司
https://omk.ru	能源	联合冶金公司
https://mail.rkn.gov.ru	传媒监督	俄罗斯联邦通信、信息技术和大众传媒监督局
https://cloud.rkn.gov.ru	传媒监督	俄罗斯联邦通信、信息技术和大众传媒监督局
https://mvd.gov.ru	政府	俄罗斯联邦内务部
https://pwd.wto.economy.gov.ru	政府	俄罗斯联邦经济发展部
https://stroi.gov.ru	政府	俄罗斯城市规划
https://proverki.gov.ru	政府	俄罗斯联邦总检察长办公室
https://www.gazeta.ru	新闻媒体	俄罗斯日报
https://www.crimea.kp.ru	新闻媒体	克里米亚新闻
https://www.kommersant.ru	新闻媒体	生意人报
https://riafan.ru	新闻通信社	联邦通讯社
https://www.mk.ru	新闻媒体	莫斯科共青团员报
https://api.sberbank.ru/prod/tokens/v2/oauth	银行金融	俄罗斯联邦储蓄银行
https://api.sberbank.ru/prod/tokens/v2/oidc	银行金融	俄罗斯联邦储蓄银行
https://www.vedomosti.ru	新闻媒体	韦多科斯蒂报
https://sputnik.by/	人造卫星	白俄罗斯卫星通讯社

该网站自 2 月 25 日起在 Twitter、Telegram 等国外互联网社交平台出现后快速传播形成了一定影响力，使得网络攻击攻势愈发猛烈。



使用 ping 查看该网站 ip，发现使用了 CDN：

```
C:\Users\yy>ping stop-russian-desinformation.near.page

Pinging gcp-us-west1-1-proxy.render.com [34.83.64.96] with 32 bytes of data:
Reply from 34.83.64.96: bytes=32 time=201ms TTL=51
Reply from 34.83.64.96: bytes=32 time=216ms TTL=51
Reply from 34.83.64.96: bytes=32 time=201ms TTL=51

34.83.64.96 的 Ping 統計資料:
    封包: 已傳送 = 3, 已收到 = 3, 已遺失 = 0 (0% 遺失),
大約的來回時間 (毫秒):
    最小值 = 201ms, 最大值 = 216ms, 平均 = 206ms
```

CDN 地址则属于美国谷歌云：

对其域名进行 whois 查询，域名服务商同样是谷歌，组织地址则显示为加拿大：

Domain	**near.page**
Nameserver	ns-cloud-a1.googledomains.com
Domain registrar	nic.google
Nameserver organisation	whois.markmonitor.com
Organisation	Contact Privacy Inc. Customer 12410033126, Redacted For Privacy, Redacted For Privacy, REDACTED FOR PRIVACY, Canada
DNS admin	cloud-dns-hostmaster@google.com
Top Level Domain	Page (.page)
DNS Security Extensions	Enabled

