



Void Balaur

Tracking a Cybermercenary's Activities

Feike Hacquebord

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

Feike Hacquebord

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963 – 2017)

Contents

6

The Starting Point of Our Investigation

10

Void Balaur in the Underground

17

Void Balaur's Targets

22

Targets with Access to a Large Amount of Private Information

24

Cryptocurrency Account Phishing

26

Working Times of Void Balaur

29

Malware Activities of Void Balaur

31


Overlap with Pawn Storm

33

Outlook for the Cybermercenary Industry

34

Defending Against Cybermercenary Attacks



The internet brings new and innovative technologies and services, yet it also serves as the battleground for malicious actors who seek to attack or steal information from organizations and individuals. To fulfill the demands of offensive cyberattacks, an industry has emerged that can sell tools, services and training to governments, corporations, organized crime and even wealthy individuals. Cybermercenaries are part of this industry, and in return for their services, they get monetary rewards or other benefits.

The problems that these cybermercenaries cause are getting more profound and are gaining more attention in recent years. While the services of cybermercenaries may theoretically be of use in the fight against terrorism and organized crime in well-established jurisdictions that have democratic control mechanisms and export controls in place, in practice, we see that the services of these cybermercenaries are being used to attack political opposition, dissidents, journalists, and human rights activists.^{1, 2}

Offensive tools are used to spy on these targets — and this can have devastating consequences. For example, some politicians and journalists who saw no other option than to flee their home country became the target of aggressive cyberattacks around the same time they decided to go into exile.³ These attacks might have been the final straw that forced them to flee the country.

The problem with selling cybermercenary services goes deep, even when they are intended for use in narrow, ultra-targeted campaigns. Offensive tools and methodologies may become widely available when advanced malware and knowledge of vulnerabilities are stolen in hacks and then leaked. For example, in 2015, a well-known hacker-for-hire organization in Italy became the victim of a hack and its tools were made available to anybody who wanted to learn how to use them.⁴

To mitigate the risks to society that these cybermercenaries' actions cause, there have been calls to regulate the cybermercenary industry with international agreements and laws.^{5, 6} These proposals, however, are difficult to implement because countries with different points of view would have to come to an agreement about what such regulations would look like and how it gets enforced. Even when worldwide regulations are in place, there will still be large gray areas where all kinds of actors can offer their services. Moreover, nations might view cybermercenaries that have headquarters in their own country as a national asset. Not only can these cybermercenaries be used for attacks that are aligned with the interests of their home country, but they can also be used as a political tool for foreign policy, just like conventional weapons.

This research looks into a threat actor group that can be considered a cybermercenary, but one that prefers to stay in the shadows. To our knowledge, this hacker-for-hire group does not operate out of a physical building, nor does it have a shiny prospectus that describes its services. The group does not try to wriggle out of a difficult position by justifying its business, nor is it involved in lawsuits against anybody attempting to report on their activities. Instead,

this group is quite open about what it does: breaking into email accounts and social media accounts for money. This threat actor is also involved in selling highly sensitive personal data like cell tower phone logs, passenger flight records, banking data, and passport details.

The group advertises its services in Russian-speaking underground forums such as Prodiv, where cybercriminals gather to do business with each other. At first glance, it seems that this hacker-for-hire mostly has customers whose main motive is financial gain. However, we can also attribute significant political attacks against human rights activists and politicians in about a dozen countries to this group.

The Russian-speaking threat actor calls itself Rockethack. While we do not know this group's whereabouts, we have a good knowledge of its working hours. We suspect that Rockethack possesses detailed knowledge of how telecommunications and ISPs work in Russia and neighboring countries.

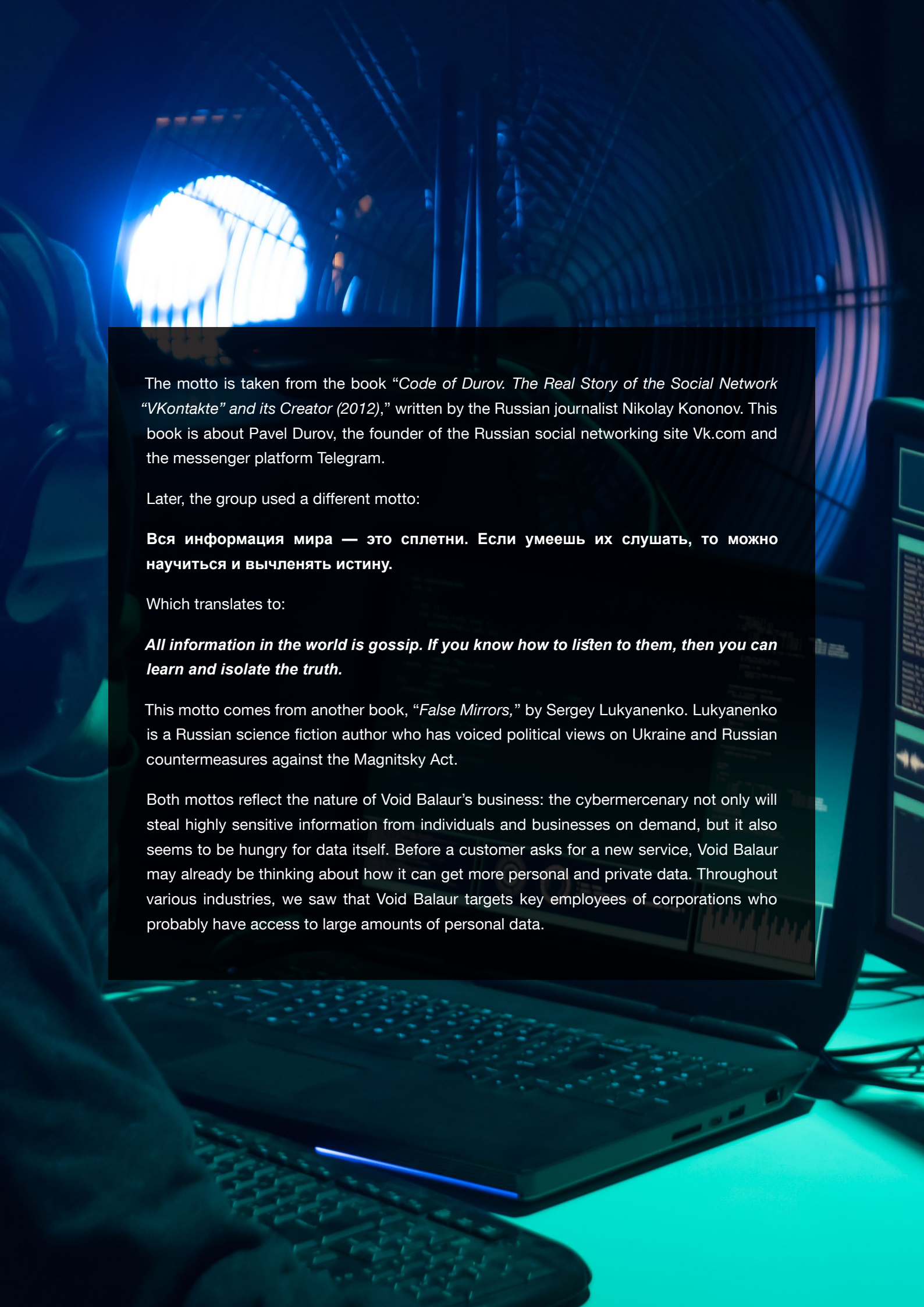
Rockethack has a massive associated intrusion set with thousands of indicators, which we are tracking under the name Void Balaur. We chose this name because Balaur is a monstrous multiheaded legendary creature in Eastern European folklore. It is fittingly symbolic for the multiple purposes for which Void Balaur is being hired: spying on a local shop in Moscow, on journalists, human right activists, politicians, scientists, doctors working in a few dozen IVF clinics, genomics and biotechnology companies, Telco engineers with deep knowledge of mobile operators' networks, and business aviation companies. Void Balaur also dabbles in corporate espionage, is suspected to be selling data to cybercriminals in order to fight their fellow cybercriminals over disputes, and has conducted attacks against cryptocurrency users.

We have uncovered more than 3,500 of the group's targets, some of whom have suffered long-lasting and repeated attacks. Our research revealed a clear picture: Void Balaur goes after the most private and personal data of businesses and individuals then sells that data to whomever wants to pay for it. This business model is perhaps best illustrated by the mottos the group has been using on the now defunct website, rockethack[.]me. The actor group used a couple of remarkable mottos in this website. One was:

Деньги не главное в свободном интернете. Главное – власть, которая принадлежит тому, кто контролирует потоки информации.

This translates to:

Money is not the main thing on the free internet. The main thing is the power that belongs to the one who controls the flow of information.



The motto is taken from the book “*Code of Durov. The Real Story of the Social Network “VKontakte” and its Creator (2012)*,” written by the Russian journalist Nikolay Kononov. This book is about Pavel Durov, the founder of the Russian social networking site Vk.com and the messenger platform Telegram.

Later, the group used a different motto:

Вся информация мира — это сплетни. Если умеешь их слушать, то можно научиться и вычленять истину.

Which translates to:

All information in the world is gossip. If you know how to listen to them, then you can learn and isolate the truth.

This motto comes from another book, “*False Mirrors*,” by Sergey Lukyanenko. Lukyanenko is a Russian science fiction author who has voiced political views on Ukraine and Russian countermeasures against the Magnitsky Act.

Both mottos reflect the nature of Void Balaur’s business: the cybermercenary not only will steal highly sensitive information from individuals and businesses on demand, but it also seems to be hungry for data itself. Before a customer asks for a new service, Void Balaur may already be thinking about how it can get more personal and private data. Throughout various industries, we saw that Void Balaur targets key employees of corporations who probably have access to large amounts of personal data.

The Starting Point of Our Investigation

While many countries around the world were in lockdown during March 2020 to combat the rapidly increasing Covid-19 infection numbers, we were contacted by a long-time target of Pawn Storm, an Advanced Persistent Threat (APT) group also known as APT28.⁷ This person told us that his wife, who works as a scientist, had received a dozen phishing emails on her Gmail account.

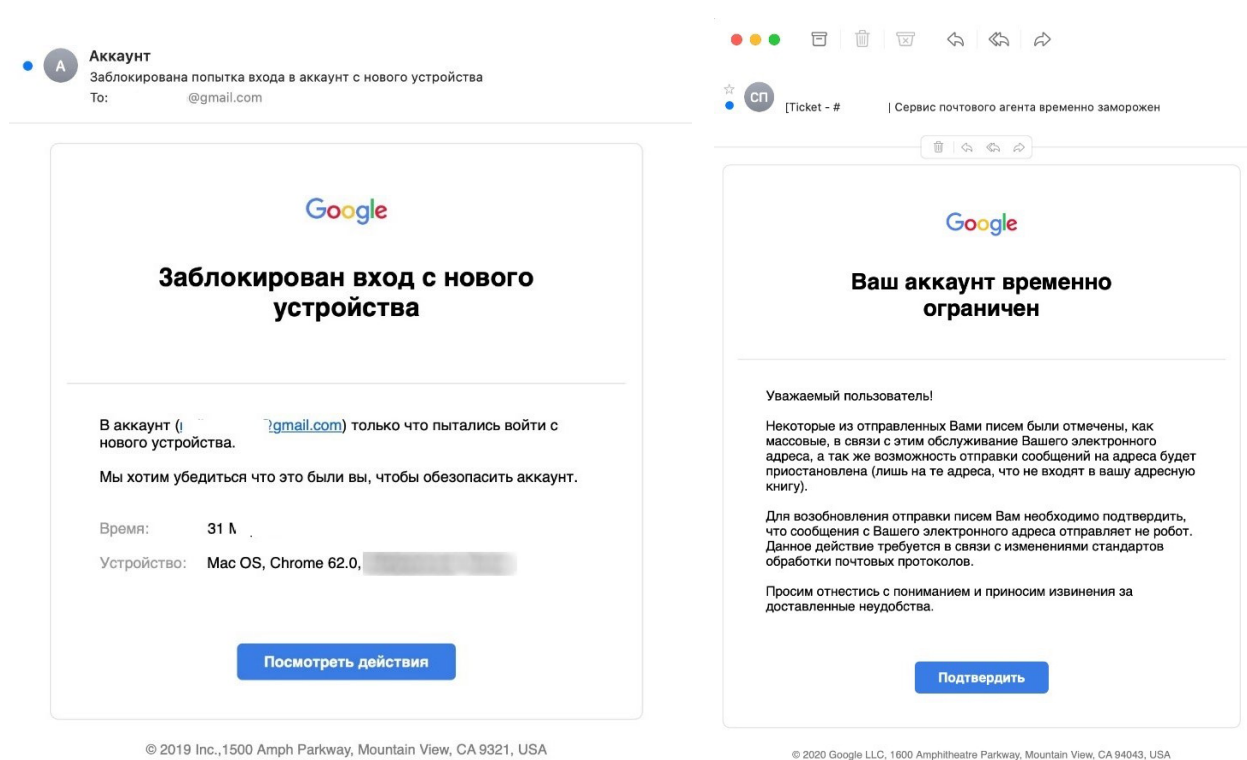


Figure 1. Gmail phishing emails that the spouse of a long-time Pawn Storm target received in 2020



Figure 2. Credential phishing email stating that the recipient must pay off a debt and must appear in court

We were immediately alarmed: this would not be the first time Pawn Storm targeted the spouses of their actual targets.⁸ However, a closer look at the phishing emails did not show any of the usual indicators and modus operandi that we have attributed to Pawn Storm during the intensive research we have been conducting on the group since 2014. The phishing emails, which the spouse received in March 2020, did not point to Pawn Storm, but they did lead us to another attribution set that we later named Void Balaur.

