

Countering hack-for-hire groups

blog.google/threat-analysis-group/countering-hack-for-hire-groups/

Shane Huntley

June 30, 2022


THREAT ANALYSIS GROUP

Countering hack-for-hire groups

Jun 30, 2022 · 6 min read



Shane Huntley
Director, Threat Analysis Group

 Share

As part of TAG's mission to counter serious threats to Google and our users, we've published analysis on a range of persistent threats including government-backed attackers, commercial surveillance vendors, and serious criminal operators. Today, we're sharing intelligence on a segment of attackers we call hack-for-hire, whose niche focuses on compromising accounts and exfiltrating data as a service.

In contrast to commercial surveillance vendors, who we generally observe selling a capability for the end user to operate, hack-for-hire firms conduct attacks themselves. They target a wide range of users and opportunistically take advantage of known security flaws when undertaking their campaigns. Both, however, enable attacks by those who would otherwise lack the capabilities to do so.

Threat Analysis Group

As part of TAG's mission to counter serious threats to Google and our users, we've published analysis on a range of persistent threats including government-backed attackers, commercial surveillance vendors, and serious criminal operators. Today, we're sharing intelligence on a segment of attackers we call hack-for-hire, whose niche focuses on compromising accounts and exfiltrating data as a service.

In contrast to commercial surveillance vendors, who we generally observe selling a capability for the end user to operate, hack-for-hire firms conduct attacks themselves. They target a wide range of users and opportunistically take advantage of known security flaws when undertaking their campaigns. Both, however, enable attacks by those who would otherwise lack the capabilities to do so.

We have seen hack-for-hire groups target human rights and political activists, journalists, and other high-risk users around the world, putting their privacy, safety and security at risk. They also conduct corporate espionage, handily obscuring their clients' role.

To help users and defenders, we will provide examples of the hack-for-hire ecosystem from India, Russia, and the United Arab Emirates and context around their capabilities and persistence mechanisms.

How Hack-For-Hire Operations Work

The hack-for-hire landscape is fluid, both in how the attackers organize themselves and in the wide range of targets they pursue in a single campaign at the behest of disparate clients. Some hack-for-hire attackers openly advertise their products and services to anyone willing to pay, while others operate more discreetly selling to a limited audience.

For example, TAG has observed Indian hack-for-hire firms work with [third party private investigative services](#) — intermediaries that reach out for services when a client requires them — and provide data exfiltrated from a successful operation. This is detailed in depth in [today's Reuters investigation](#) into the Indian hack-for-hire ecosystem. We have also observed Indian hack-for-hire firms work with freelance actors not directly employed by the firms themselves.

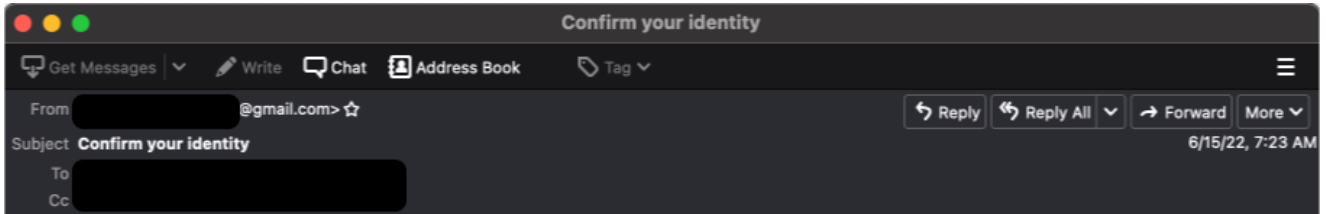
The breadth of targets in hack-for-hire campaigns stands in contrast to many government-backed operations, which often have a clearer delineation of mission and targets. A recent campaign from an Indian hack-for-hire operator was observed targeting an IT company in Cyprus, an education institution in Nigeria, a fintech company in the Balkans and a shopping company in Israel.

