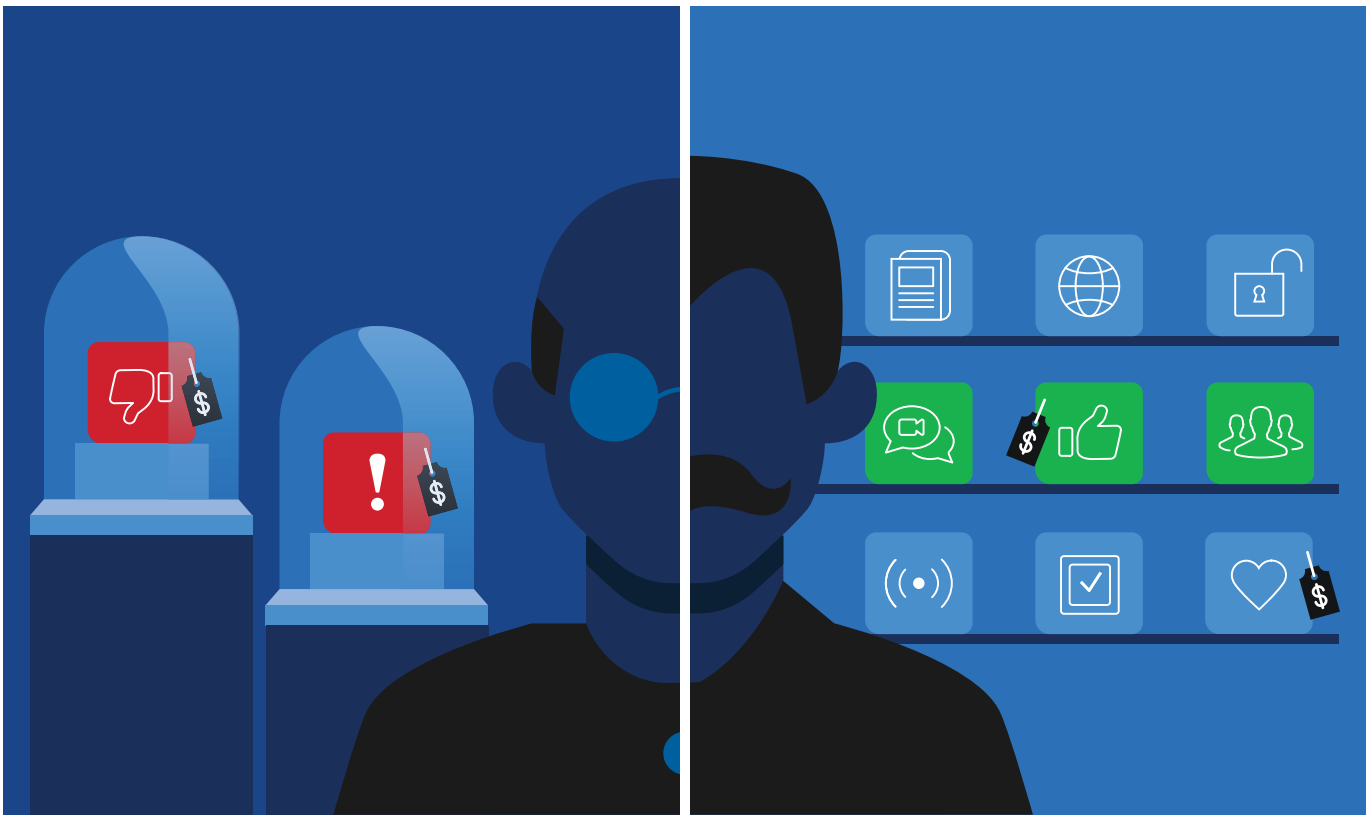
Recorded Future

CYBER THREAT ANALYSIS

The Price of Influence:

Disinformation in the Private Sector

By Insikt Group®



CTA-2019-0930

Insikt Group® used the Recorded Future® Platform, proprietary sources, and underground forum analysis to provide deeper insight into the operations of two of the more sophisticated disinformation vendors on Russian-speaking underground forums. To test the operational capabilities of these vendors, Insikt Group engaged with one threat actor to generate positive disinformation and the other for negative disinformation, both directed at a fictitious company we created.

This report will be of interest to private, public, and political organizations concerned with disinformation campaigns, as well as those interested in how threat actors create and distribute disinformation content throughout the internet.