In this attribution set, we found the domain name rockethack[.]me, which belonged to a hacking service that advertises in underground forums such as Probiv under the name “Rockethack.” Throughout the rest of this report, we will refer to this hacking service as Void Balaur.

Void Balaur offers services for hacking into the email mailboxes of several email providers and social media accounts for money (and possibly other benefits). For some email providers like rambler.ru and mail.ru, the group offers services at a premium rate where complete copies of mailboxes are stolen without any user interaction. We have no reason to believe that the latter is not a real business offering. This means that in some cases, Void Balaur can access mailboxes without the user noticing it. How they do this will be discussed in a later section.

| Domain | Registrant | Description |
|---------------------------------------|-------------------|---------------|
| 27g4dwjallqnzu0[.]space | Privacy protected | Spam URL |
| account-googl[.]com | poxxpoz@pm.me | Sender domain |
| bflqj2xmpbwqkzpwg[.]fun | Privacy protected | Spam URL |
| izwg17taoz9noedve[.]xyz | Privacy protected | Spam URL |
| myaccount.mail.sessionverify.com[.]ru | Privacy protected | Phishing site |
| oapjiyfybhj0jszll[.]fun | Privacy protected | Spam URL |
| wnppid4qunpuwuvqk[.]fun | Privacy protected | Spam URL |
| yen9y2flnrcbwsvy9[.]fun | Privacy protected | Spam URL |

Table 1. Indicators of credential phishing spam sent to the spouse of a long-term APT28 target in early 2020. For one of the sender domains, privacy protection was lifted in 2021

Table 1 lists some of the indicators that we extracted from the phishing emails that were sent to the spouse of the long-term Pawn Storm target. We can correlate these indicators in a straightforward manner to the now-expired domain rockethack[.]me using a couple of steps. We explain this method of pivoting in Appendix A.

In addition, we can relate the indicators to a collection of IP addresses. A small set of these IP addresses are shown in Tables 2 and 3.

| IP address | First accessed | Last accessed | Description |
|-----------------|----------------|---------------|--|
| 139.60.163[.]29 | Oct 12, 2017 | Aug 8, 2018 | Phishing and web attacks ⁹ |
| 139.60.163[.]34 | Oct 10, 2017 | Sep 19, 2018 | Phishing domains |
| 139.60.163[.]35 | Nov 20, 2017 | Mar 15, 2018 | Phishing domains, rockethack[.]me pDNS |
| 139.60.163[.]38 | Nov 9, 2017 | Feb 5, 2019 | Phishing domains |
| 139.60.163[.]43 | Apr 21, 2018 | Jun 22, 2018 | Phishing domains |
| 139.60.163[.]53 | Oct 19, 2018 | Dec 19, 2020 | Hosts rockethack[.]me on port 443 |
| 139.60.163[.]59 | May 8, 2018 | Jun 22, 2018 | Phishing domains |

Table 2. Neighboring IP addresses related to Void Balaur

By pivoting using passive DNS, the whois data of domain names, historic SSL certificates, and historic internet scan data, we can make correlations between rockethack[.]me and a lot of other hostnames and IP addresses.

| IP address | Hostname | First accessed | Last accessed | Target |
|-----------------|---------------------------|----------------|---------------|------------------------------------|
| 139.60.163[.]34 | mail.mfa.tj.task.ru[.]net | Jan 8, 2018 | Jan 8, 2018 | MFA |
| 139.60.163[.]34 | e.mail.ru.bin.ru[.]com | Dec 9, 2017 | Nov 1, 2018 | General |
| 139.60.163[.]29 | mail-support[.]info | Oct 20, 2017 | Dec 25, 2017 | Uzbekistan Incidents ¹⁰ |
| 23.88.228[.]248 | exmo[.]jms | May 10, 2018 | Apr 12, 2019 | Cryptocurrency |
| 23.88.228[.]248 | diamondaero-amocrm[.]ru | Sep 4, 2018 | Sep 2, 2019 | Business aviation |
| 23.88.228[.]248 | m-bizavclub[.]com | Aug 19, 2018 | Aug 18, 2019 | Business aviation |

Table 3. A small selection of domains in the large intrusion set of Void Balaur

Table 3 suggests that the targets of Void Balaur are quite diverse. We see hostnames that look like generic phishing hostnames, a domain name that resembles a well-known cryptocurrency exchange, two domains that are related to business aviation companies in Russia, and a domain that was mentioned in a report by eQualitie on notable attacks against human right activists in Uzbekistan.¹¹

The next sections will show that these apparent low-confidence relations are not a coincidence, but part of Void Balaur's long-term campaigns. We will show that Void Balaur is not only into hacking email mailboxes but is also in the business of selling the sensitive private information of its targets. This includes cell tower log data, passport details, SMS messages, and more. In addition, Void Balaur appears to target many organizations and individuals that are likely to have access to highly sensitive data on people.

Void Balaur in the Underground

The earliest reference to Void Balaur we could find in underground forums dates back to September 8, 2017. On that day, complaints about spam advertising Void Balaur's services (under the name Rockethack) were posted on the underground forum exploit.in. The actual contents of the spam message from 2017 stated that Void Balaur had already been selling its services via resellers in the past, so it is likely that Void Balaur was in the hacker-for-hire business before 2017. This corresponds with digital traces we were able to find that pointed to the group's activities in September 2015 (see Appendix C).

It took another six months before Void Balaur started placing paid advertisements in underground forums like Darkmoney and Probiv. Probiv, which was established in 2014, acts as an underground marketplace where malicious actors gather to offer specialized services mostly aimed at providing access to data, making it an ideal place for Void Balaur to advertise. Darkmoney, meanwhile, is an underground forum for carders. Void Balaur also advertised their services on Tenec, an underground forum specializing in monetizing stolen credentials, and Dublikat — yet another underground forum.

The feedback that Void Balaur receives on underground forums is unanimously positive. Posters mention that the hacking service delivers the requested information on time, while others commented positively on the quality of the delivered information from mailboxes. Yet others posted about passport details they had requested.

To our knowledge, Void Balaur has never advertised in underground forums that were not Russian language-oriented. However, there used to be a website on rockethack[.]me that was registered on February 21, 2018 and was available on its bare IP address 139.60.163[.]53 until at least December 2020. On the website, Void Balaur listed services such as hacking into mailboxes or flooding them with spam, distributed denial-of-service (DDoS) attacks, and flooding phone numbers (in Commonwealth of Independent States or CIS countries only).

| Email provider | Amount in March 2021 (Russian Rubles) | Amount in September 2017 (Russian Rubles) |
|--|---------------------------------------|---|
| Gmail | > 40,000 (US\$550) | > 25,000 (US\$344\$) |
| Protonmail | > 50,000 (US\$688) | - |
| Mail.ru | 10,000 (US\$138) | 4,000 (US\$55) |
| Rambler.ru | 12,000 (US\$165) | 4,000 (US\$55) |
| Rambler.ru (no hack) | - | 60,000 (US\$826) |
| Yandex.ru | 12,000 (US\$165) | ,5000 (US\$69) |
| Yandex.ru (no hack) | > 20,000 (US\$275) | > 30,000 (US\$413) |
| Vk.com | 10,000 (US\$138) | 8,000 (US\$110) |
| Vk.com (hijacking without password change) | > 20,000 (US\$275) | > 80,000 (US\$1,101) |
| Telegram | 150,000 (US\$2,064) | - |
| Corporate email | > 30,000 (US\$413) | >10,000 (US\$138) |

Table 4. Starting prices of Void Balaur’s services in Russian Rubles as advertised on Proбив. We added equivalent US Dollar amounts based on the exchange rate on September 14, 2021

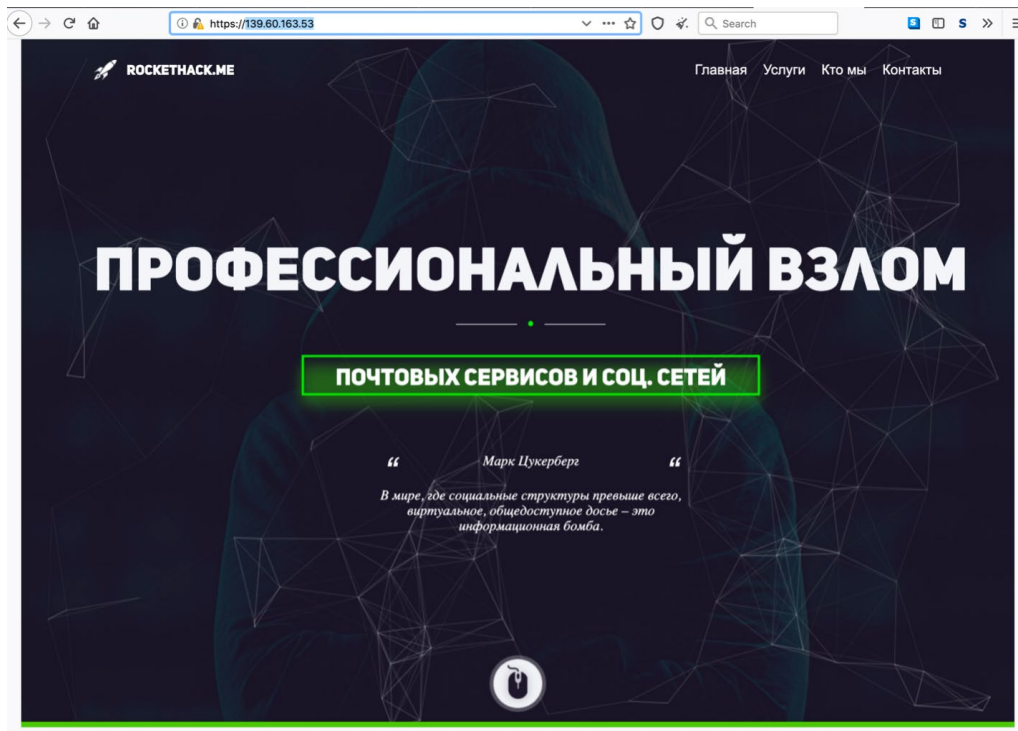


Figure 3. The website of Void Balaur (under the name Rockethack) in 2020 when it was still available on its bare IP address. At the time we took a screenshot, the website had a motto in Russian that is attributed to Mark Zuckerberg, the CEO and founder of Facebook. We have not been able to verify the authenticity of this quote.

The screenshot displays the website's offerings, categorized into 'НАШИ УСЛУГИ' (Our Services). It is divided into two main sections: 'ПРЕДОСТАВЛЕНИЕ ДОСТУПА' (Access Provision) and 'УСЛОЖНЕНИЕ ДОСТУПА' (Access Complication).

ПРЕДОСТАВЛЕНИЕ ДОСТУПА (Access Provision):

| | |
|---------------------------|--------------|
| OK.RU | 15 000 P. |
| VK.COM | 15 000 P. |
| MAIL.RU | 5 000 P. |
| YANDEX | 8 000 P. |
| GMAIL (ДОСТУП) | 30 000 P. |
| RAMBLER | 7 000 P. |
| UKR.NET | 15 000 P. |
| КОР. ПОЧТЫ И ЛЮБЫЕ ДРУГИЕ | ОТ 15 000 P. |

УСЛОЖНЕНИЕ ДОСТУПА (Access Complication):

- ФЛУД ЗВОНКАМИ СМС НОМЕРОВ (SMS Flood)
- СПАМ EMAIL (Spam Email)
- DDOS АТАКИ (DDoS Attacks)

ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ (Frequently Asked Questions):

- СКОЛЬКО ВРЕМЕНИ ПОТРЕБУЕТСЯ НА ВЫПОЛНЕНИЕ РАБОТЫ? (How long will it take to complete the work?)
- КАКИЕ ДОКАЗАТЕЛЬСТВА ВЫПОЛНЕННОЙ РАБОТЫ ВЫ (What evidence of completed work do you have?)
- УЗНАЕТ ЛИ ЧЕЛОВЕК О ВЗЛОМЕ? (Will anyone know about the breach?)
- КАКИЕ ДАННЫЕ ТРЕБУЮТСЯ ДЛЯ ЗАКАЗА? (What data is required for the order?)
- ОПЛАТА УСЛУГ ПРОИЗВОДИТСЯ ДО ИЛИ ПОСЛЕ ВЗЛОМА? (Is payment for services made before or after the breach?)