Recent Hack-for-Hire Campaigns

India

Since 2012, TAG has been tracking an interwoven set of Indian hack-for-hire actors, with many having previously worked for Indian offensive security providers [Appin](#) and [Belltrox](#).

One cluster of this activity frequently targets government, healthcare, and telecom sectors in Saudi Arabia, the United Arab Emirates, and Bahrain with credential phishing campaigns. These credential phishing campaigns have ranged from targeting specific government organizations to AWS accounts to Gmail accounts.



Hello there,

You have recently changed password of your AWS account.

Please verify your account to confirm the identity via below link:

<https://aws.amazon.com/confirm-identity/500244512004874>

The following are some common reasons for unintentional or irregular activities:

- Unauthorized or unexpected resources activity - An unpatched Amazon Elastic Compute Cloud (EC2) instance could be infected and become a botnet agent.
- Exposed credentials or access keys.
- Unintentional abuse - An overly aggressive web crawler might be classified as a denial-of-service attack by some internet sites.
- Secondary abuse - An end user of a service provided by an AWS customer might post malware files on a public Amazon S3 bucket.
- False complaints - Sometimes internet users mistakenly report legitimate activities as abuse.

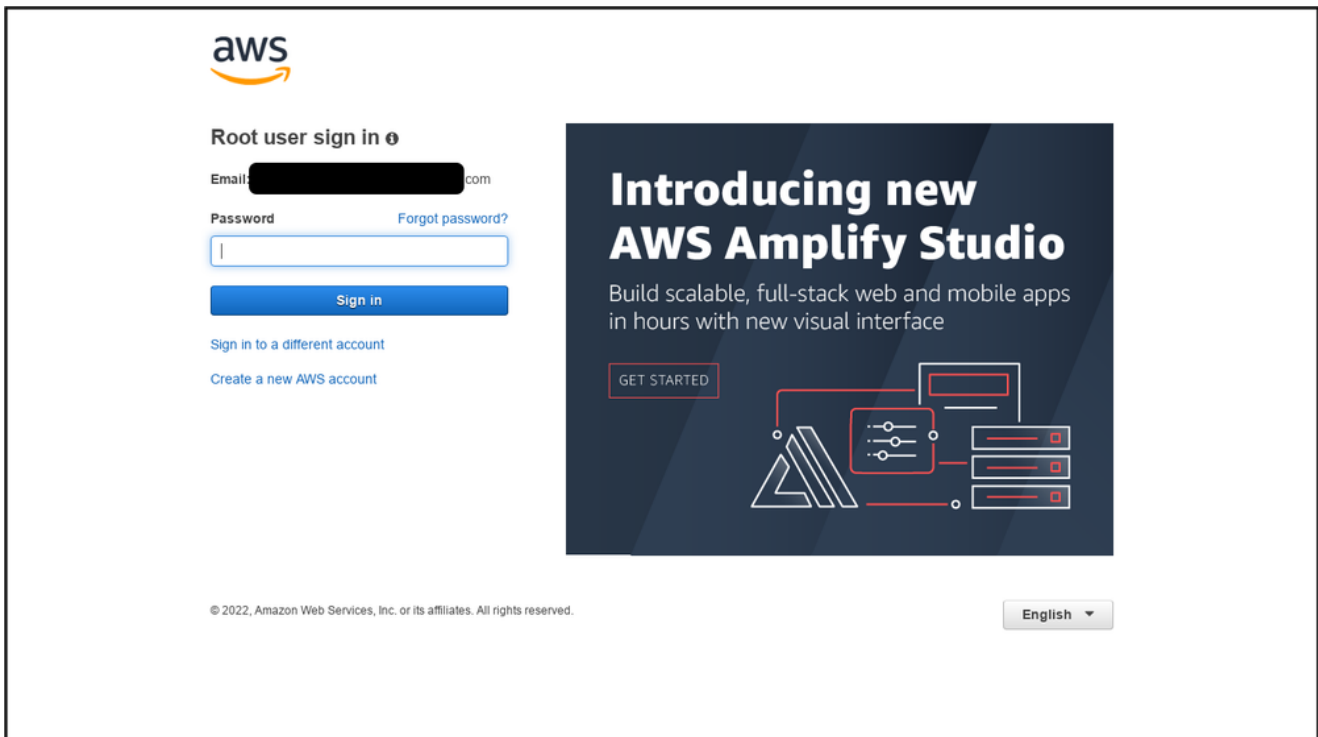
I appreciate your patience while we work on this case.