该域名证书记录最早出现于 2021 年 4 月 22 日。

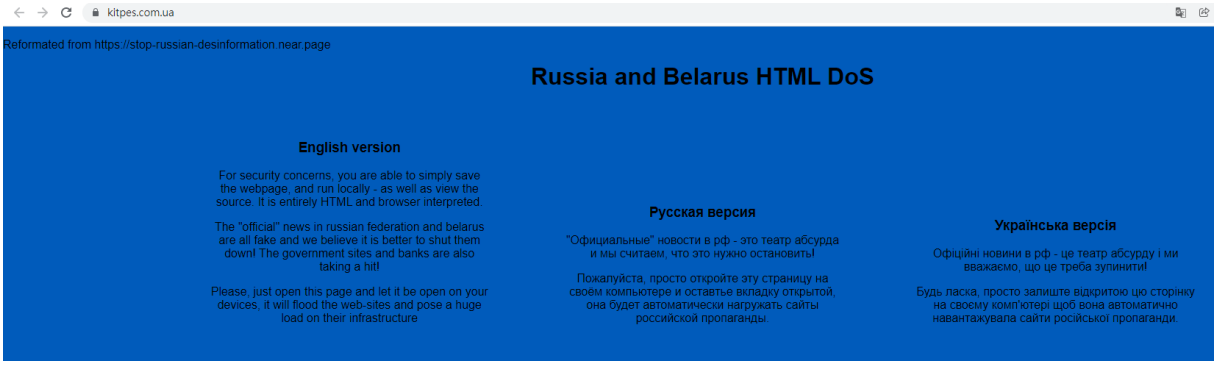
Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	Issuer Name
6069711082	2022-01-28	2022-01-28	2022-04-28	*.near.page	*.near.page near.page	C=US, O=Let's Encrypt, CN=R3
6060951964	2022-01-28	2022-01-28	2022-04-28	*.near.page	*.near.page near.page	C=US, O=Let's Encrypt, CN=R3
5988291385	2022-01-16	2022-01-16	2022-04-16	near.page	near.page	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5968607255	2022-01-13	2022-01-13	2022-04-13	www.near.page	www.near.page	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5697968520	2021-11-29	2021-11-29	2022-02-27	*.near.page	*.near.page near.page	C=US, O=Let's Encrypt, CN=R3
5697970445	2021-11-29	2021-11-29	2022-02-27	*.near.page	*.near.page near.page	C=US, O=Let's Encrypt, CN=R3
5636502038	2021-11-19	2021-11-19	2022-02-17	near.page	near.page	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5626914036	2021-11-17	2021-11-17	2022-02-15	www.near.page	www.near.page	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5311699268	2021-09-30	2021-09-30	2021-12-29	*.near.page	*.near.page near.page	C=US, O=Let's Encrypt, CN=R3
5311692705	2021-09-30	2021-09-30	2021-12-29	*.near.page	*.near.page near.page	C=US, O=Let's Encrypt, CN=R3
5262875785	2021-09-21	2021-09-21	2021-12-20	near.page	near.page	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5262854839	2021-09-21	2021-09-21	2021-12-20	www.near.page	www.near.page	C=US, O=Google Trust Services LLC, CN=GTS CA 1D4
5262817564	2021-09-21	2021-09-21	2022-09-20	www.near.page	www.near.page	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc ECC CA-3
5262817561	2021-09-21	2021-09-21	2022-09-20	www.near.page	www.near.page	C=US, O="Cloudflare, Inc.", CN=Cloudflare Inc RSA CA-2
5075534619	2021-08-20	2021-08-20	2021-11-18	*.near.page	*.near.page	C=US, O=Let's Encrypt, CN=R3
5075534059	2021-08-20	2021-08-20	2021-11-18	*.near.page	*.near.page	C=US, O=Let's Encrypt, CN=R3
4738539393	2021-06-21	2021-06-21	2021-09-19	*.near.page	*.near.page	C=US, O=Let's Encrypt, CN=R3
4735686685	2021-06-21	2021-06-21	2021-09-19	*.near.page	*.near.page	C=US, O=Let's Encrypt, CN=R3
4413731426	2021-04-22	2021-04-22	2021-07-21	*.near.page	*.near.page	C=US, O=Let's Encrypt, CN=R3
4413731881	2021-04-22	2021-04-22	2021-07-21	*.near.page	*.near.page	C=US, O=Let's Encrypt, CN=R3

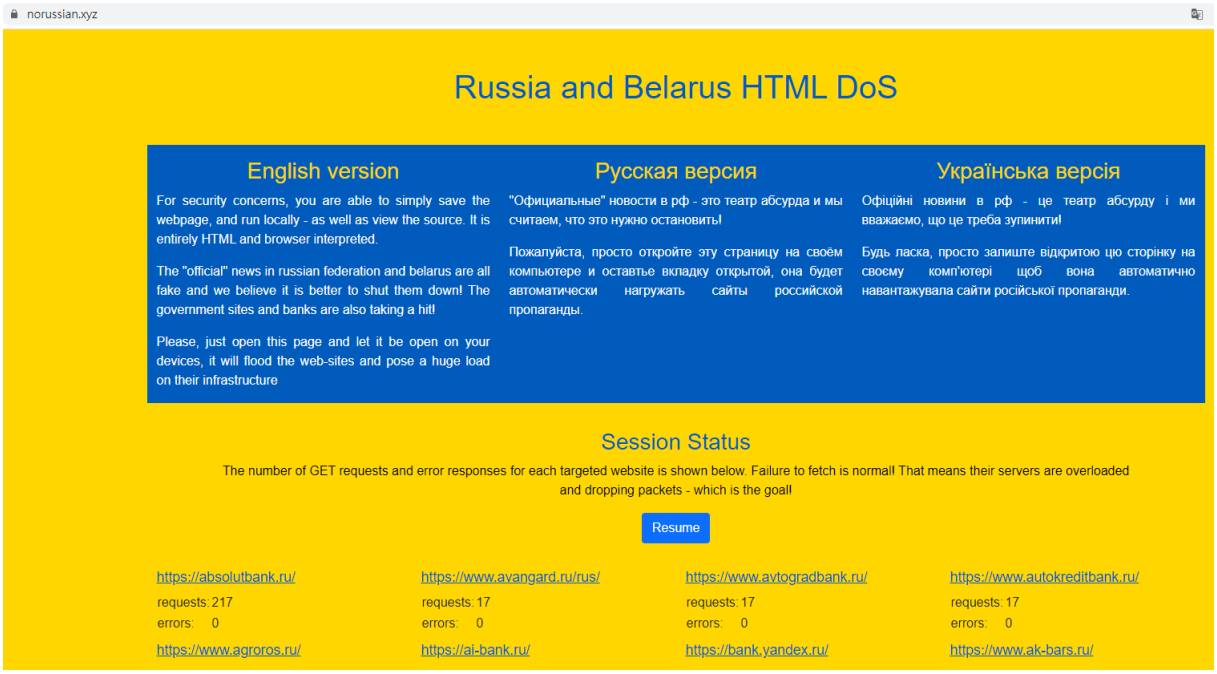
其域名解析地址为 216.239.36.21，同样是谷歌云服务，该 IP 在过去被多次标记为用于黑