Figure 4. Offerings from the website of Void Balaur in 2020

The main activities of Void Balaur that were initially advertised on underground forums were breaking into free webmail, social media, and corporate email accounts. Copies of mailboxes were being offered both with and without user interaction. Most likely, the option to deliver data with user interaction happens via credential phishing, and when needed, includes two-factor authentication. For some Russian email providers, copies of mailboxes are offered without any user interaction. We have no reason to doubt that this is a real business offering, because we have not seen negative feedback on Void Balaur in underground forums. We don't know how customer data like emails are stolen without user interaction, but there are some scenarios where this would be possible. Note that these are only our conjectures on how the information is stolen; Void Balaur could have used other methods to gather data from their targets without user interaction.

- Key employees of email providers are knowingly selling data — either directly or indirectly — to the actors behind Void Balaur.
- Key employees who have legal access to mailboxes have been compromised.
- Law enforcement personnel who may have legal access to mailboxes are compromised.
- The computer systems of the email provider have security issues or have been breached.
- The group uses databases with leaked credentials to access mailboxes without user interaction.

Naturally, the service that retrieves emails without user interaction is offered at a premium rate. We were unable to establish how they can offer this kind of data.

Starting in 2019, Void Balaur advertised the sale of very private and sensitive data of individuals from Russia in underground forums. For example:

| Type of Information | Starting Prices (Rubles) |
|--|--------------------------|
| Information on Russian passports, foreign passports, marriage certificates, and N1 forms | > 1,500 (US\$21) |
| Information on purchased tickets where a passport is needed (train, bus, airlines, and ferries). No charters and private planes. | > 2,000 (US\$28) |
| Border data on individual persons | > 9,000 (US\$124) |
| Data on passengers arriving at Russian airports | > 9,000 (US\$124) |
| Data on passengers of Russian long distance train stations | > 9,000 (US\$124) |
| Interpol records | price on request |
| Criminal records | > 1,500 (US\$21) |
| Migrant permit | > 3,000 (US\$41) |
| Traffic camera shots | > 5,000 (US\$69) |
| Traffic safety records | > 1,300 (US\$18) |
| Traffic police data (fines, registration of cars) | > 1,300 (US\$18) |
| Weapon registration | > 2,500 (US\$34) |
| Federal tax service records | > 1,300 (US\$18) |
| Unified Housing Document (Moscow only) | > 4,000 (US\$55) |
| Cadastral information | > 1,500 (US\$21) |
| Credit history records | > 1,500 (US\$21) |
| Pension fund records | > 3,000 (US\$41) |
| Registry office records | > 5,000 (US\$69) |
| FSSP records | > 5,000 (US\$69) |

| Banking services for individuals and legal entities | Starting Prices (Rubles) |
|---|--------------------------|
| Account Balance | N/A |
| Account statements | N/A |
| Phone number associated with bank account | N/A |
| Banking card registration data | N/A |
| Reason and date for account blocking | N/A |

| Cellular services | Starting Prices (Rubles) |
|---|---|
| Retrieve the phone number give passport information | 700 – 5,000 (US\$10 to US\$69) depending on cellular provider |
| Phone call and SMS records without cell tower locations | 2,000 – 35,000 (US\$28 to US\$482 USD) |
| Phone call records with cell tower locations | > 60,000 (US\$826) |
| Blocking phone numbers | 4,000 (US\$55) |
| Map where calls were located | > 10,000 (US\$138) |
| Location of phone/SIM card | price depends on region |
| Printout of an SMS message | price on request |

Table 5. Some of the offerings on sensitive personal data that Void Balaur is advertising in underground forums. Starting prices are in Russian rubles. We added equivalent US Dollar amounts based on the exchange rate on September 14, 2021

The telecom data that Void Balaur is peddling includes phone call records with cell tower locations that could reveal who a person has been calling, the duration of the calls, and the approximate location where the calls were made. Knowledge of these details could serve several purposes, including committing serious crimes. Furthermore, blocking phone numbers, a service that Void Balaur also offers, can help facilitate serious crimes — for example, by ensuring that someone is unreachable by phone while the crime is taking place.

The price for getting phone call records with or without cell tower information varies a lot between different Russian providers, up to about a factor of ten. Apparently, getting phone records from some telecom companies are much easier than from others.

We are not sure how they obtain such sensitive private data — it’s possible that they get it by paying bribes to insiders in the telecom companies. This scenario was supported by a media article that was published in 2019 by BBC Russia.¹² Other possible scenarios are that key engineers of telecom operators are being hacked or that the network of telecom companies is being compromised. During our research, we found supporting evidence for the former: Void Balaur has been targeting key engineers and management of various mobile telco companies, as shown in Table 6.

| Target | Country | Date |
|--|------------------|---------------------|
| Deputy director of core telco network | Russia | Aug 2021 |
| Senior manager of telecom company | Russia | May 2021 |
| Senior telco network engineer | Russia | Mar 2021 |
| Senior telco network engineer | US/Russia | Nov 2020 |
| Senior telco network engineer | US/Russia/Israel | before Jun 2020 |
| Founder of a mobile virtual network operator | UK/Russia | May 2021 |
| Mobile satellite communications operator | Russia | May 2021 |
| Manufacturer of cellular equipment 1 | Russia | Dec 2020 |
| Manufacturer of cellular equipment 2 | Russia | Oct 2021 |
| Radio navigation company 1 | Russia | Jul 2020 – May 2021 |
| Radio navigation company 2 | Russia | Apr 2021 |
| Radio navigation company 3 | Russia | May 2021 |
| Radio navigation company 4 | Russia | May 2021 |

Table 6. Noteworthy Void Balaur targets in the telecom industry. For one target, we only have an approximate target date

In December 2020, reports were released on the investigative journalism website Bellingcat alleging that there are direct relations between persons working for an intelligence agency and attempted assassinations. As part of their investigation, Bellingcat journalists bought private flight data from a service that advertises on Prodiv.¹³ We do not know the exact data sources that these investigative journalists used, but we do know that Void Balaur offers telecom and passenger flight record data, which was possibly one of the sources used by the journalists (and we also know that Void Balaur advertises on Prodiv, which we mentioned earlier).

Naturally, the allegations generated a lot of attention in international media. In addition, the news reports were discussed in underground forums as well. In a posting on an underground forum, Void Balaur expressed concern about the allegations, as they could be a threat to its business.

One message posted by Void Balaur roughly translates to “Do you think they [Russian LE] will try to discover the whole chain, or just calm down the noise [generated by the media reports]?” This shows that Void Balaur was concerned about potential backlash. However, we did not notice any visible consequences. To our knowledge, Void Balaur did not slow down its services during the time international media showed a higher interest in underground forums like Prodiv.

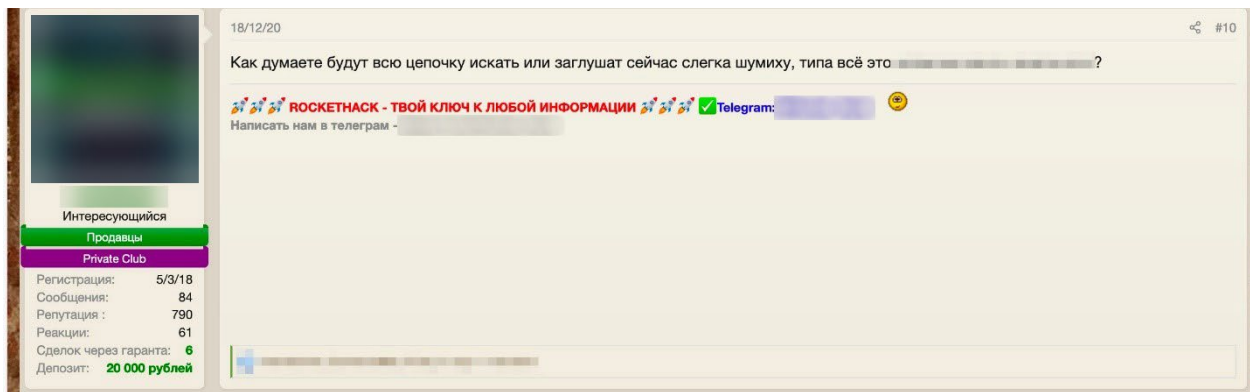


Figure 5. A Void Balaur post in the underground forum Probiv published on December 18, 2020. The poster expressed concerns about an investigative journalists claims of being able to buy airline passenger and cell tower data on Probiv.

Void Balaur's Targets

During our research we were able to collect a significant amount of information on Void Balaur's campaigns. We found more than 3,500 email addresses for individuals and companies that the group targeted.

We do not have a list of the users of Void Balaur's services, but we do know about customers who commented positively on the group's services in semi-public underground posts. These customers were satisfied with the services that Void Balaur provided, such as breaking into email boxes, providing information on passports, breaking into Telegram accounts, and offering sensitive telco information. These customers were active participants in underground forums like tenec.cc, Prodiv and Darkmoney.

We suspect, however, that the more important customers of Void Balaur are not active participants of forums like Prodiv. We started to realize this when we read a report published in 2019 by the Canadian nonprofit organization eQualitie.¹⁴

The report describes various phishing and web attacks that have been launched against human rights activists and journalists in Uzbekistan since 2016. It also shows attacks against the websites of media outlets between 2016 and 2017. The phishing campaigns were done over nearly a year, from March 2018 to February 2019. The report mentions that a threat actor was using professional vulnerability scanning tools such as Acunetix, NetSparker, and WPScan against three websites that cover political news in Uzbekistan. EQualitie also reported that it suspects that the same threat actor sent 14 phishing emails to targets who are either journalists or human right activists in Uzbekistan. In 2020, Amnesty International published a follow-up report that linked the campaigns that eQualitie originally reported to both Windows and Android malware.¹⁵ Moreover, Amnesty International was able to find an additional 170 targeted accounts in Uzbekistan and neighboring countries.

Amnesty International and eQualitie clearly indicate that the attacks in Uzbekistan had a serious impact on the lives of some individuals. This is a telling example of a cybermercenary providing services for a possibly larger campaign that is causing significant harm to human lives.

While both reports do not attribute the attacks to a particular threat actor, we attribute the attacks with a medium confidence level to Void Balaur based on the following:

- An overlap in infrastructure between Void Balaur and the indicators that were posted by eQualitie and Amnesty International.

- The hostnames that were used in known Void Balaur cases we are tracking and the attacks described by eQualitie have a form that is virtually unique in an enormous database of multibillion records of passive DNS data spanning 10 years.
- Some of the Uzbek targets we found to have been targeted by Void Balaur in 2020 are the same as the targets described in the eQualitie and Amnesty reports.
- The editor in chief of a media website that was attacked in 2016 and 2017 according to the eQualitie report was targeted by Void Balaur in 2020 through his private email address.
- We found one of the email addresses that was mentioned in the eQualitie report as a sender of credential phishing emails was back on the group’s target list.

Appendix B provides a more detailed explanation on why we think Void Balaur was behind the campaigns as described in the eQualitie report and the Amnesty International report.

We do not know who paid Void Balaur to target Uzbek-related media and civil rights activists. Apparently, the client was able to buy Void Balaur’s services even before the group started actively advertising in underground forums. The campaigns against Uzbek targets started as early as 2016 and were still ongoing as of 2020, according to our data (and probably even extended to 2021). This shows that Void Balaur is being hired for long-term campaigns, something we have seen for other targets as well.

| Target | First attack | Last attack |
|---|--------------|--------------|
| Uzbek journalist platform | Nov 3, 2020 | Nov 11, 2020 |
| Sender email address mentioned in the Deflect report | Nov 5, 2020 | Dec 23, 2020 |
| Individual who signed a political petition in Uzbekistan | Nov 5, 2020 | Nov 9, 2020 |
| Editor-in-chief of a media organization focused on Uzbekistan | Nov 5, 2020 | Nov 7, 2020 |
| Uzbek human rights activist | Nov 7, 2020 | Nov 9, 2020 |
| Uzbek political party | Nov 5, 2020 | Nov 5, 2020 |

Table 7. Uzbek media and human rights activists that Void Balaur targeted in 2020. The indicated timeframes are conservative; these attacks likely occurred over longer periods.

While Void Balaur advertises in underground forums where criminals gather to do business, its services are not only used for typical cybercrime but for political reasons as well. This shows that Void Balaur is knowingly or unknowingly facilitating attacks in which human rights may be violated, a pattern we have also seen in a couple of other campaigns. A significant part of these campaigns look like the work of an APT attacker with long-term goals.