We value your feedback. Please share your experience by rating this correspondence using the AWS Support Center link at the end of this correspondence. Each correspondence can also be rated by selecting the stars in top right corner of each correspondence within the AWS Support Center.

Best regards,

(v)

Sample AWS phishing email



Sample AWS phishing page

TAG has linked former employees of both Appin and Belltrox to Rebsec, a new firm that openly advertises corporate espionage as an offering on its company website.



CORPORATE ESPIONAGE

Espionage Incarnate is the dissemble or pattern of spying to gain secret entropy on a government or a patronage competitor. We can amend approximately mutual gestures of corporate espionage as:

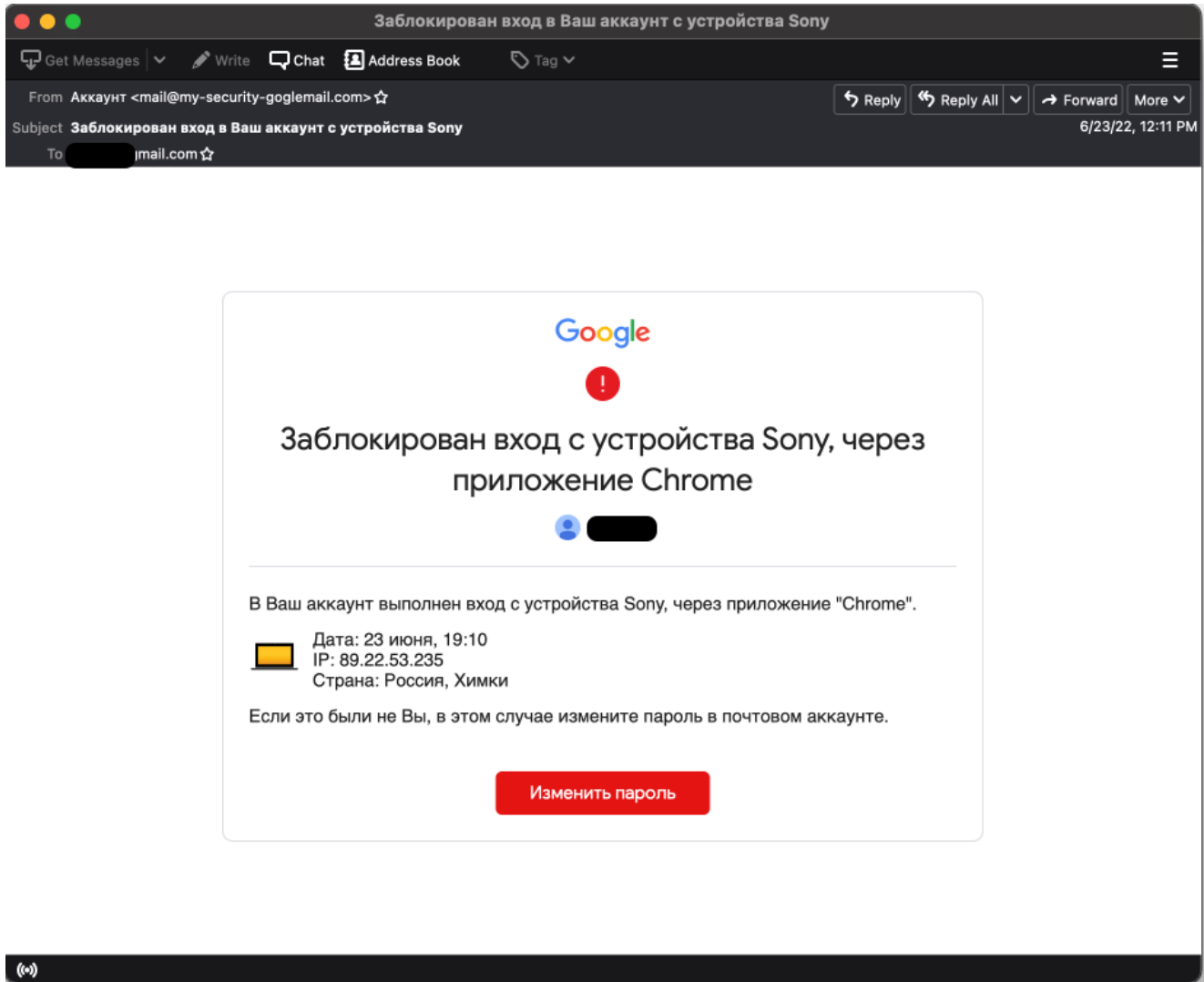
- Private entropy has become public
- Documents or conversations found exclusively in your private federal agency are being referenced by others.
- Secret troupe information, formulas, or schematics have been implemented by other companies.