***Editor's Note**: In order to protect Recorded Future sources and operations, this report will use pseudonyms for all involved parties, identifying the threat actors involved with the code names "Raskolnikov" and "Doctor Zhivago," while the fictitious company involved will be identified as "Tyrell Corporation" for the purposes of this report.*

Executive Summary

Insikt Group analyzed the operations of two threat actors who were offering disinformation as a service on Russian-speaking underground forums in order to understand the business model of how disinformation is used by cybercriminals, as opposed to nation-states. To do so, we created a fictitious company and commissioned two different threat actors to generate intentionally false narratives across the web.

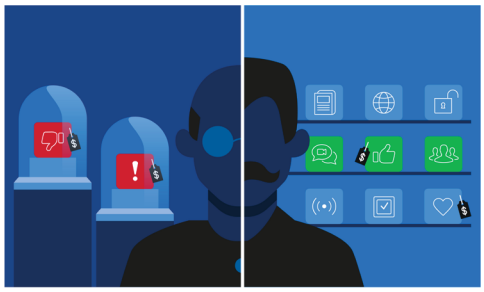
One threat actor created propaganda in the form of positive PR to make our company seem appealing, while the other generated malicious material accusing that same company of unethical business practices. In the end, we were able to launch both campaigns in less than a month for only a few thousand dollars.

Key Judgments

- Disinformation services are publically available on underground criminal forums and are run by criminal threat actors and nation-states.
- Disinformation services are highly customizable in scope, costing anywhere from several hundreds of dollars to hundreds of thousands of dollars, or more depending on the client's needs.
- Disinformation service providers have the ability to publish articles in media sources ranging from dubious websites to more reputable news outlets.
- Disinformation service providers have the ability to create and maintain social media accounts in bulk and use a combination of both established and new accounts to propagate content without triggering content moderation controls.

Our Experience

To investigate both aspects of the disinformation spectrum, we created the Tyrell Corporation, a fictitious company located in a Western country, to use as the target. One threat actor was tasked with destroying the Tyrell Corporation's reputation, and the other was asked to create a positive public perception.



- Was told our contact held a personal grudge against the Tyrell Corporation, a competitor, and wanted their reputation destroyed
- Claimed to work with a team of journalists, editors, translators, search engine optimization specialists, and hackers
- Services ranged from $15 for an article of up to 1,000 characters to $1,500 for SEO services and traditional media articles

- Was told our contact was a business owner who needed more social media attention for their new company: Tyrell Corporation
- Provided the Tyrell Corporation with a list of media sources and prices for publishing articles on each — some obscure, some relatively well-known
- Services ranged from $45 for an article of up to 1,000 characters to $350-550 per month for social media marketing

Both threat actors patiently answered questions, outlined their respective processes, and even provided samples of similar work done in the past

THEIR METHODS

SOCIAL MEDIA

- Created multiple individual and group accounts on major Western platforms so the disinformation would appear to come from real people
- Also used "aged" accounts with established history on platforms
- Befriended citizens in the Tyrell Corporation's country to target the message

- Created accounts for the Tyrell Corporation on major Western platforms
- Gathered 100+ followers on each account

MEDIA ARTICLES

- Wrote and published articles claiming the Tyrell Corporation manipulated employees
- Shared articles using aged accounts first, then new accounts

- Produced generic articles about the company and its supposed prowess
- Wrote in clearly non-native English but revised upon feedback from the client
- Distributed to one low-profile publication within two weeks, as well as another more reputable publication that has been in operation for over 100 years

The process was alarmingly simple

The entire process took less than a month.

The scope of work is highly customizable, with services ranging from hundreds of dollars to hundreds of thousands or more.

Disinformation service providers have the ability to create and maintain social media accounts in bulk and propagate content without triggering content moderation controls.

If the ease of this experience is any indication, we predict that disinformation as a service will soon spread from a nation-state tool to one increasingly used by individuals and organizations.

Recorded Future

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

Threat Analysis

Disinformation has been a tactic used in information warfare commonly associated with the statecraft of the Soviet Union throughout the Cold War. Disinformation, or "dezinformatsiya," is defined by the Great Soviet Encyclopedia as false information with the intention to deceive public opinion. The term was coined by Joseph Stalin, and even the word itself was a form of disinformation; according to Soviet defector Ion Mihai Pacepa, Stalin deliberately gave it a French-sounding name in order to claim that both the term and the tactic originated in Western Europe and was a tool used by the "Capitalist Imperialists" to destroy Communism and the workers' paradise.