Some of Void Balaur’s campaigns are quite brazen. For example, we found that in September 2021, the group targeted the private email addresses of a former head of an intelligence agency, five active government ministers (including the minister of defense) and two members of the national parliament of an Eastern European country.

We also found presidential candidates for the 2020 Belarus elections on Void Balaur’s target list.

| Target | Country | Sector | Date |
|--------------------------------|---------|----------|----------|
| Presidential candidate | Belarus | Politics | Sep 2020 |
| Presidential candidate | Belarus | Politics | Sep 2020 |
| Member of the opposition party | Belarus | Politics | Sep 2020 |

Table 8. Void Balaur targeted high-profile Belarusian political personalities in 2020

Aside from political targets in Uzbekistan and Belarus, Void Balaur also targeted politicians and government officials in the Ukraine, Slovakia, Russia, Kazakhstan, Armenia, Norway, France, and Italy. Some of these attacks were part of a larger campaign and not necessarily restricted to attacks over the internet alone. Some of the victims felt so threatened that they left their home countries and went into exile.

| Target | Country | Sector | Date |
|----------------------|------------|------------|----------|
| Politician | Armenia | Parliament | Dec 2020 |
| Politician | Ukraine | Parliament | Oct 2020 |
| Spouse of politician | Ukraine | | Nov 2020 |
| Diplomat | Russia | Government | Oct 2020 |
| Minister | Russia | Government | Sep 2021 |
| Politician | Kazakhstan | Government | Jan 2021 |

Table 9. Noteworthy political personalities from other countries targeted by Void Balaur. The dates in the table are examples of when the targets likely received a credential phishing email from the group.

| Target | Country | Sector | Date |
|-------------------|---------|--------------------|----------|
| Politician | France | Parliament | Aug 2021 |
| Politician | France | EU parliament | Aug 2021 |
| Former politician | France | Activist | Sep 2021 |
| Politician | Italy | EU parliament | Aug 2021 |
| Politician | Norway | Political activist | Aug 2021 |

Table 10. Void Balaur very likely targeted four politicians in France, Italy, and Norway for the first time on the same day in August 2021. Another French former politician was targeted in September 2021. The targets are from different countries, but they shared similar political views.

Journalists and media organizations are also frequent targets of Void Balaur. We have seen the group target more than 25 journalists, although we expect the actual number of targeted journalists to be higher.

Some phishing attacks by Void Balaur that, at first glance, look to have a financial motive may actually be associated with large-scale disruptive attacks. For example, the group launched attacks against a cryptocurrency exchange for years, targeting not only their customers, but executives as well through their corporate and personal email addresses. The website of the company has been a regular victim of DDoS and hacking attacks and one of their employees was even kidnapped for ransom in the past.¹⁶ While we do not know whether Void Balaur had anything to do with the kidnapping and the DDoS attacks, this is again an example where a Void Balaur victim also suffered from larger-scale attacks with real-life consequences.

Several of the group’s targets are from Russia and other neighboring countries, But the group is also active in other countries, including the US, Israel, Japan and European countries.

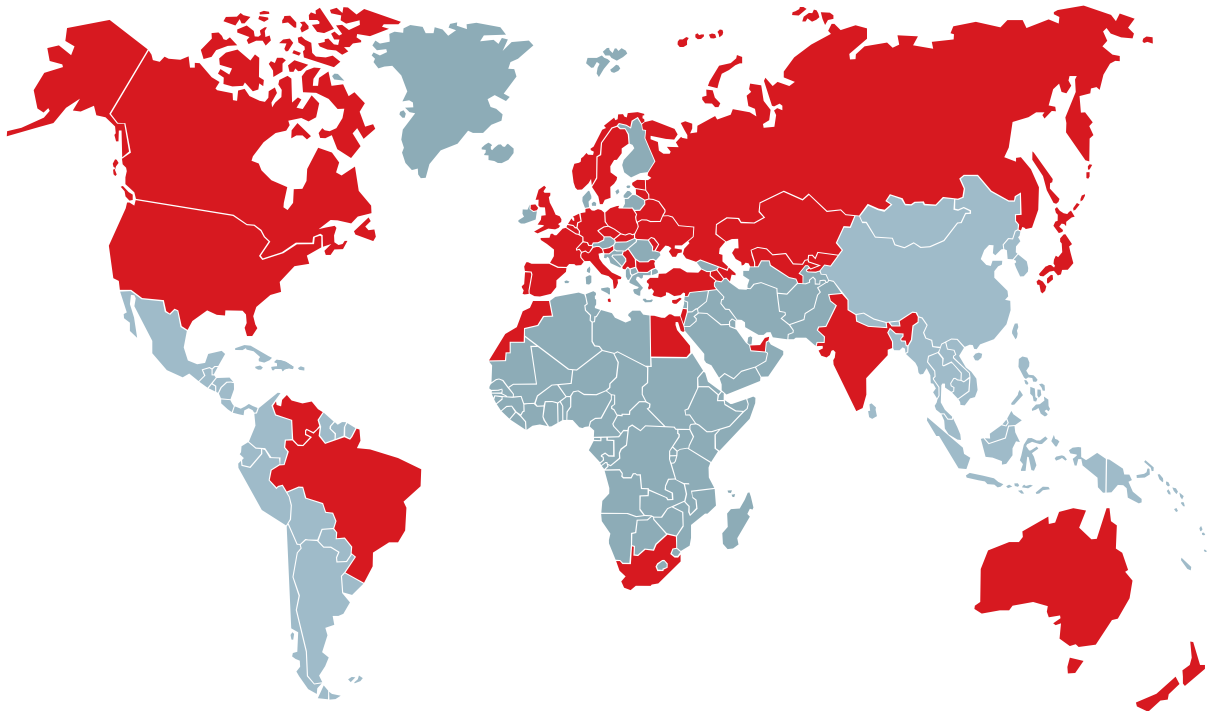


Figure 6. Countries in which Void Balaur email targets were located (companies were targeted via corporate email addresses; individuals were targeted via private email addresses)

Some of the threat actor’s campaigns span a long period of time. The timeline in Figure 8 illustrates a long, ongoing campaign against the companies of one of the most successful conglomerates in Russia. From at least September 2020 to August 2021, Void Balaur has been targeting board members, directors, executives and family members — all associated with the same commercial conglomerate.

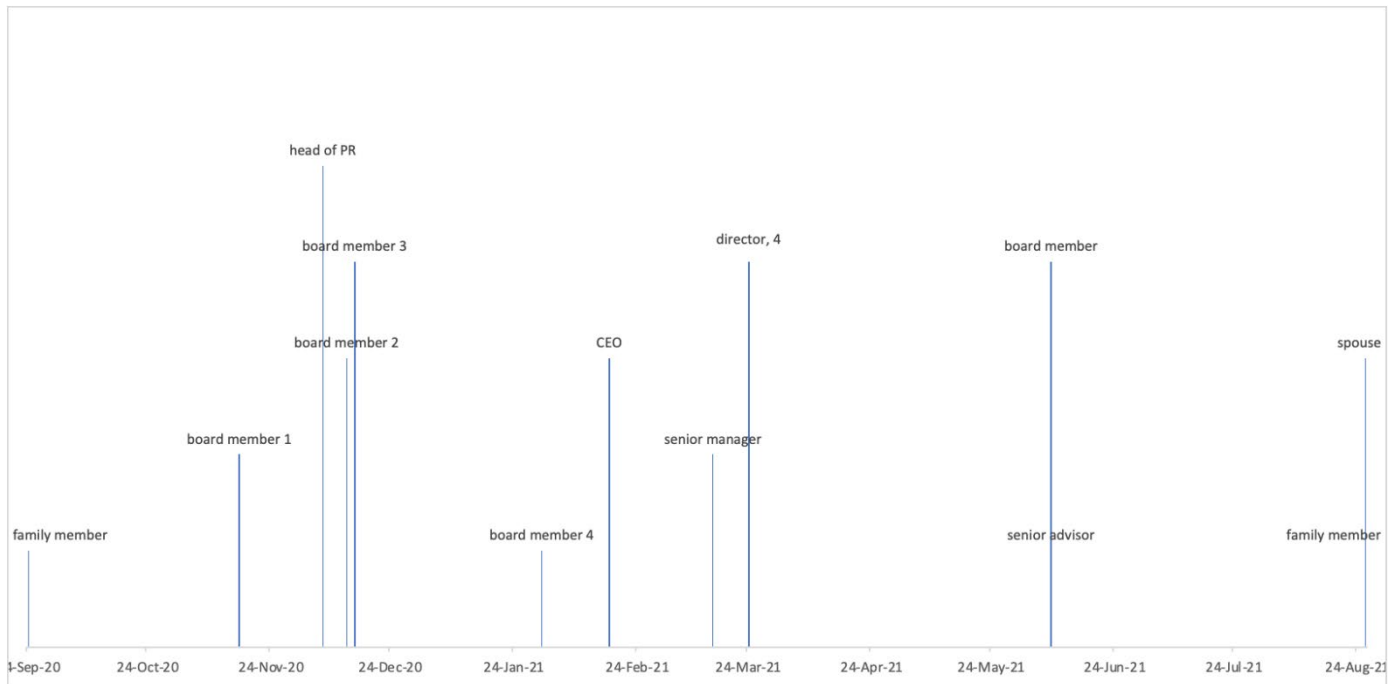


Figure 7. The timeline of a campaign launched against one of the largest conglomerates in Russia. Several board members, executives, directors and even family members of the billionaire owner were targeted over a year. This shows that for corporate espionage-related attacks, the campaigns of Void Balaur can be persistent and long lasting.

Targets with Access to a Large Amount of Private Information

While investigating the campaigns of Void Balaur, we noticed that the threat actor was targeting organizations and individuals who potentially have access to a large amount of individuals' sensitive data. Some of these targets align with Void Balaur's offerings in underground forums, while others are new.

We have observed Void Balaur targeting organizations and individuals in the following sectors:

- Mobile and core telco companies
- Cellular equipment vendors
- Radio and satellite communication companies
- ATM machine vendors
- Point-of-sale (POS) system vendors
- Fintech companies and banks
- Business aviation companies
- Medical insurance organizations in at least three regions of Russia
- In Vitro Fertilization (IVF) clinics in Russia
- Biotechnology companies that offer genetic testing services

The campaigns are often conducted over an extended period. We do not know exactly why these organizations and individuals are being targeted. The size and lucrativeness of the industry may play a role — take for example the IVF market, which has grown into a multibillion industry and could be a reason for Void Balaur's interest in IVF clinics (likely for corporate espionage). Besides targeting IVF doctors, Void Balaur is also taking aim at academic researchers who study human and animal reproduction, which could also support corporate espionage motives.

However, we also suspect that Void Balaur is hungry for data and information on individuals and could be looking to expand their current business offerings and explore new methods of providing services to customers. Offering individuals' medical data is one example of this. Between May 23, 2020 and April 1,

2021, Void Balaur targeted more than 50 employees of over 20 Russian IVF clinics. Furthermore, the group most likely targeted employees of at least four other companies that offer genetic testing services. The threat actor also showed an interest in compulsory health insurance companies in at least three republics of Russia. Finally, the group also targeted medical test labs, general physicians, and companies that sell medical equipment. Doctors and medical service providers possess a sizeable amount of sensitive information on their patients and there is likely a demand for this kind of data. Offering medical data would be a natural addition to the services that Void Balaur is advertising today.

We already mentioned that Void Balaur offers sensitive telco data of individuals in some CIS countries, including text messages and cell tower log files. We also discussed possible ways Void Balaur could have retrieved this kind of data, such as compromising either a telco company or some of their key employees. For this, we have supporting evidence (shown in Table 6): the threat actor has targeted key engineers and managers working for mobile telco operators in Russia and Kazakhstan. The group has also targeted two manufacturers of cellular equipment as well as companies that specialize in mobile satellite communications and radio navigation (multiple times for the former).

In May and June 2021, Void Balaur added four Russian vendors of ATM and POS (Point of Sale) vendors and two Russian virtual cash register service providers to their target list. A couple of Russian fintech companies that offer innovative products were targeted as well. In our paper on the risks of open banking, we warned that new fintech startups would be interesting targets for cybercriminals, because they have plenty of information on the finances of individuals and sales data from shops and malls.¹⁷

In Table 5, we mentioned that Void Balaur offers data on purchased plane tickets, except for charters and private planes. We also observed that the group has been targeting executives of various business aviation companies. The reason why these executives were targeted could have been to fill the gap of Void Balaur's offerings on passenger details of charter flights and private planes.