Rebsec's offerings as per the company's website

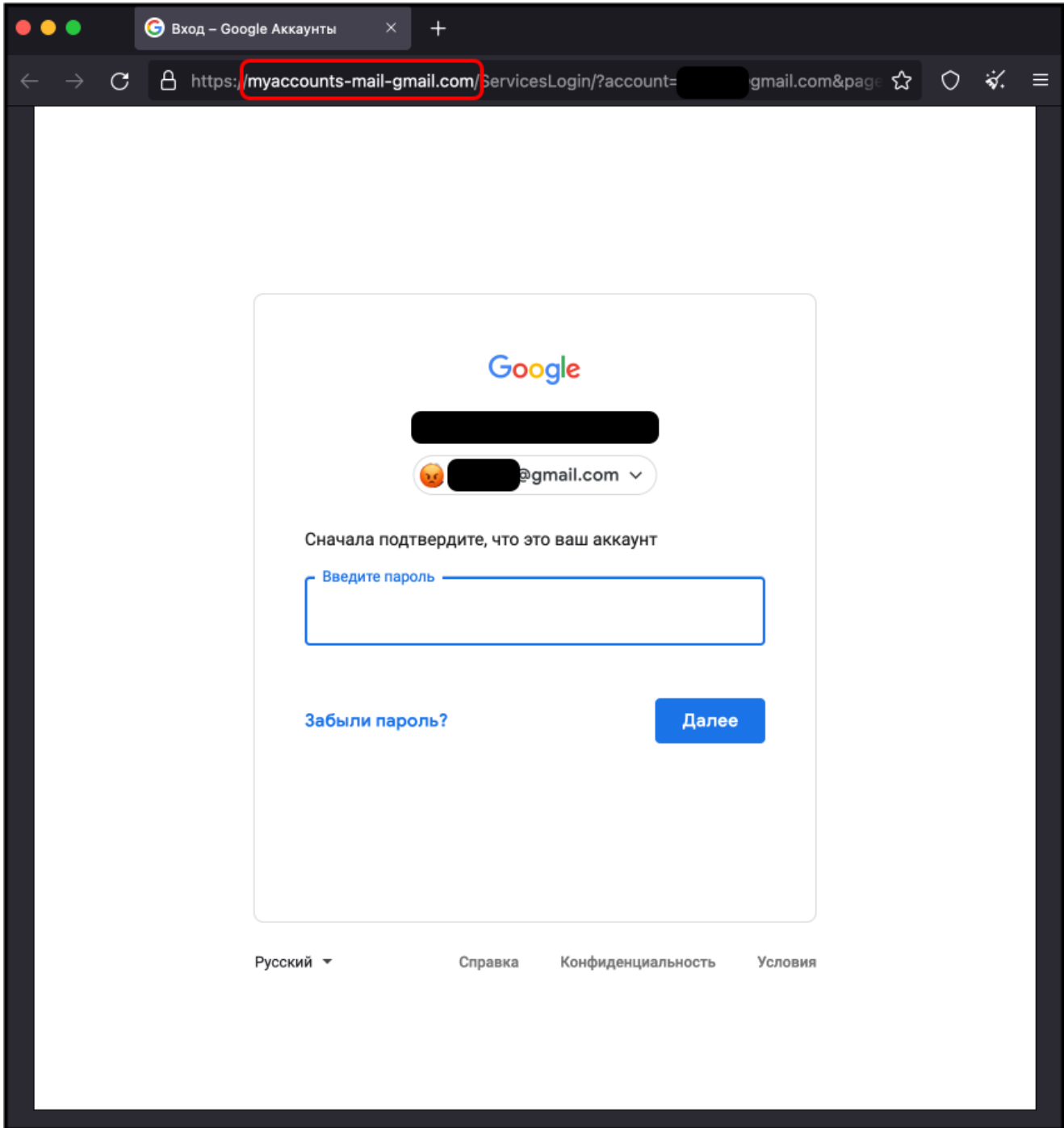
Russia

While investigating a 2017 credential phishing campaign that targeted a prominent Russian anti-corruption journalist, we discovered the Russian attacker targeting other journalists, politicians across Europe, and various NGOs and non-profit organizations. But what stuck out during this investigation was the breadth of targeting, which also included individuals that had no affiliation with the selected organizations, and appeared to be regular, everyday citizens in Russia and surrounding countries. This hack-for-hire actor has been publicly referred to as 'Void Balaur'.

These campaigns were similar regardless of target, consisting of a credential phishing email with a link to an attacker-controlled phishing page. The lures ranged from fake Gmail and other webmail provider notifications to messages spoofing Russian government organizations. After the target account was compromised, the attacker generally maintained persistence by granting an OAuth token to a legitimate email application like Thunderbird or generating an App Password to access the account via IMAP. Both OAuth tokens and App Passwords are revoked when a user changes their password.











Russian hack-for-hire phishing email



Russian hack-for-hire phishing site

During our early investigation, TAG discovered the attacker's public website (no longer available) advertising account hacking capabilities for email and social media services. The site claimed to have received positive reviews on Russian underground forums such as Dublikat and Probiv.cc. Over the past five years, TAG has observed the group targeting accounts at major webmail providers like Gmail, Hotmail, and Yahoo! and regional webmail providers like abv.bg, mail.ru, inbox.lv, and UKR.net.