Disinformation operations have existed throughout history and have been used by kings, dictators, and governments throughout the world. Octavian wielded propaganda to destroy the reputation of Mark Antony during the last of the Roman civil wars. The Soviet Union launched a multitude of campaigns slandering Pope Pious XII as "Hitler's Pope" and distributed copies of the antisemitic "Protocols of the Elders of Zion" throughout Islamic regions of the world to foster religious tensions.[1] In another campaign, the USSR spread a conspiracy theory via Indian news outlets that the United States had developed the AIDS virus in a laboratory as a biological weapon.[2] The Reich Ministry of Propaganda and Public Enlightenment headed by Joseph Goebbels in Nazi Germany spread propaganda throughout Germany and its occupied territories. Recent disinformation campaigns include attacks against the 2016 and 2018 U.S. elections by the Russian intelligence services, including the GRU and SVR, along with Kremlin-backed media sites RT and Sputnik News.

[1] Ion Mihai Pacepa and Ronald J. Rychlak (2013), Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism.
[2] United States Department of State (1987), Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986–87, Washington D.C.: Bureau of Public Affairs, pp. 34–35, 39, 42.

While in recent years there has been an increased focus on state-sponsored disinformation campaigns, Recorded Future identified that there is also a private-sector market for disinformation and threat actors who are ready to provide the services to those who are willing to pay. In particular, Recorded Future analysts have identified established threat actors operating in the Russian-speaking underground forums offering these services. There, Insikt Group discovered two threat actors advertising such services. For the sake of this report, we will refer to them as "Doctor Zhivago" and "Raskolnikov." To put their skills to the test, we decided to create a fictitious company located in a Western country to use as our target. We will refer to this company as "Tyrell Corporation."

We wanted to investigate both aspects of the disinformation spectrum, so we hired Raskolnikov to market Tyrell Corporation with positive PR, and Doctor Zhivago to do the opposite. In Doctor Zhivago's case, they proposed spreading invented stories of misconduct and poor business practices to damage the reputation of Tyrell Corporation. In the end, both Raskolnikov and Doctor Zhivago delivered on their promises, and Insikt Group discovered that disinformation campaigns, even against a Western company using Western media, could be launched in a timely and affordable manner.

Launching a disinformation campaign was a simple process, and both Raskolnikov and Doctor Zhivago were very informative and helpful. Their services were advertised on popular Russian-language underground forums, where they listed their Jabber and Telegram handles for all to see. Both actors had pricing models showing the cost of content generation so you could budget out your disinformation campaign. Doctor Zhivago's services were priced very specifically, as seen below:

- $15 for an article up to 1,000 characters
- $8 for social media posts and commentary up to 1,000 characters
- $10 for Russian to English translation up to 1,800 characters
- $25 for other language translation up to 2,000 characters
- $1,500 for SEO services to further promote social media posts and traditional media articles, with a time frame of 10 to 15 days

Raskolnikov, on the other hand, had less specific pricing:

- $150 for Facebook and other social media accounts and content
- $200 for LinkedIn accounts and content
- $350–$550 per month for social media marketing
- $45 for an article up to 1,000 characters
- $65 to contact a media source directly to spread material
- $100 per 10 comments for a given article or news story

We contacted Raskolnikov claiming to be a business owner who needed some media attention for their new company: Tyrell Corporation. Shortly thereafter, we used a different alias to contact Doctor Zhivago, claiming to have a personal grudge against the Tyrell Corporation, who we competed with, and needing Doctor Zhivago's services accordingly.

Both Raskolnikov and Doctor Zhivago were true salespeople. They patiently answered question after question about what they would do and how they would do it, even providing samples of what they had done in previous operations. After our objectives were agreed upon and payment was made, first our positive and then our negative disinformation campaigns were launched targeting the Tyrell Corporation. In all, the process took less than a month.

Raskolnikov created accounts for Tyrell Corporation on several social media platforms and gathered a following of over 100 users for each account on various platforms. The profiles generally appeared authentic, using images and names of managers from Tyrell Corporation's website. At this time, we are unsure how many of the followers were trolls or bots, but we did see what appeared to be comments from real people asking questions about the company. This led us to believe that it was probably a combination of both: bots, or trolls, spreading disinformation content that was picked up by real users. There is really nothing suspicious about the Tyrell Corporation's social media accounts aside from it being a new company.