Cryptocurrency Account Phishing

Void Balaur has been consistently trying to get access to wallets of various cryptocurrency exchange services. For this activity, Void Balaur narrowly targets people who are interested in cryptocurrencies. Stealing cryptocurrency is profitable and interesting to cybercriminals as the virtual money that is associated with cryptocurrency can be transferred to wallets controlled by the criminals, where there is little chance of recovering the stolen goods.

Since at least 2018, Void Balaur has set up numerous phishing sites related to various cryptocurrency exchange and cryptocurrency wallet sites. There is one service that stands out, however: EXMO. Some of Void Balaur's phishing sites for EXMO user, like exmo[.]ms, were used for about three years, which is a rather lengthy time. Besides this domain, Void Balaur set up several other domains for EXMO phishing.

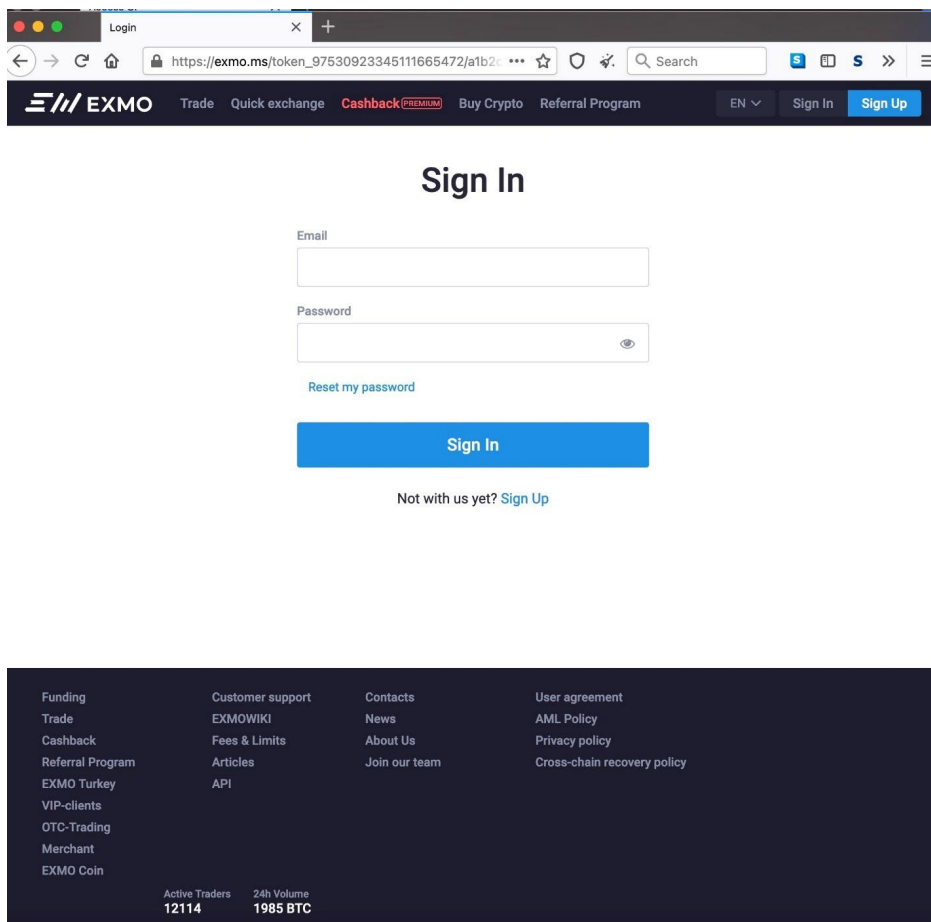


Figure 8. A Void Balaur phishing site that targets Exmo users

| Phishing domain | Date created | Real domain | Description |
|-------------------------|--------------|-----------------|----------------------------------|
| advcash.com[.]ru | May 02, 2018 | advcash.gi | Cryptocurrency exchange |
| exmo[.]ms | May 03, 2018 | exmo.com | Bitcoin exchange |
| yobit[.]one | May 06, 2018 | yobit.net | Ethereum exchange |
| nicehash.com[.]cm | May 07, 2018 | nicehash.com | Cryptocurrency mining |
| cryptopia.co[.]cm | May 11, 2018 | cryptopia.co.nz | Bitcoin exchange |
| wex[.]so | May 11, 2018 | wexinc.com | FinTech company |
| binance.com[.]ht | May 19, 2018 | binance.com | Crypto exchange |
| wallet-cryptonator[.]ru | Sep 3, 2018 | cryptonator.com | Cryptocurrency wallet |
| bitpay.ru[.]com | Dec 17, 2019 | bitpay.com | Bitcoin payment service provider |
| trezor-live[.]com | Dec 17, 2019 | trezor.io | Cryptocurrency wallet |
| epayments[.]run | Jan 30, 2020 | epayments.com | Financial services provider |
| exmo.me[.]uk | Mar 26, 2021 | exmo.com | Bitcoin exchange |

Table 11. Phishing domain names of Void Balaur, targeting various cryptocurrency platforms

Working Times of Void Balaur

We were curious about the working habits of Void Balaur. We collected enough data to gain an idea of the actor's working hours. We plotted statistics on hours, weekdays, and months when Void Balaur was active (Figures 9-13). We did this for both attacks on email addresses of Russian service providers and attacks on the email addresses of a major international email provider.

It appears that Void Balaur usually starts the working day around 6 a.m. GMT and works until around 7 p.m. We saw hardly any activity from 10 p.m. to 4 a.m. GMT. While Void Balaur is less active during weekends, the actor often works seven days a week and does not take long vacations such as during Christmas or in the summer. This is in contrast with an actor like Pawn Storm (APT28) who works during Christmas holidays, but often takes a break in the summer and during a period from the end of December until around mid-January.

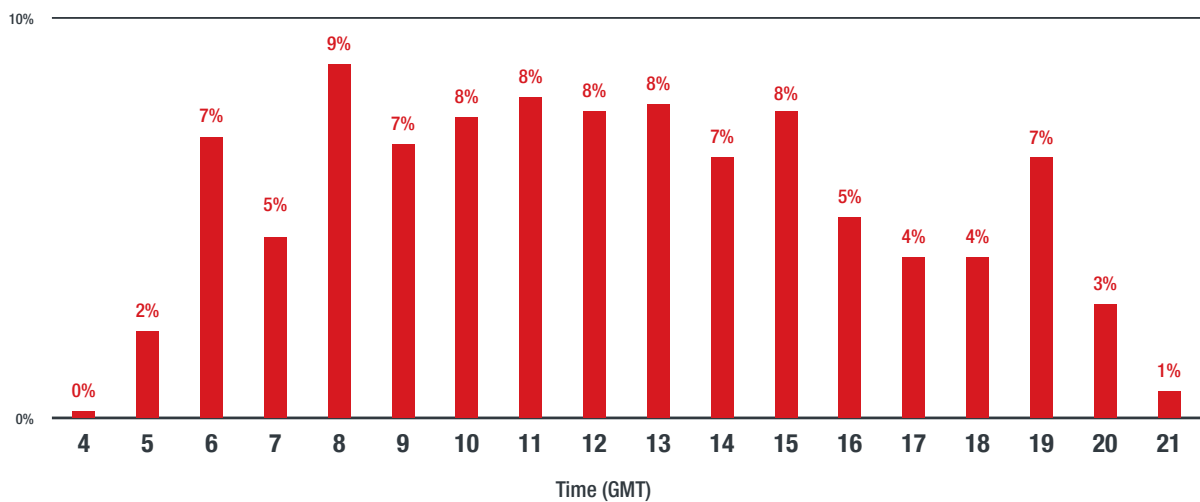


Figure 9. Void Balaur's active hours during its attacks on targets outside Russia

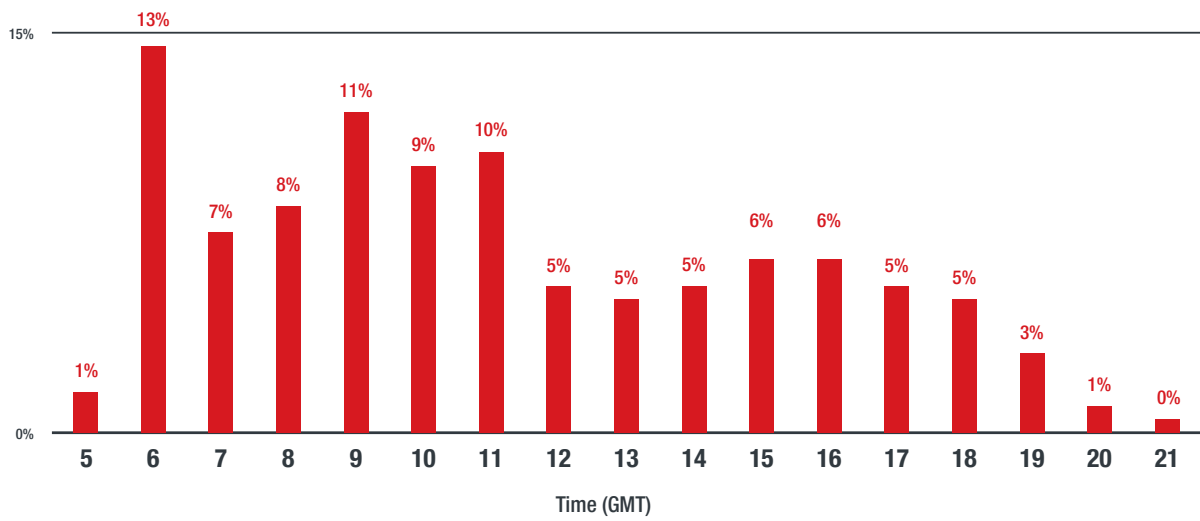


Figure 10. Void Balaur's active hours during their attacks targeting email addresses of Russian providers

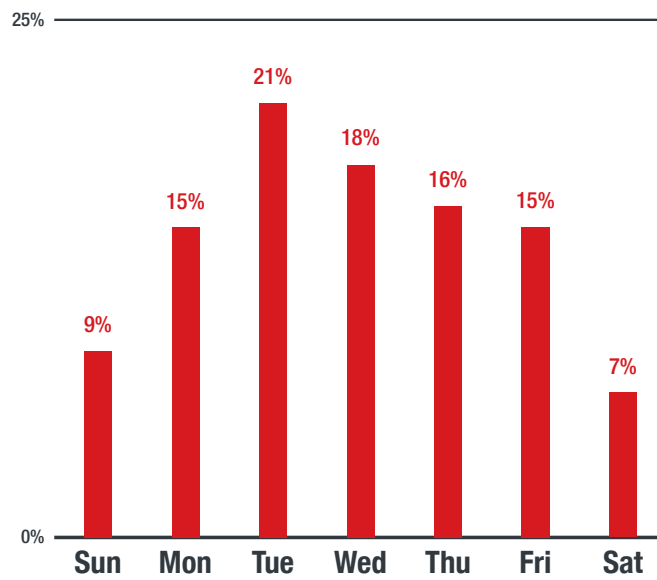


Figure 11. Void Balaur's active time per day for attacks on targets outside Russia

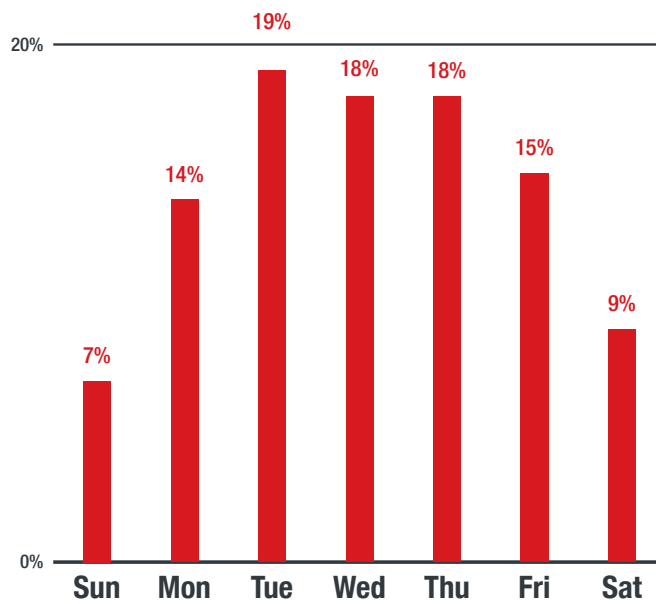


Figure 12. Void Balaur's active time per day for attacks targeting email addresses of Russian providers