客攻击。

该网站在传播扩散后，也引起了其他网站的效仿，https://www.kitpes.com.ua/标明其修改自 https://stop-russian-desinformation.near.page。该网站在左上角标注了是原网站的重构页面，目标是对俄罗斯和白俄罗斯进行 DDOS 攻击，同时将 DDOS 的目标列表扩展到了 166 个。虽然保持了原有功能，但是页面的排版比较混乱。



另一相似 DDoS 网站 https://norussian.xyz/出现的晚一些，但页面进行了部分优化，并将进行 DDOS 的网址列表扩展到了 252 个。同时改善原网站保持开启造成的卡顿现象，还添加了开始和暂停按钮。



三、 技术分析

stop-russian-desinformation.near.page 攻击页面分为两个部分。第一部分为网页的介绍信息，包括英语、乌克兰语和俄语三个版本，主旨大意是希望反对俄罗斯政府的人保持该页面开启；第二部分是俄罗斯宣传网址列表和当前请求的次数以及错误次数。该页面主要通过 JS

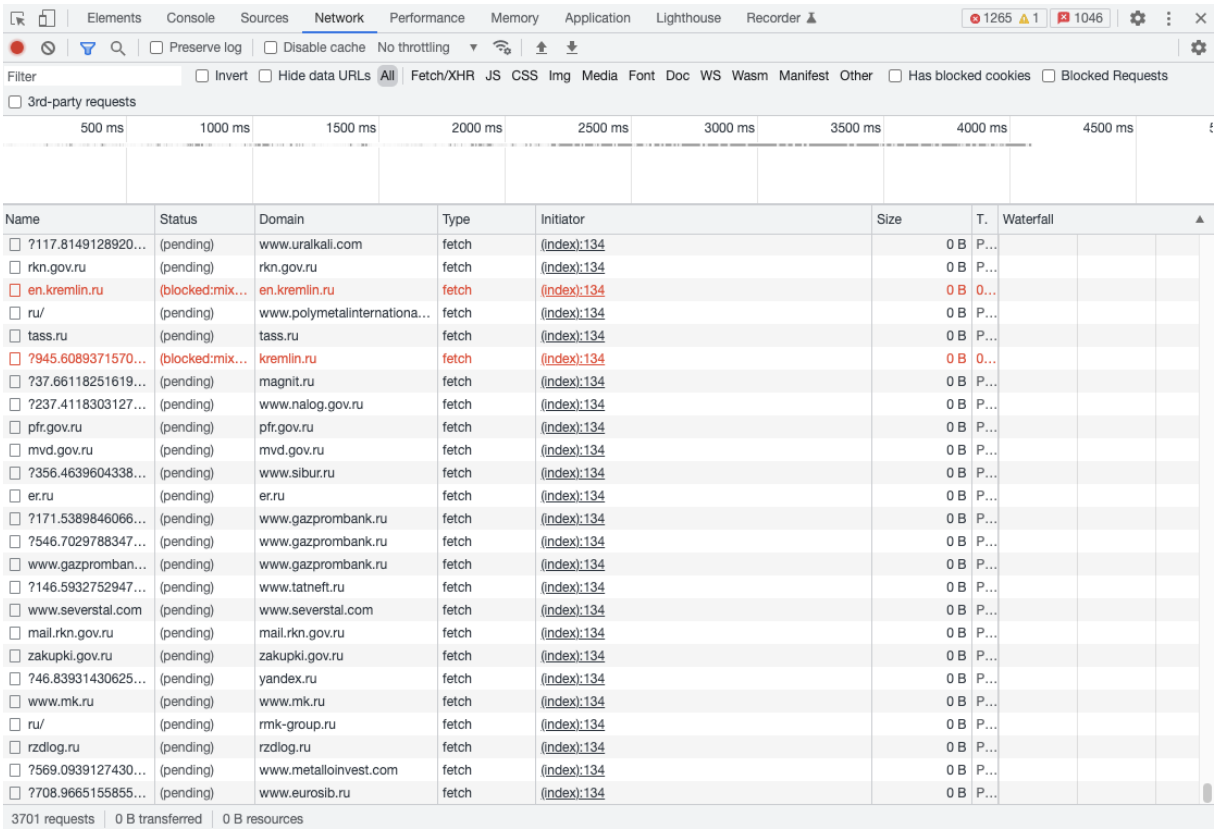
向俄罗斯网址发送请求实现 DOS 攻击，页面中写入一个静态的地址列表，为 66 个需要请求的俄罗斯宣传网址。

```
var targets = [
  'https://lenta.ru/',
  'https://ria.ru/',
  'https://ria.ru/lenta/',
  'https://www.rbc.ru/',
  'https://www.rt.com/',
  'http://kremlin.ru/',
  'http://en.kremlin.ru/',
  'https://smotrim.ru/',
  'https://tass.ru/',
```

