CLOUDFLARE
AREA 1 SECURITY

# PHISHING BURISMA HOLDINGS

Cloudflare, Inc. acquired Area 1 Security in 2022

## PHISHING BURISMA HOLDINGS

The mission of Area 1 Security is to eliminate phishing, and through the course of our normal business, we frequently discover the origins and outcomes of cyber campaigns. Nine out of ten cyberattacks begin with phishing, and the damages are having a significant impact on public, private, and political organizations globally.

This report details an ongoing Russian government phishing campaign targeting the email credentials of employees at Burisma Holdings and its subsidiaries and partners. The campaign against the Ukrainian oil & gas company was launched by the Main Intelligence Directorate of the General Staff of the Russian Army or GRU.

Phishing for credentials allows cyber actors to gain control of an organization's internal systems by utilizing trusted access methods (e.g.: valid usernames and passwords) in order to observe or to take further action. Once credentials are phished, attackers are able to operate covertly within an organization in pursuit of their goal.

Like all phishing campaigns, we observe the GRU was successful because they found ways to appear authentic to their targets, rather than using any technical sophistication. Everything about their approach is technically unremarkable, yet highly effective. In this campaign the GRU combines several different authenticity techniques to achieve success:

1. Domain-based authenticity
2. Business process and application authenticity
3. Partner and supply chain authenticity

A key aspect of cyberattack preemption is having a deep understanding of cyber actor patterns and continually discovering and deconstructing campaigns to anticipate future ones. Our report is not noteworthy because we identify the GRU launching a phishing campaign, nor is the targeting of a Ukrainian company particularly novel. It is significant because Burisma Holdings is publically entangled in U.S. foreign and domestic politics. The timing of the GRU's campaign in relation to the 2020 U.S. elections raises the spectre that this is an early warning of what we have anticipated since the successful cyberattacks undertaken during the 2016 U.S. elections.