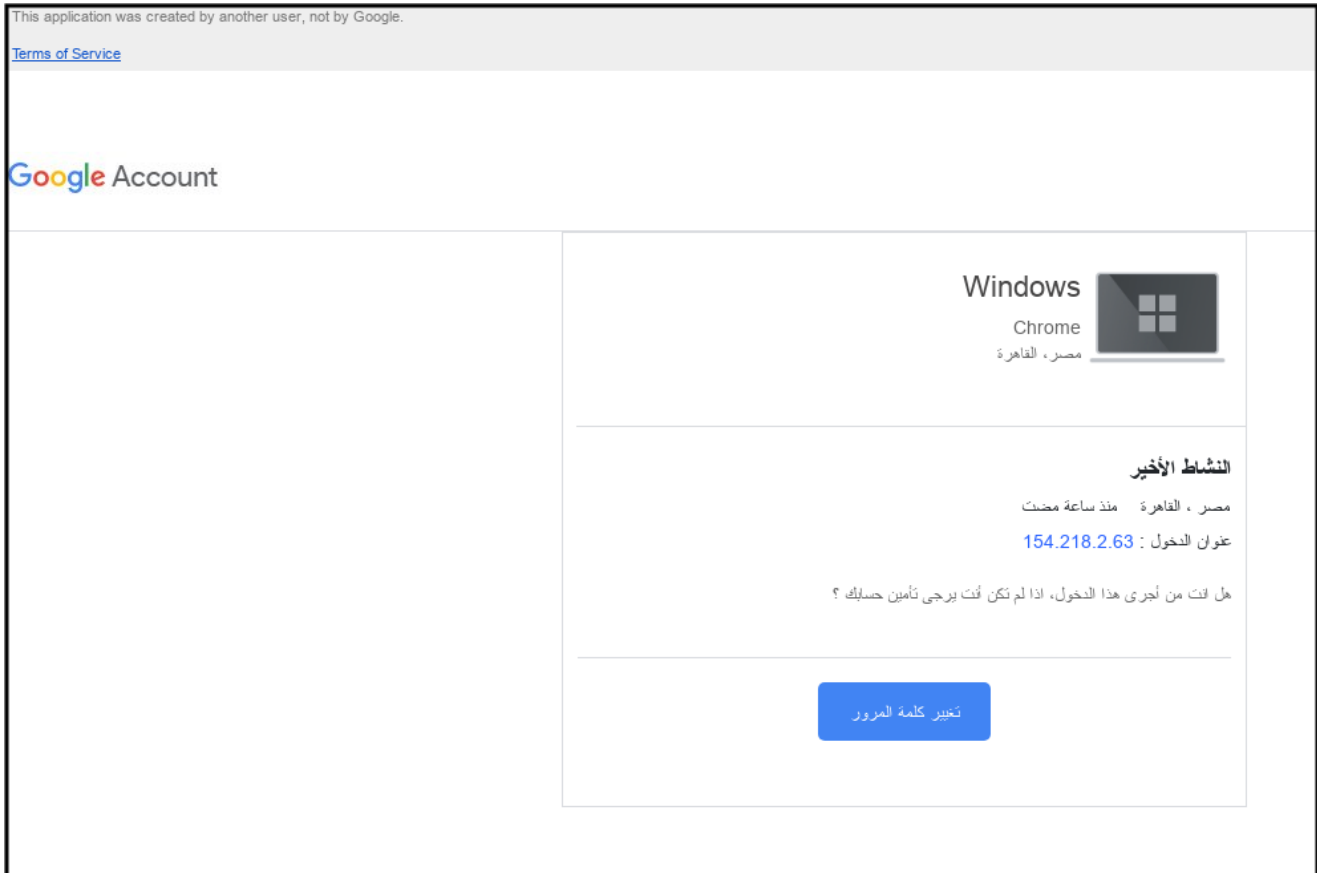
 YAHOO.COM Archive of Yahoo mail ₹19990 Prepay half From 5 minutes to 5 days <input type="button" value="TO ORDER"/>	 CORPORATIV.MAIL Hacking Corporate Mail ₹_OT 14990 Password does not change From 5 minutes to 5 days <input type="button" value="TO ORDER"/>	 VKONTAKTE.COM Hacking the VK.COM page ₹9990 Password does not change From 5 minutes to 5 days <input type="button" value="TO ORDER"/>	 ODNOKLASSNIKI.RU Hacking OK.RU ₹9990 Password changes From 5 minutes to 5 days <input type="button" value="TO ORDER"/>
 INSTAGRAM.COM Hacking the INSTAGRAM page ₹19990 Password does not change From 5 minutes to 5 days <input type="button" value="TO ORDER"/>	 FACEBOOK.COM Hacking the FACEBOOK page ₹19990 Password does not change From 5 minutes to 5 days <input type="button" value="TO ORDER"/>	 MAILS, SOCIAL NETWORK 100% Content Pumping ₹69990 Full prepayment 1 to 7 days <input type="button" value="TO ORDER"/>	 LEARNING TRAINING Mail, social network ₹24990 Full prepayment We bring to the result <input type="button" value="TO ORDER"/>