The next step was publishing articles in the media. Raskolnikov informed us that we could essentially publish as many articles praising our new company as we wanted, so we chose to start with two. Raskolnikov wrote up two separate articles with essentially identical content, and sent them to us for review before publication. The articles were generic, announcing our new, wonderful company — Tyrell Corporation — to the world, and why we were better than the rest. However, the writing was not at the level of a native English speaker and we had Raskolnikov rewrite the articles multiple times until we felt the language could pass for a genuine article in an English-language media outlet.

Raskolnikov provided the following price list for publications where articles could allegedly be published for a U.K.-based disinformation promotion campaign:

Number	Source	Price
1	cheapautoinsuranceee[.]com	$180.00
2	taftcollege[.]org	$180.00
3	loan-st[.]com	$200.00
4	marketingwithmiles[.]com	$220.00
5	entrepreneurshiplife[.]com	$250.00
6	traveltweaks[.]com	$250.00
7	bluntmoney[.]com	$250.00
8	lovebelfast[.]co[.]uk	$250.00
9	housingpedia[.]com	$250.00
10	makemoneysaving[.]com	$250.00
11	herjobs[.]com	$250.00
12	brussels[.]com	$500.00
13	savingadvice[.]com	$630.00
14	seethru[.]co[.]uk	$600.00
15	aboutmanchester[.]co[.]uk	$600.00
16	abcmoney[.]co[.]uk	$600.00
17	calculator[.]co[.]uk	$600.00

Number	Source	Price
18	filmoria[.]co[.]uk	$600.00
19	flatpackhouses[.]co[.]uk	$600.00
20	newstoday[.]co[.]uk	$600.00
21	soundltout[.]co[.]uk	$600.00
22	teamtalk[.]com	$448.18
23	sundaypost[.]com	$567.43
24	glassofbubbly[.]com	$445.00
25	breakingtravelnews[.]com	$500.00
26	ninetyminutesonline[.]com	$505.00
27	stories.swns[.]com	$508.75
28	angliya[.]com	$791.25
29	thefintechtimes[.]com	$810.00
30	eatsleepsport[.]com	$713.75
31	trustedreviews[.]com	$8,405.30
32	dezeen[.]com	$3,416.37
33	order-order[.]com	$1,928.34
34	thecourier[.]co[.]uk	$1,021.50
35	eveningexpress[.]co[.]uk	$832.14
36	wallpaper[.]com	$8,404.80
37	eveningtimes[.]co[.]uk	$1,260.00
38	londonist[.]com	$3,469.60
39	worldtravelguide[.]net	$2,081.60
40	thelondoneconomic[.]com	$740.80
41	research-live[.]com	$1,260.00
42	examinerlive[.]co[.]uk	$631.20
43	accessaa[.]co[.]uk	$1,260.00
44	ft[.]com	$49,440.00
45	buzzfeed[.]com	Unspecified

In two weeks, the Tyrell Corporation was in the "news" — one of the media sources was a less established media outlet, though the other was a very reputable source that had published a newspaper for nearly a century. While creating and publishing disinformation content with Raskalnikov was bumpy, in the end, the actor delivered, confirming the claim of being able to operate disinformation campaigns in Western countries.

However, of these two threat actors, Recorded Future analysts believe Doctor Zhivago to be the more experienced. This threat actor had been on the underground forums longer than Raskolnikov and had a well-established status. Based on discussions we had with Doctor Zhivago, we believe our primary contact was a Russian national and native Russian speaker, similar to Raskolnikov. In our communications, Doctor Zhivago was politely formal, as well as informative, even providing examples showing publications in some very reputable Russian-language media sources. Doctor Zhivago claimed to work with a team that included journalists, editors, translators, search engine optimization (SEO) specialists, and hackers. Doctor Zhivago maintained that this organization could spread disinformation accusing an individual or company of everything from business misconduct to criminal activity — whatever it took to permanently destroy a reputation.

Since the Tyrell Corporation now had a positive presence on the internet, it was time to see if it could be destroyed. We decided to use Doctor Zhivago to discredit our company's business practices, staying away from any criminal accusations that could theoretically have real-world implications. Doctor Zhivago estimated that our campaign would take a month or two to go into full effect because a successful disinformation operation happens in phases by gradually introducing an intentionally false narrative in an organic manner. The "proof" for our disinformation needed to come from "real people," so Doctor Zhivago created them in the form of individual and group accounts on the same major social media platforms that Raskolnikov had used.