OREN J. FALKOWITZ | CO-FOUNDER & CEO

BLAKE DARCHE | CO-FOUNDER & CSO

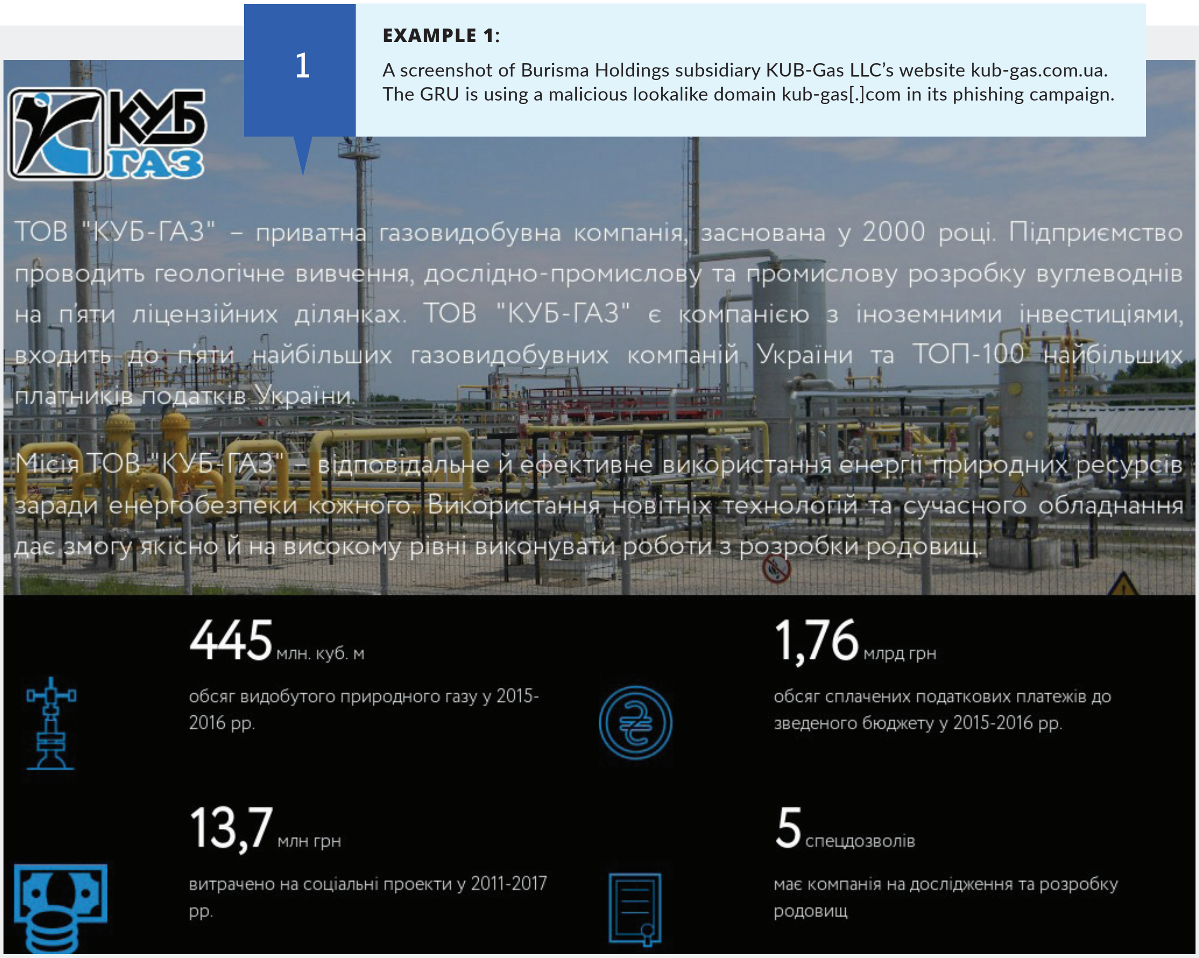
# Campaign Details

Beginning in early November of 2019, the Main Intelligence Directorate of the General Staff of the Russian Army (GRU)[1] launched a phishing campaign targeting Burisma Holdings, a holding company of energy exploration and production companies based in Kiev, Ukraine. The phishing campaign identified is designed to steal email credentials (usernames and passwords) of employees at Burisma Holdings and its subsidiaries and partners.

1

**EXAMPLE 1:**

A screenshot of Burisma Holdings subsidiary KUB-Gas LLC's website kub-gas.com.ua. The GRU is using a malicious lookalike domain kub-gas[.]com in its phishing campaign.



ТОВ "КУБ-ГАЗ" – приватна газовидобувна компанія, заснована у 2000 році. Підприємство проводить геологічне вивчення, дослідно-промислову та промислову розробку вуглеводнів на п'яти ліцензійних ділянках. ТОВ "КУБ-ГАЗ" є компанією з іноземними інвестиціями, входить до п'яти найбільших газовидобувних компаній України та ТОП-100 найбільших платників податків України.

Місія ТОВ "КУБ-ГАЗ" – відповідальне й ефективне використання енергії природних ресурсів заради енергобезпеки кожного. Використання новітніх технологій та сучасного обладнання дає змогу якісно й на високому рівні виконувати роботи з розробки родовищ.

445 млн. куб. м

обсяг видобутого природного газу у 2015-2016 рр.

1,76 млрд грн

обсяг сплачених податкових платежів до зведеного бюджету у 2015-2016 рр.

13,7 млн грн

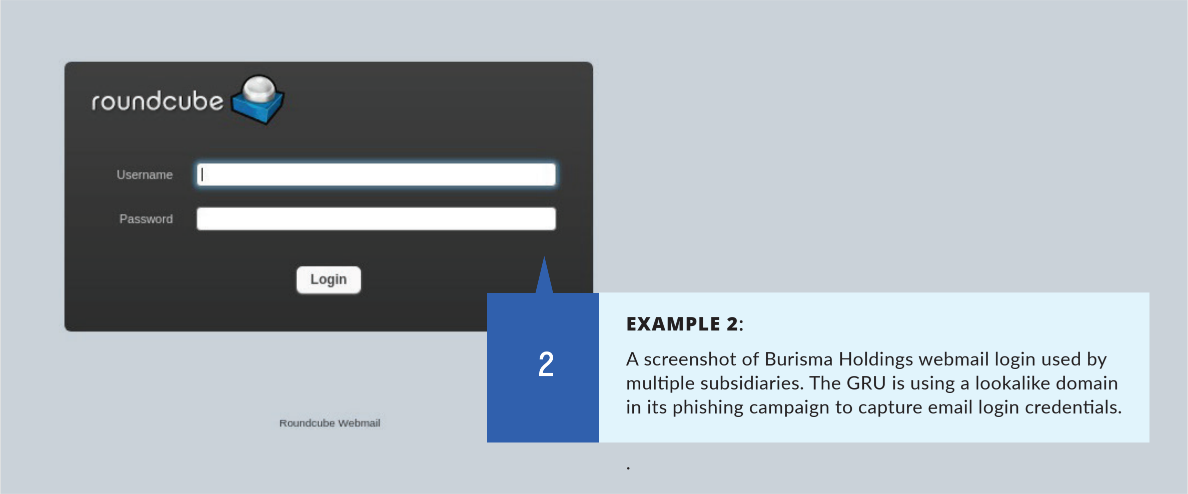
витрачено на соціальні проекти у 2011-2017 рр.