Pricing list from hacknet-service.com in 2018

United Arab Emirates

TAG is also tracking a hack-for-hire group now based in the United Arab Emirates that is mostly active in the Middle East and North Africa. They have primarily targeted government, education, and political organizations including Middle East focused NGOs in Europe and the Palestinian political party Fatah. [Amnesty International](#) has also reported on their campaigns.

The group commonly uses Google or OWA password reset lures to steal credentials from targets, often using the MailJet or SendGrid API to send phishing emails. Unlike many hack-for-hire actors that use open source phishing frameworks like [Evilginx](#) or [GoPhish](#), this group uses a custom phishing kit that utilizes [Selenium](#), a self described 'suite of tools for automating web browsers.' Previously described by Amnesty, this phishing kit has remained under active development over the past five years.



Google Security Alert phishing page

After compromising an account, the actor maintains persistence by granting themselves an OAuth token to a legitimate email app like Thunderbird, or by linking the victim Gmail account to an attacker-owned account on a third-party mail provider. The attacker would then use a custom tool to download the mailbox contents via IMAP.

This group also has links to the original developers of H-Worm, also known as njRAT. In 2014, Microsoft filed a civil suit against the developer, Mohammed Benabdellah, for the development and dissemination of H-Worm. Benabdellah, who also goes by the moniker Houdini, has been actively involved in the day-to-day development and operational deployment of the credential phishing capabilities used by this group since its inception.

Protecting Our Users

As part of our efforts to combat serious threat actors, we use results of our research to improve the safety and security of our products. Upon discovery, all identified websites and domains were added to Safe Browsing to protect users from further harm. We encourage any high risk user to enable Advanced Protection and Google Account Level Enhanced Safe Browsing and ensure that all devices are updated. Additionally, our CyberCrime Investigation Group is sharing relevant details and indicators with law enforcement.

TAG is committed to sharing our findings as a way of raising awareness with the security community, and with companies and individuals that might have been targeted. We hope that improved understanding of the tactics and techniques will enhance threat hunting capability and lead to stronger user protections across the industry.

With contributions from Winnona DeSombre

Indicators of Compromise

UAE hack-for-hire Group Domains:

- myproject-login[.]shop
- mysite-log[.]shop
- supp-help[.]me
- account-noreply3[.]xyz
- goolge[.]ltd
- goolge[.]help
- account-noreply8[.]info
- account-server[.]xyz
- kcynvd-mail[.]com
- mail-goolge[.]com
- kcynve-mail[.]com

Indian hack-for-hire Group Domains:

- dtiwa.app[.]link
- share-team.app[.]link
- mipim.app[.]link
- processs.app[.]link
- aws-amazon.app[.]ink
- clik[.]sbs
- loading[.]sbs
- userprofile[.]live
- requestservice[.]live
- unt-log[.]com
- webtech-portal[.]com
- id-apl[.]info
- rmanage-icloud[.]com
- apl[.]onl
- go-gl[.]io

Russian hack-for-hire Group Domains:

- login-my-oauth-mail[.]ru

- [oauth-login-accounts-mail\[.\]ru](#)
- [my-oauth-accounts-mail\[.\]ru](#)
- [login-cloud-myaccount-mail\[.\]ru](#)
- [myaccounts-auth\[.\]ru](#)
- [security-my-account\[.\]ru](#)
- [source-place-preference\[.\]ru](#)
- [safe-place-smartlink\[.\]ru](#)
- [safe-place-experience\[.\]ru](#)
- [preference-community-place\[.\]ru](#)

POSTED IN:

[Threat Analysis Group](#)