Since the Tyrell Corporation was both new and fictitious, there wasn't any publicly available information for Doctor Zhivago to manipulate. The group submitted a few articles for our review that accused the Tyrell Corporation of manipulating its employees by putting them in compromising situations. The articles stopped just short of accusing the company of criminal offenses, but anyone reading the articles would likely come to the conclusion that the Tyrell Corporation was not reputable and treated its employees as disposable objects. The content was written in much better English than what Raskolnikov had provided us, though there were a few awkward sentences that suggested this too wasn't the writing of a native English speaker. But like Raskolnikov, Doctor Zhivago was quick to correct these linguistic issues after we provided our feedback. With the articles published, it was now time to spread them throughout Doctor Zhivago's social media apparatus.

Doctor Zhivago had an organic, layered approach to propagating material throughout social media. First, a group of older accounts — referred to as "aged accounts" — that posted links to the articles they had published in media sources was employed. Then, a new batch of accounts that reposted content from the aforementioned aged accounts to amplify the messages was used. These new accounts befriended citizens living in the same country the Tyrell Corporation was located in to make the campaign more effective by targeting the audience. Doctor Zhivago explained to us that they usually create a few thousand social media accounts when engaging in these types of operations, as only a percentage of them would survive without being banned. Once the operation began, the articles went live on a number of media sites and were referenced throughout the social media platforms by accounts controlled by Doctor Zhivago.

Doctor Zhivago's list of media resources available for a U.K.-based disinformation campaign can be seen below. Doctor Zhivago broke up the media resources into categories they identified as "low profile," "medium profile," and "top level."

Low Profile	Medium Profile	Top Level
viennatimes[.]com — $600	Aboutmanchester[.]co[.]uk — $1,340	reuters[.]com — $8,360
amiranews[.]com — $500	stories[.]swns[.]com — $1,340	dailypioneer[.]com — $6,350
dailyreleased[.]com — $500	abcmoney[.]co[.]uk — $1,340	econotimes[.]com — $6,685
xulnews[.]com — $500	calculator[.]co[.]uk — $1,340	mashable[.]com — $13,370
thesocialmagazine[.]com — $600	fortuneherald[.]com — $1,340	chamberofcommerce[.]com — $6,020
westernrelease[.]com — $600	newstoday[.]co[.]uk — $1,340	newsmax[.]com — $6,685
broowaha[.]com — $500		techradar[.]com — $18,385
srjnews[.]com — $650		techtimes[.]com — $4,010
lovebelfast[.]co[.]uk — $560		
talk-business[.]co[.]uk — $600		
15zjazd.whus[.]pl — $100		
businessexponow[.]co[.]uk — $400		
esrel2016[.]org — $400		
internet-directory-web[.]com — $400		

Outlook

From our research, Insikt Group discovered that launching a disinformation campaign is alarmingly simple and inexpensive. Recorded Future spent a total of $6,050 on both campaigns, with $1,850 going to the initial promotion by Raskolnikov, and $4,200 going to Doctor Zhivago for the negative disinformation to discredit our fictitious company.

Disinformation services are publically available on the underground criminal forums, and accessible to private sector clients — not only nation-states. These services are affordable and customizable. Their operators work in teams to publish articles on media websites and to propagate that material throughout social media accounts under their direct control.

They are willing to go to extreme lengths to accomplish their tasks, including filing false accusations with law enforcement against target entities. In the case of Doctor Zhivago, the threat actor offered to file a complaint against our fictitious company for involvement in human trafficking. And even though we used the Raskolnikov threat actor to promote Tyrell Corporation, Raskolnikov also offered a "takedown service" should we ever need to get even with another individual, set someone up at their place of work, destroy a competitor's reputation, counter an opponent's disinformation attack, or even "sink an opponent in an election."

Today, the Tyrell Corporation lives on in social media and search engine results. Googling the domain name will present the unfavorable content created by Doctor Zhivago, though searching the company name directly will produce the positive articles and social media accounts created by Raskolnikov. If our experience is any indication, we predict that disinformation as a service will spread from a nation–state tool to one increasingly used by private individuals and entities, given how easy it is to implement.

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.