5 спецдозволів

має компанія на дослідження та розробку родовищ

[1] Also referred to as: Pawn Storm, Fancy Bear, Sofacy, Tsar Team, and Strontium. The GRU is known to conduct cyber espionage campaigns, reveal and publicize records previously held privately, and use cyberattacks against those of interest to the Russian government. The GRU has been linked to cyberattacks at the Democratic National Committee in 2016 and the compromise of the World Anti-Doping Agency. The GRU has also been linked to the targeting of European foreign ministries and defense agencies, campaigns for the 2018 U.S. midterm elections, FIFA, and Westinghouse.

Area 1 Security's analysis of the Burisma Holdings email server indicates that it is also used by the following subsidiaries: ALDEA (Aldea Україна), Esko-Pivnich (Еско-Північ), Naftogazopromyslova geologiya, (Нафтогазпромислова геологія), Nadragasvydobuvannya (Надрагазвидобування), Pari (Парі), and Tehnokomservis (Технокомсервіс).

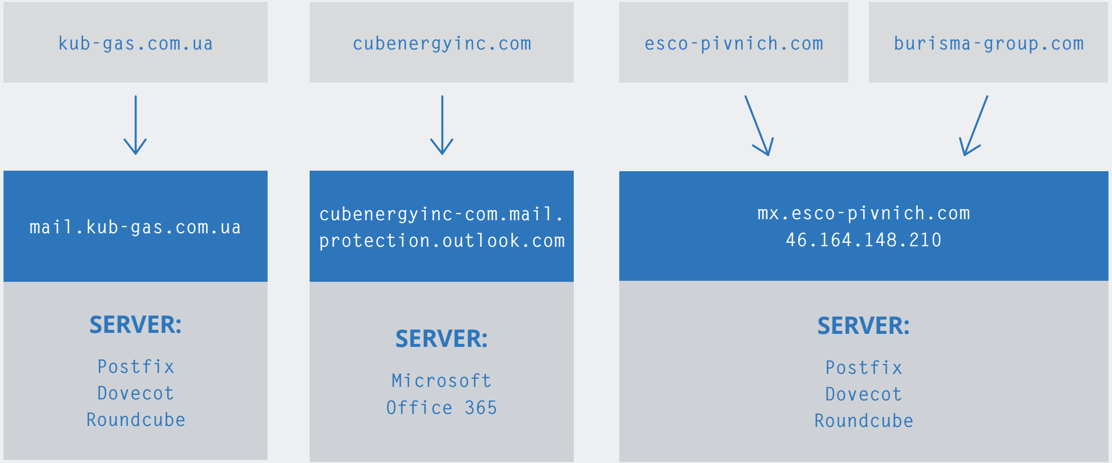


**EXAMPLE 2:**

A screenshot of Burisma Holdings webmail login used by multiple subsidiaries. The GRU is using a lookalike domain in its phishing campaign to capture email login credentials.

.

OVERVIEW OF THE LEGITIMATE EMAIL SERVICES PROVIDING HOSTING FOR THE LEGITIMATE VERSIONS OF THE DOMAINS BELOW:



kub-gas.com.ua → mail.kub-gas.com.ua

**SERVER:**
Postfix
Dovecot
Roundcube

cubenergyinc.com → cubenergyinc-com.mail.protection.outlook.com

**SERVER:**
Microsoft
Office 365

esco-pivnich.com, burisma-group.com → mx.esco-pivnich.com
46.164.148.210

**SERVER:**
Postfix
Dovecot
Roundcube

Since 2016, the GRU has consistently used an assembly line process to acquire and set up infrastructure for their phishing campaigns. Area 1 Security has correlated this campaign against Burisma Holdings with specific tactics, techniques, and procedures (TTPs) used exclusively by the GRU in phishing for credentials. Repeatedly, the GRU uses Ititch, NameSilo, and NameCheap for domain registration; MivoCloud and M247 as Internet Service Providers; Yandex for MX record assignment; and a consistent pattern of lookalike domains.

| GRU CAMPAIGN | MALICIOUS DOMAIN |
|---|---|
| Phishing Burisma Holdings (2020) | cubenergy-my-sharepoint[.]com |
| Phishing George Soros (2019)[2] | soros-my-sharepoint[.]com |
| Phishing U.S. Political Organizations Including the Hudson Institute (2018)[3] | hudsonorg-my-sharepoint[.]com |

Sample of domain lookalikes used by the GRU in phishing campaigns.

The GRU has been a specific actor of interest to Area 1 due to their history of targeting commercial and state organizations. Consequently, Area 1 has been tracking GRU TTPs for several years, and the TTPs utilized in this campaign have been tied to those observed by Area 1 in prior GRU campaigns. This phishing campaign against Burisma Holdings also uses a specific HTTP redirect, attributed to GRU, where non-targeted individuals are sent to the legitimate Roundcube webmail login, while targets who receive the GRU-generated URL are taken to the GRU's malicious phishing Roundcube website.