在构造请求时，设置了较长的 timeout，使得 HTTP 请求不能基地释放，消耗目标服务器的连接数，达到 DD　OS 攻击的目的。同时使用 Get 请求并设置‘no-cors’模式，使得浏览器进行跨域请求时不妨问也不保存服务器返回的内容，减小了客户端的压力。

```
async function fetchWithTimeout(resource, options) {
  const controller = new AbortController();
  const id = setTimeout(() => controller.abort(), options.timeout);
  return fetch(resource, {
    method: 'GET',
    mode: 'no-cors',
    signal: controller.signal
  }).then((response) => {
    clearTimeout(id);
    return response;
  }).catch((error) => {
    clearTimeout(id);
    throw error;
  });
}
```

在打开该网页后，短短几秒钟就会发起几千个请求，目前对于大部分站点的请求状态是挂起，只有少量被屏蔽。一旦有大量的人员访问这个页面，就会形成 DDOS 攻击。而且这种 DDOS 攻击对于攻击发起者来讲没有流量和管理的代价，十分经济实惠。



查看某一个请求的请求头信息，其中的 Refer 信息中包含了本地活动的网站地址：https://stop-russian-desinformation.near.page/。服务端可以通过检查 Refer 信息区分请求是否是本次攻击所发起的异常请求。

四、战术分析

传统的网络空间作战是围绕争夺网络空间控制权而展开的各种技术战术行动。利用网络空间武器来压制和摧毁敌方在陆、海、空、天等领域的基础设施和电子攻击系统，取得作战优势。但是此次俄乌冲突有一个非常重要的技术发展背景，就是数字化时代以来的第一次全民都有参与感、沉浸式体验、网红式的“视频战争”。带给普通人的观感，跟以往的战争相比已经出现了颠覆性的变化。由于互联网的特性，每个人都能接受到这些具体战争信息，对于大众舆论的争夺和操纵变得极为重要。

战争三大要素之一就是人，人是战争的主体，战争需要人来参与，网络空间作战也不例外。该组织利用了简单的技术和资源，却能够发动起针对俄罗斯的 DDOS 攻击，其主要利用

全民参与的思想，将任何访问该页面的人都转化本地 DDOS 攻击中的一份力量，达到了四两拨千斤的效果。该 DDOS 攻击的网络流量完全依托于访问该页面的访问人员数量，利用网络中所谓“吃瓜”、“反战”等网络风向来诱导更多的人访问并进一步扩散。在这种频繁的网络攻击下，我们也可以理解俄罗斯为什么打算与全球互联网断开，启用自己的大局域网“Runet”。

五、解读

随着网络信息化的快速发展，现代化战争的边界变得模糊。攻击者利用信息舆论影响发动网络攻击致瘫敌方新闻媒体，以此削弱敌方对外的舆论影响。与传统的 DDOS 攻击形态不一样的地方在于攻击者此次并未花费很多网络资源，而是借助认知影响和互联网传播能力散播网络武器，操纵大众完成网络攻击。目前，俄乌军事冲突形势还不明朗，此次网络攻击行动也还在持续，不可否认，网络战已经成为现代化战争中的重要组成部分。