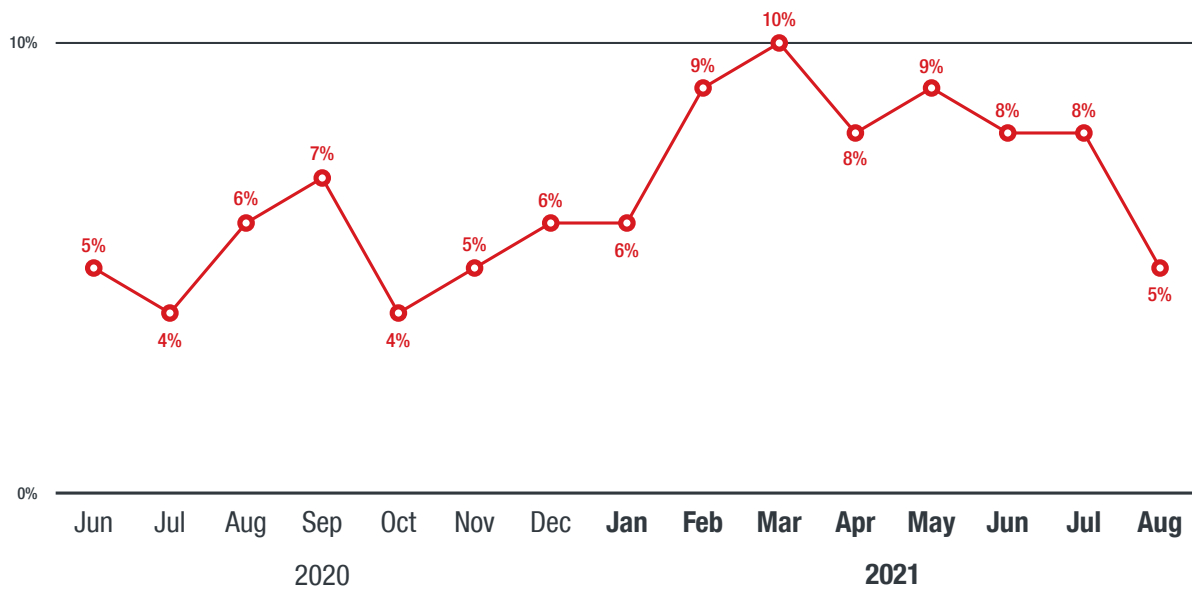


Figure 13. Void Balaur's active times during their attacks against international targets from May 2020 to August 2021. The vertical scale has been normalized over the total activity we have seen over a 16-month period. There is no clear vacation or holiday period in the chart.

Malware Activities of Void Balaur

Z*Stealer

As first reported in the report by Amnesty International, Void Balaur has used malware against its targets as well. One file was downloaded from the command-and-control (C&C) server msoffice365[.]win and had the SHA256 sum 5a2c9060f6cc1e6e0fd09b2b194631d2c7e7f024d9e2d3a9be64570e263f565f. An analysis of this sample shows that it is a simple information stealer. The malware is highly tuned for stealing credentials from the following applications and software:

- Instant messaging software: Pidgin, ICQ/QIP, Miranda, Psi, Jabber accounts
- File Transfer Protocol (FTP) and Secure Shell (SSH) software: FlashFXP, CuteFTP, FileZilla, SmartFTP, WS_FTP, WinSCP, Total Commander
- Email clients: Outlook, Yandex, Thunderbird, Windows Live Mail, mail.ru, The Bat
- Virtual Network Computing (VNC) software: RealVNC, TightVNC, TigerVNC, UltraVNC
- Browser software: Opera, Chrome, Chromium, Torch, YandexBrowser, Comodo Dragon, Firefox, Internet Explorer, Amigo Browser, Sleipnir Browser, Safari
- Remote Desktop Protocol software

The malware also has cryptocurrency wallet stealing capabilities related to:

- MultiBit
- Electrum
- Terracoin
- PPCoin
- PrimeCoin

This kind of malware is perfect for the nature of business in which Void Balaur is involved. It can be used to steal sensitive data and it has a component for stealing cryptocurrency wallets.

DroidWatcher malware

The Amnesty International report also mentioned that Void Balaur had been using Android malware such as DroidWatcher, an Android malware that has been around for a long time and is quite easy to find on the internet.

We found a sample used by Void Balaur that communicated with one of their C&C servers at `garant-help[.]com`. The filename for that sample was “Rasmlar.apk”. It is interesting to note that “rasmlar” means “photos” in Uzbek language. The sample had the SHA256 sum `902c5f46ac101b6f30032d4c5c86ecec115add3605fb0d66057130b6e11c57e6`.

The malware sample had several functions:

- Transferring incoming/outgoing SMS and phone call logs
- Phone call recording (exfiltration is done by email)
- Taking screenshots at specified interval (exfiltration is done by email)
- GPS position transfer at specified intervals
- Notification of SIM card changes
- Automatic silent updates
- Remote control for phone settings
- Spying on VK and WhatsApp

The version we found had been tweaked and modified, both for additional functions and to hide its presence better:

- Anti-VM and anti-debug features have been added, based on public code.¹⁸
- Addition of XMPP protocol (default XMPP channel admin name set to “opr6”) with Rooster client.¹⁹
- Phone rooting functionalities based on public code “RootTools v3.2.”
- Remote shell addition
- Use of Websocket to send information
- C&C fetching capabilities via a Twitter account
- Additional spying capabilities for more Android apps:
 - Email : ru.mail
 - Messengers: imo, OK, Telegram, Viber

The malware sample had two predefined C&C servers configured, `garant-help[.]com` and `192.168.35[.]40:3355` (possibly a leftover from internal testing).

It also had a Twitter account configured, “world181061401,” which has been taken down prior to our investigation.

Overlap with Pawn Storm

We started our investigation into Void Balaur because we initially suspected that copies of a dozen phishing emails we had received from a source were the work of Pawn Storm threat actors. We soon realized that these campaigns belonged to a different group who we later called Void Balaur. However, we did find a small, but clear overlap between Pawn Storm and Void Balaur during our research.

We have been following Pawn Storm campaigns since 2014, and have collected information on Pawn Storm targets throughout in all those years. We have seen that thousands of email addresses were targeted either via spear phishing or credential phishing. This makes it possible for us to compare the campaigns of Pawn Storm and Void Balaur and their targets.

While there are clear differences between the two threat actors, we can also see some overlap. The difference is that Void Balaur is a cybermercenary with a wide range of clientele. This makes the Void Balaur targets a lot more diverse than that of Pawn Storm. Void Balaur is often motivated by crime and economic espionage while virtually all of the attacks launched by Pawn Storm that we have observed is motivated by espionage, politics, geopolitics, and the military. We did not observe Void Balaur attacking military targets except for one minister of defense, but we did see a substantial number of politicians on their target list. The same holds true for journalists, activists, and religious leaders: Pawn Storm aggressively targeted one particular group of religious leaders in 2014 to 2016; the same religious leaders were on Void Balaur's target list in 2020 and 2021.

| Sector | Attacks by Pawn Storm | Attacks by Void Balaur |
|------------------------|-----------------------|------------------------|
| Military | Significant | Very few observed |
| Defense industry | Significant | Very few observed |
| Government | Significant | Moderate |
| Diplomats | Significant | Moderate |
| Politicians | Significant | Moderate |
| Human rights activists | Significant | Significant |
| Oligarchs | Moderate | Significant |
| Journalists | Significant | Significant |
| Religious leaders | Moderate | Moderate |

| Sector | Attacks by Pawn Storm | Attacks by Void Balaur |
|---------------------------------|-----------------------|------------------------|
| Scientists | Significant | Significant |
| Telco engineers | Not observed | Moderate |
| ATM / PoS sellers | Not observed | Moderate |
| Business aviation | Not observed | Moderate |
| Lawyers | Not observed | Moderate |
| IVF clinics | Not observed | Significant |
| Medical | Not observed | Significant |
| Fashion | Not observed | Significant |
| Cryptocurrency | Not observed | Significant |
| Long tail of various businesses | Not observed | Significant |

Table 12. Comparing credential phishing attacks by Pawn Storm from 2014 to 2016 and Void Balaur from 2020 to 2021. Since 2020, Pawn Storm has been using brute force attacks on a wider scale.

In total, we have observed a dozen email addresses that were targeted by both Pawn Storm during the period of 2014 to 2015, and by Void Balaur from 2020 to 2021. Besides the religious leaders, we also saw attacks on diplomats, politicians and a journalist from both Pawn Storm and Void Balaur.

Generally, there is a clear overlap in the sectors that are being targeted by both groups as we have illustrated in the table above. However, there are clear differences as well: Based on our observations, Void Balaur has targeted sectors that Pawn Storm is not active in. For example, Void Balaur has had long running campaigns against cryptowallet users and even some cryptoexchange platforms. In our research on Pawn Storm, we never saw any significant targeting of cryptocurrency platforms.

| Sector | Pawn Storm 2014 to 2016 | Void Balaur 2020 to 2021 | Exact overlap |
|---------------------|-------------------------|--------------------------|---------------|
| Religious leaders | 5 | 12 | 5 |
| Diplomats (Ukraine) | Many | Several | 3 |
| Journalists | Many | Many | 1 |
| Other | N/A | N/A | 2 |

Table 13. Overlap in targets for Pawn Storm and Void Balaur

As we reported in 2020, Pawn Storm is still using the classic technique of sending credential phishing emails to gain access to mailboxes.²⁰ It also does large scale brute force attacks and password spray attacks via Tor, VPN networks, and occasionally, dedicated IP addresses. We don't know if Void Balaur is also trying to use brute force attacks on email account credentials.

Outlook for the Cybermercenary Industry

The reality is that regular internet users cannot easily deter a determined cybermercenary. More than once, media outlets have reported on advanced offensive tools in a cybermercenary's arsenal being used against journalists and human rights activists. Some of these tools include so-called zero-click zero-day exploits, which do not require any user interaction to infect the target with malware.²¹ While these tools might be meant to be used in the fight against terrorism and organized crime, the reality is that they — knowingly or unknowingly — end up in the hands of threat actors who use it against unwitting targets.

The core issue that causes these recurring problems is that some countries may view cybermercenaries within their borders as strategic assets that can be used in multiple ways. First, the services and tools of cybermercenaries can be used in offensive attacks against terrorism and organized crime, and for targeting foreign assets. Second, they can also be sold to other countries and used as an economic or political tool in foreign policy. Though this might benefit some countries, it also poses a tremendous risk of possible backlash when malicious elements use these tools. Even worse, tools that have been sold overseas might end up being used against citizens of the country that originally exported these tools.

Citizens can pressure national lawmakers into implementing better regulations for the development and export of cyberweapons for its national industry of cybermercenaries. This is not an easy task, but it's likely one of the few solutions that can better protect the public against cybermercenary attacks at the government level. Cybermercenaries could also be made accountable for both their actions and the cyberweapons they export, as was advocated in a Microsoft blog post in 2020.²²

Defending Against Cybermercenary Attacks

Defending against cybermercenaries such as Void Balaur is not an easy task. The group claims it can retrieve sensitive data on individuals without user interaction and we have no reason to doubt that this business proposition is a real one under certain circumstances.

Void Balaur sells private data such as emails and cell tower data to anyone who wants to pay for it. This means that users and organizations should carefully consider the security policies of their email and mobile providers to determine whether these services are fit for their needs and situation. Users should also look into alternatives to two-factor authentication via SMS messages since Void Balaur also has interception of SMS messages in its business offerings. We do not know how Void Balaur is intercepting SMS messages in Russia, but other threat actors have used tricks like SIM swapping to intercept SMS messages.²³

While the techniques used by Void Balaur might be difficult to defend against, that doesn't mean that security best practices are rendered ineffective. In fact, observing simple security practices can go a long way in helping defend against cybermercenary groups like Void Balaur:

- Use the email services of a reputable provider that is known to have robust security and have high privacy standards
- Use two-factor authentication for email and social media accounts, but instead of using SMS, consider the use of an app or a device such as Yubikey instead
- Use apps with end-to-end encryption for communications
- Use encryption systems like Pretty Good Privacy (PGP) for communication involving sensitive information or dialogue
- Permanently delete old, unneeded messages to prevent sensitive data from ending up in the hands of third parties in case the machine gets hacked
- Consider using some of the features of mobile apps that allow for setting a time after which chats for both the sender and receiver disappear
- Use drive encryption on all computing devices
- Turn off laptops and computers when not in use

Appendices

Appendix A

This Appendix shows how we linked the original phishing emails, which the spouse of a long-term Pawn Storm target received in early 2020, to Rockethack/Void Balaur.

| URL | Status | Details |
|---------------------------------------|-------------------|---------------|
| 27g4dwjallqnzu0[.]space | Privacy protected | Spam URL |
| account-googl[.]com | poxxpoz@pm.me | Sender domain |
| bflqj2xmpbwqkzpwg[.]fun | Privacy protected | Spam URL |
| izwg17taoz9noedve[.]xyz | Privacy protected | Spam URL |
| myaccount.mail.sessionverify.com[.]ru | Privacy protected | Phishing site |
| oapjiyfybhj0jszll[.]fun | Privacy protected | Spam URL |
| wnppid4qunpuwuvqk[.]fun | Privacy protected | Spam URL |
| yen9y2flnrcbwsvy9[.]fun | Privacy protected | Spam URL |

Table A.1. The indicators of phishing campaigns sent to the spouse of a long-term Pawn Storm target; privacy protection was lifted for one of the sender domains in 2021

One of the spam messages the spouse received used the domain name 27g4dwjallqnzu0[.]space, which resolved to the Iranian IP address 93.126.60[.]101. This IP address has had a few SSL certificates.

| Hostnames | Date | Registrant email address |
|-------------------------------|--------------|--------------------------|
| e.mail.ru-cloud[.]site | Mar 31, 2020 | egor_kredd@protonmail.ch |
| auth.yandex.ru-support[.]host | Apr 3, 2020 | Privacy protected |
| auth.yandex.ru-tech[.]site | Apr 7, 2020 | Privacy protected |
| auth.yandex.ru-temp[.]host | Apr 8, 2020 | Privacy protected |
| auth.yandex.ru-tech[.]host | Apr 10, 2020 | Privacy protected |
| 27g4dwjallqnzu0[.]space | Apr 14, 2020 | Privacy protected |

Table A.2. SSL certificates of 93.126.60.101

The IP address 93.126.60[.]101 had the same public SSH key between at least March 31, 2020 and April 25, 2020 with the fingerprint e8:9a:64:ad:38:36:c1:e2:a5:31:5c:f8:3a:1f:5d:c4. This provides a link between the spam campaign and the registrant's email address, egor_kredd@protonmail.ch.