Area 1 Security has also further connected this GRU phishing campaign to another phishing campaign targeting a media organization founded by Ukraine's President Volodymyr Zelensky.

[2] Poulsen, Kevin. "Russia's Election Hackers Are Back-and Targeting George Soros." The Daily Beast, The Daily Beast Company, 15 July 2019, www.thedailybeast.com/russias-election-hackers-are-backand-targeting-george-soros-and-his-open-society-foundations.

[3] Elizabeth Dwoskin, Craig Timberg. "Microsoft Says It Has Found a Russian Operation Targeting U.S. Political Institutions." The Washington Post, WP Company, 21 Aug. 2018, www.washingtonpost.com/business/economy/microsoft-says-it-has-found-a-russian-operation-targeting-us-political-institutions/2018/08/20/52273e14-a4d2-11e8-97ce-cc9042272f07_story.html.

# Summary

In this campaign the GRU specifically sought the email credentials of employees at Burisma Holdings and its subsidiaries and partners. Phished credentials permit the GRU to masquerade as specific email users and access data contained within email accounts. Access to Burisma Holdings email accounts permits future phishing campaigns, which can be made to appear even more authentic by using observed data and for the GRU to develop Type 2 and Type 3 Business Email Compromise phishing campaigns.

**The GRU campaign against Burisma holdings was successful because it was authentic in three distinct ways:**

## 1 DOMAIN-BASED AUTHENTICITY

The GRU established lookalike domains to appear as legitimate domains used by Burisma Holdings to conduct its business.

| TARGETED ENTITY | RELATIONSHIP TO BURISMA | LEGITIMATE DOMAIN | MALICIOUS DOMAIN |
|---|---|---|---|
| KUB-Gas LLC | Subsidiary of Burisma Holdings | kub-gas.com.ua | kub-gas[.]com |
| KUB-Gas LLC | Subsidiary of Burisma Holdings | mail.kub-gas.com.ua | mail.kub-gas[.]com |
| Esko-Pivnich | Subsidiary of Burisma Holdings | mail.esco-pivnich.com | mail.esco-plvnlch[.]com |
| CUB Energy Inc. | 35% Joint Venture Owner of KUB-Gas LLC | cubenergyinc.com | cubenergy-my-sharepoint[.]com |

Targeted individuals were unable to discern the difference between legitimate domains and those used by the GRU. Also, the GRU ensured reliable phishing delivery by setting up appropriate email sender authentication records using SPF and DKIM.

| MALICIOUS DOMAIN | SPF RECORD | DKIM RECORD |
|---|---|---|
| kub-gas[.]com | "v=spf1 redirect=_spf. yandex.net" | “v=DKIM1; k=rsa; t=s; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADC BiQKBgQDHmyzwHPXNRG0Q2mDIFPR8hfWSLh HMcEqndEbcxqef24gvt0HOFA+8YZC7VZnwH6Tz OofySR1MEh3ssau9iwXy+QVyIDNlQLwzZ8x8qWd HPP8NC/05R+VBDIpnx7blIbPYpt7ClJ/sXLt2tvzLdJ bln P4vABcjGoMYibZ5JGbrwIDAQAB” |
| mail.esco-plvnlch[.]com | "v=spf1 include:spf. privateemail.com ~all" | |
| cubenergy-my-sharepoint[.]com | "v=spf1 include:spf. privateemail.com ~all" | |

## 2 BUSINESS PROCESS AND APPLICATION AUTHENTICITY

The GRU focused on masquerading the same business applications used by Burisma Holdings, such as the Roundcube webmail login and SharePoint.  Burisma Holdings employees’ familiarity of these applications in their daily business ensured the success of the phishing campaign.

## 3 PARTNER AND SUPPLY CHAIN AUTHENTICITY

Targeting multiple subsidiaries of Burisma Holdings, the GRU was able to successfully phish multiple angles of the same target, increasing the likelihood of launching Type 2 and Type 3 BEC phishing campaigns.

**All cyber actors have goals, and they figure out what works to guarantee that they are successful with the least resistance possible. What works to lure unsuspecting targets and bypass cybersecurity defenses is used repeatedly. The Burisma Holdings campaign is yet another example of the phishing playbook being applied to great effect.**

**The success of phishing relies on authenticity. The GRU has applied verisimilitude in extensive masquerading of common business tools and productivity applications to steal account credentials, gain access to internal systems and data, impersonate employees through the unauthorized use of their accounts, and manipulate outcomes successfully.**