We then did a reverse lookup on egor_kredd@protonmail.ch and these domain names:

| Domain | Created | Registrant email address |
|-------------------------|--------------|--------------------------|
| ru-cloud[.]site | Mar 30, 2020 | egor_kredd@protonmail.ch |
| exmo[.]tech | Jun 23, 2020 | egor_kredd@protonmail.ch |
| exmoney-zendesk[.]com | Feb 17, 2020 | egor_kredd@protonmail.ch |
| exmoney[.]tech | Jun 23, 2020 | egor_kredd@protonmail.ch |
| google-activity[.]pw | Jul 19, 2019 | egor_kredd@protonmail.ch |
| offshoehosting[.]name | Jul 10, 2019 | egor_kredd@protonmail.ch |
| usercheckactivity[.]com | Nov 27, 2019 | egor_kredd@protonmail.ch |

Table A.3. Linking domains with the email address egor_kredd@protonmail.ch

| Hostname | Date | Registrant email address |
|------------------------|--------------|---------------------------|
| advcash.com[.]ru | May 4, 2020 | dizain.alto@yandex.ru |
| advcash.com[.]ru | Mar 12, 2020 | dizain.alto@yandex.ru |
| cryptonator[.]cc | Dec 11, 2019 | privacy protected |
| mail-roundcube[.]site | Oct 28, 2019 | privacy protected |
| offshoehosting[.]name | Jul 11, 2019 | egor_kredd@protonmail.ch |
| advcash.com[.]ru | Apr 8, 2019 | dizain.alto@yandex.ru |
| localbitcoins.com[.]co | Mar 9, 2019 | N/A |
| exmo.com[.]cm | Mar 8, 2019 | velikpnov.1992@mail.ru |
| binance.com[.]ht | Mar 8, 2019 | N/A |
| nicehash.com[.]cm | Mar 4, 2019 | dizain.alto@yandex.ru |
| exmo[.]ng | Feb 14, 2019 | alisa-kolchina@rambler.ru |
| binance.com[.]ht | Jan 23, 2019 | N/A |
| exmo.com[.]cm | Jan 15, 2019 | velikpnov.1992@mail.ru |
| advcash.com[.]ru | Jan 15, 2019 | dizain.alto@yandex.ru |
| cryptopia.co[.]cm | Jan 12, 2019 | velikpnov.1992@mail.ru |
| nicehash.com[.]cm | Jan 11, 2019 | dizain.alto@yandex.ru |
| localbitcoins.com[.]co | Dec 17, 2018 | N/A |
| advcash.com[.]ru | Oct 22, 2018 | dizain.alto@yandex.ru |

Table A.4. SSL Certificates for 23.88.228.248

We think that the IP address 23.88.228.248 has been controlled by the same threat actor for a long time. Between October 10, 2018 and April 24, 2020, the public SSH key has been recorded multiple times by both a public SSH scanner as well as a private SSH scanner. It was always the same key with the fingerprint 55:bd:a1:eb:5f:ac:9e:3f:10:a4:7a:0a:1a:68:0c:a1. This is strong evidence that all of these domains belonged to the same intrusion set.

In the table showing the DNS resolutions for 23.88.228.[.]248, we have listed associated registrant email addresses. Let's look at one of them, velikpnov.1992@mail.ru, and do a reverse lookup:

| Domain | Date created | Registrant email address |
|----------------------|---------------------|--------------------------|
| cryptopia.co[.]cm | May 11, 2018 | velikpnov.1992@mail.ru |
| exmo.com[.]cm | May 10, 2018 | velikpnov.1992@mail.ru |
| exmo[.]ms | May 3, 2018 | velikpnov.1992@mail.ru |
| mail-gibdd[.]online | Mar 31, 2018 | velikpnov.1992@mail.ru |
| mail-google.com[.]de | Before Mar 11, 2018 | velikpnov.1992@mail.ru |
| Wex[.]so | May 11, 2018 | velikpnov.1992@mail.ru |
| Yobit[.]one | May 6, 2018 | velikpnov.1992@mail.ru |

Table A.5. Domain names registered by velikpnov.1992@mail.ru

| Domain | First Seen (GMT) | Last Seen (GMT) |
|-------------------------------------|------------------------|-----------------------|
| com-o2[.]ru | Apr 4, 2018, 1:25 PM | Apr 23, 2018, 3:59 PM |
| for-gmail-42naledm7cuuu3fwfch[.]ru | April 1, 2018, 7:01 PM | Apr 4, 2018, 5:06 PM |
| for-gmail-3gpzsl2v824czj0lr4[.]ru | Mar 31, 2018, 1:00 PM | Apr 6, 2018, 11:06 AM |
| for-yad-4whmgekuvh3ikfr8v8w2[.]ru | Mar 31, 2018, 11:47 AM | Mar 27, 2019, 5:48 PM |
| for-mail-1c0vr83nclr87vt7f7ws[.]ru | Mar 31, 2018, 11:47 AM | Apr 18, 2018, 1:41 PM |
| for-gmail-12y1uilzzlzvgd6l7yxb[.]ru | Mar 31, 2018, 7:40 AM | Apr 17, 2018, 6:02 AM |
| for-gmail-2m4e3qovxmlgqw3fiq[.]ru | Mar 31, 2018, 6:25 AM | Apr 7, 2018, 6:26 PM |
| for-mail-2fn9itdkpaolefd801tk[.]ru | Mar 31, 2018, 5:10 AM | Apr 6, 2018, 4:53 AM |
| for-gmail-5hcdd2w88fd7xudtfwbt[.]ru | Mar 31, 2018, 4:25 AM | Apr 6, 2018, 4:53 AM |
| for-yad-39ha3cp536lg6b13jgwy[.]ru | Mar 31, 2018, 12:20 AM | Mar 27, 2019, 1:37 AM |
| for-mail-512fs2nyvtmbi42lysw[.]ru | Mar 31, 2018, 12:20 AM | Apr 6, 2018, 4:53 AM |
| for-yad-5h55rj8tbr5czqgbwy3g[.]ru | Mar 31, 2018, 12:19 AM | Mar 27, 2019, 5:48 PM |
| for-mail-39gkfg30oi4jp62azz03[.]ru | Mar 31, 2018, 12:13 AM | Apr 6, 2018, 11:06 PM |
| for-mail-4hfmkk7e0gk6i948u4od[.]ru | Mar 31, 2018, 12:11 AM | Apr 6, 2018, 4:53 AM |
| for-yad-2nk9h2322q8913jo9410[.]ru | Mar 31, 2018, 12:11 AM | Mar 27, 2019, 5:48 PM |
| for-yad-1rhwhdloo6g6fiv5bv35[.]ru | Mar 31, 2018, 12:10 AM | Mar 27, 2019, 1:39 AM |

| Domain | First Seen (GMT) | Last Seen (GMT) |
|----------------------------|------------------------|------------------------|
| gibdd-mail.ru[.]com | Mar 29, 2018, 8:10 AM | Mar 31, 2018, 4:40 AM |
| 7fjvxlxcia29w08gf71[.]ru | Mar 22, 2018, 11:27 PM | Mar 19, 2019, 4:45 PM |
| disk-yandex.ru[.]com | Mar 22, 2018, 8:35 PM | Apr 17, 2018, 6:02 AM |
| o2-mail.ru[.]com | Mar 22, 2018, 3:42 PM | Mar 30, 2018, 2:53 PM |
| 4bcso7i5v7zff3el90gzc[.]ru | Mar 22, 2018, 2:01 PM | Mar 19, 2019, 4:42 PM |
| 801l4rg3bvvt22kcckt5[.]ru | Mar 22, 2018, 11:13 AM | Mar 19, 2019, 4:46 PM |
| 9n9cz2mlyoqkrp3zewwa[.]ru | Mar 22, 2018, 11:04 AM | Mar 19, 2019, 4:43 PM |
| 6t1nsinjn7o3j59s0jhf[.]ru | Mar 22, 2018, 7:51 AM | Mar 19, 2019, 4:54 PM |
| 5qvpao0ckjzsw76a7o9d5[.]ru | Mar 22, 2018, 7:47 AM | Mar 19, 2019, 4:45 PM |
| 10mv0yfp9l83bbozpawq3[.]ru | Mar 22, 2018, 6:03AM | Mar 19, 2019, 4:52 PM |
| 2xfonj0lgvpmo2icfp551[.]ru | Mar 22, 2018, 6:00 AM | Mar 19, 2019, 4:44 PM |
| 1d4woaazyq86ap2594rs[.]ru | Mar 22, 2018, 3:46 AM | Mar 19, 2019, 4:54 PM |
| 3y7ayvsmwl2spkeypjf66[.]ru | Mar 22, 2018, 1:46 AM | Mar 19, 2019, 4:47 PM |
| rockethack[.]me | Mar 21, 2018, 6:13 AM | Apr 11, 2018, 12:24 PM |
| www.rockethack[.]me | Mar 21, 2018, 6:13 AM | Mar 26, 2018, 7:22 PM |
| mail-yandex.pp[.]ru | Mar 21, 2018, 6:11 AM | Apr 2, 2018, 4:17 AM |
| passport-yandex.ru[.]com | Mar 21, 2018, 5:01 AM | Apr 17, 2018, 6:01 AM |
| yandex-gibdd[.]online | Mar 21, 2018, 4:21 AM | Apr 10, 2018, 10:23 AM |
| mail-google.com[.]de | Mar 21, 2018, 3:54 AM | Mar 21, 2018, 4:21 AM |

Table A.6 Passive DNS data for IP address 198.98.122.6

| Domain | First Seen (GMT) | Last Seen (GMT) |
|------------------------------|-----------------------|------------------------|
| www.mail-yandex.pp[.]ru | Mar 15, 2018, 9:48 AM | Mar 15, 2018, 12:03 PM |
| rockethack[.]me | Mar 14, 2018, 1:45 AM | Mar 20, 2018, 12:39 PM |
| www.ru-emx[.]ru | Mar 12, 2018, 1:47 AM | Mar 12, 2018, 1:47 AM |
| mail-google.com[.]de | Mar 11, 2018, 4:50 AM | Mar 11, 2018, 5:45 AM |
| www.mail-google.com[.]de | Mar 11, 2018, 4:50 AM | Mar 11, 2018, 5:45 AM |
| mail-yandex.pp[.]ru | Mar 9, 2018, 5:40 AM | Mar 15, 2018, 10:02 AM |
| www.e-mail.pp[.]ru | Mar 5, 2018, 11:48 AM | Mar 17, 2018, 7:46 AM |
| e-mail.pp[.]ru | Mar 5, 2018, 11:48 AM | Sept 9, 2018, 3:46 AM |
| e.mail.ru-u11[.]ru | Feb 28, 2018, 1:44 AM | Feb 2, 2019, 1:56 AM |
| ru-u11[.]ru | Feb 22, 2018, 2:14 AM | Feb 15, 2019, 1:54 AM |
| s-erokhia-authorization[.]ru | Feb 1, 2018, 10:40 AM | Jan 22, 2019, 5:03 AM |

| Domain | First Seen (GMT) | Last Seen (GMT) |
|---|------------------------|------------------------|
| relaunch-account-load-009374882714[.]ru | Feb 1, 2018, 10:40 AM | Jan 15, 2019, 9:20 AM |
| load-account-relaunch-834993884711[.]ru | Jan 31, 2018, 3:08 AM | Jan 25, 2019, 4:50 AM |
| account-load-relaunch-784689934878[.]ru | Jan 29, 2018, 10:30 AM | Jan 22, 2019, 12:05 AM |
| karibjanov-authorization[.]ru | Jan 29, 2018, 6:04 AM | Jan 22, 2019, 2:40 AM |
| ignatkovdmitrij-authorization[.]ru | Jan 28, 2018, 11:28 AM | Jan 23 2018, 4:50 AM |
| mebelstol-authorization[.]ru | Jan 27, 2018, 12:43 AM | Jan 22, 2019, 3:08 AM |
| umlaut-authorization[.]ru | Jan 27, 2018, 11:07 AM | Jan 23, 2019, 6:20 AM |
| svetlana-shaipova-authorization[.]ru | Jan 27, 2018, 11:04 AM | Jan 23, 2019, 6:10 AM |
| gwozdeck-authorization[.]ru | Jan 27, 2018, 10:36 AM | Jan 23, 2019, 6:00 AM |
| ivlevurji-authorization[.]ru | Jan 27, 2018, 3:59 AM | Jan 22, 2019, 2:36 AM |
| osverkanovav7-authorization[.]ru | Jan 27, 2018, 3:48 AM | Jan 23, 2019, 5:30 AM |
| westerosking15-authorization[.]ru | Jan 27, 2018, 3:41 AM | Jan 16, 2019, 3:34 AM |
| miera0909-authorization[.]ru | Jan 27, 2018, 3:00 AM | Jan 22, 2019, 3:13 AM |
| mail-kodeks[.]ru | Jan 16, 2019, 5:14 AM | Jan 8, 2019, 6:28 AM |
| ru-ll[.]ru | Jan 13, 2018, 11:39 AM | Jan 8, 2019, 4:40 AM |
| www.mail.yanex.ru-po[.]ru | Jan 12, 2018, 1:38 AM | Jan 6, 2019, 7:19 AM |
| mail.yanex.ru-po[.]ru | Jan 12, 2018, 1:38 AM | Jan 7, 2019, 11:30 AM |
| www.ru-po[.]ru | Jan 12, 2018, 1:38 AM | Jan 6, 2019, 7:09 AM |
| ru-po[.]ru | Jan 12, 2018, 1:07 AM | Jan 8, 2019, 4:41 AM |
| ru-emx[.]ru | Dec 25, 2017, 12:17 AM | Jun 24, 2018, 7:32 AM |
| ru-imap[.]ru | Dec 25, 2017, 12:17 AM | Nov 23, 2018, 7:31 AM |
| www.e.mail.ru-authpopup[.]ru | Nov 20, 2017, 7:20 AM | Nov 20, 2017, 8:15 AM |
| e.mail.ru-authpopup[.]ru | Nov 20, 2017, 7:20 AM | Nov 20, 2017, 8:15 AM |
| mail.yandex.ru-authpopup[.]ru | Nov 20, 2017, 5:10 AM | Nov 25, 2017, 12:57 AM |
| www.mail.yandex.ru-authpopup[.]ru | Nov 20, 2017, 5:10 AM | Nov 20, 2017, 5:10 AM |
| www.ru-authpopup[.]ru | Nov 20, 2017, 4:40 AM | Nov 20, 2017, 4:40 AM |
| ru-authpopup[.]ru | Nov 20, 2017, 4:40 AM | Nov 20, 2017, 4:40 AM |

Table A.7. Passive DNS data for IP address 139.60.163.35

Eventually, rockethack[.]me moved to IP address 139.60.163[.]53. On this IP address, the website of Rockethack was available until the end of 2020, even when rockethack[.]me did not resolve anymore. This whole chain makes us confident enough to attribute the original phishing emails to Rockethack/Void Balaur.

Appendix B

The attribution of attacks described in the eQualitie and Amnesty International reports.

EQualitie mentions the origin IP addresses for web attacks against three media websites that publish content on Uzbekistan and one website about human rights issues in Palestine.

| IP address | First web attack | Last web attack |
|-----------------|------------------|-----------------|
| 46.45.137[.]74 | 2016 | 2017 |
| 51.15.94[.]245 | Sep 2018 | Feb 2019 |
| 139.60.163[.]29 | Oct 2017 | Aug 2018 |

Table B.1. Origin IP addresses used in the web attacks against three Uzbek-focused media websites and one Palestine-focused website

| Domain | Created | Registrant email address or SOA rname record |
|------------------------|--------------|--|
| my-id[.]top | Oct 16, 2017 | b.adan1@walla.co.il |
| email-service[.]host | Oct 14, 2018 | denismininlan@gmail.com |
| myconnection[.]website | Nov 3, 2018 | denismininlan@gmail.com |

Table B.2. Domains used in the web attacks against three Uzbek-focused media websites and one Palestine-focused website

An Amnesty International report expanded on the original report from eQualitie. One crucial IP address that was listed in Amnesty International’s list of indicators was 51.83.97.40. The following table lists passive DNS data for this IP address:

| Hostname | First seen (GMT) | Last seen (GMT) |
|--------------------------------|------------------------|------------------------|
| www.myaccount-support[.]top | Mar 14, 2020, 1:04 AM | Mar 20, 2020, 12:56 AM |
| www.accountsgoog1e[.]com | Mar 14, 2020, 12:50 AM | Jun 11, 2020, 12:49 AM |
| www.gmail-warning[.]top | Mar 14, 2020, 12:45 AM | May 20, 2020, 12:55 AM |
| www.mail-google[.]email | Mar 13, 2020, 11:35 AM | Jun 15, 2020, 12:43 AM |
| accounts.accountsgoog1e[.]com | Mar 12, 2020, 6:44 AM | Mar 12, 2020, 6:44 AM |
| play.accountsgoog1e[.]com | Mar 12, 2020, 6:44 AM | Mar 12, 2020, 6:44 AM |
| www.accounts.mail-auth[.]email | Aug 26, 2019, 7:29 AM | Aug 26, 2019, 7:29 AM |
| testdom3[.]xyz | Aug 19, 2019, 9:05 AM | Nov 10, 2019, 6:10 AM |

| Hostname | First seen (GMT) | Last seen (GMT) |
|------------------------------------|------------------------|------------------------|
| www.lifesonnik[.]xyz | Aug 17, 2019, 4:44 AM | Aug 28, 2019, 3:02 AM |
| lifesonnik[.]xyz | Aug 17, 2019, 4:35 AM | Oct 13, 2019, 8:49 AM |
| www.testdom3[.]xyz | Aug 12, 2019, 4:51 AM | Nov 5, 2019, 10:49 AM |
| www1.testdom3[.]xyz | Aug 11, 2019, 4:26 AM | Aug 11, 2019, 4:26 AM |
| adservice.mail-auth[.]email | Jul 21, 2019, 1:32 AM | Sep 13, 2019, 10:14 AM |
| desktest1[.]xyz | Jul 17, 2019, 5:57 AM | Jul 19, 2019, 4:06 AM |
| accounts.mail-auth[.]email | Jul 16, 2019, 1:58 AM | Sep 14, 2019, 6:48 AM |
| mynavyfedera1[.]org | Jul 16, 2019, 6:47 AM | Jul 17, 2019, 1:57 AM |
| mynavyfedral[.]org | Jul 16, 2019, 6:29 AM | Jul 17, 2019, 1:06 AM |
| id-support-email[.]com | Jul 11, 2019, 9:02 AM | Jul 11, 2019, 9:02 AM |
| static.corp.account-mail[.]info | Jul 2, 2019, 11:28 AM | Jul 2, 2019, 11:28 AM |
| mail-auth[.]email | Jul 1, 2019, 3:32 AM | Sep 18, 2019, 2:43 AM |
| com-google[.]site | Jul 1, 2019, 3:32 AM | Jul 1, 2019, 7:08 AM |
| fonts.badoo-account-security[.]com | Jun 25, 2019, 9:38 AM | Jun 25, 2019, 9:38 AM |
| com-gm[.]site | Jun 24, 2019, 9:52 AM | Jun 24, 2019, 10:25 AM |
| com-enter[.]site | Jun 24, 2019, 1:45 AM | Jun 24, 2019, 2:35 AM |
| badoo-account-security[.]com | Jun 24, 2019, 1:08 AM | Jun 26, 2020, 8:33 AM |
| vkontak1e[.]com | Jun 24, 2019, 12:48 AM | Jul 14, 2019, 2:16 AM |
| contacts.myaccount-support[.]top | Jun 23, 2019, 2:09 AM | Oct 7, 2019, 1:16 AM |
| accounts.myaccount-support[.]top | Jun 21, 2019, 8:09 AM | Apr 1, 2020, 10:45 AM |
| store.account-mail[.]info | Jun 21, 2019, 3:52 AM | Jun 21, 2019, 3:52 AM |
| play.myaccount-support[.]top | Jun 21, 2019, 3:52 AM | Sep 29, 2019, 8:20 AM |
| myaccount.account-mail[.]info | Jun 21, 2019, 3:52 AM | Jun 21, 2019, 3:52 AM |
| myaccount.gmail-warning[.]top | Jun 21, 2019, 3:52 AM | Jun 21, 2019, 3:52 AM |
| ogs.myaccount-support[.]top | Jun 21, 2019, 3:52 AM | Sep 29, 2019, 8:20 AM |
| id.myaccount-support[.]top | Jun 21, 2019, 3:50 AM | Sep 29, 2019, 8:20 AM |
| login.corp.account-mail[.]info | Jun 21, 2019, 3:50 AM | Jun 21, 2019, 3:50 AM |
| mail.myaccount-support[.]top | Jun 21, 2019, 3:50 AM | Sep 29, 2019, 8:20 AM |
| books.myaccount-support[.]top | Jun 21, 2019, 3:50 AM | Sep 29, 2019, 8:20 AM |
| clients1.myaccount-support[.]top | Jun 21, 2019, 3:50 AM | Sep 29, 2019, 8:20 AM |
| accounts.gmail-warning[.]top | Jun 21, 2019, 3:48 AM | Jun 21, 2019, 3:48 AM |
| adservice.account-mail[.]info | Jun 21, 2019, 3:48 AM | Jun 21, 2019, 3:48 AM |
| accounts.account-mail[.]info | Jun 21, 2019, 3:48 AM | Jun 23, 2019, 3:23 AM |
| productforums.account-mail[.]info | Jun 21, 2019, 12:19 AM | Jun 21, 2019, 11:13 PM |
| adssettings.account-mail[.]info | Jun 20, 2019, 2:03 AM | Jun 20, 2019, 2:03 AM |

| Hostname | First seen (GMT) | Last seen (GMT) |
|-----------------------------|------------------------|------------------------|
| support.account-mail[.]info | Jun 20, 2019, 2:03 AM | Jun 22, 2019, 2:09 AM |
| services.auth-mail[.]email | Jun 19, 2019, 6:43 AM | Jun 19, 2019, 6:43 AM |
| store.auth-mail[.]email | Jun 19, 2019, 5:54 AM | Jun 19, 2019, 5:54 AM |
| m.comericac[.]com | Jun 19, 2019, 3:03 AM | Jun 19, 2019, 3:03 AM |
| www4.comericac[.]com | Jun 19, 2019, 3:02 AM | Jun 19, 2019, 3:02 AM |
| magento.comericac[.]com | Jun 19, 2019, 3:01 AM | Jun. 19, 2019, 3:01 AM |
| store.comericac[.]com | Jun 19, 2019, 3:01 AM | Jun 19, 2019, 3:01 AM |
| shop.comericac[.]com | Jun 19, 2019, 3:01 AM | Jun 19, 2019, 3:01 AM |
| support.auth-mail[.]email | Jun 18, 2019, 9:36 AM | Jun 18, 2019, 9:36 AM |
| www.comericac[.]com | Jun 18, 2019, 9:34 AM | Jun 18, 2019, 9:34 AM |
| com-auth[.]site | Jun 12, 2019, 9:43 AM | Jun 20, 2019, 2:01, AM |
| accountsgoog1e[.]com | Jun 12, 2019, 9:01 AM | Jun 11, 2020, 1:10 AM |
| accountapp[.]xyz | Jun 11, 2019, 12:34 AM | Jun 15, 2019, 11:12 AM |
| frostdank[.]com | Jun 11, 2019, 10:01 AM | Jul 2, 2019, 3:30 AM |
| comericac[.]com | Jun 11, 2019, 9:13 AM | Jun 19, 2019, 8:57 AM |
| nitroqensports[.]eu | Jun 11, 2019, 9:13 AM | Jul 2, 2019, 11:28 AM |
| navyfedera1[.]org | Jun 11, 2019, 9:07 AM | Jun 17, 2019, 10:14 AM |
| accountsgoog1e[.]com | Jun 10, 2019, 4:17 AM | Jun 11, 2019, 7:49 AM |
| account-mail[.]info | Jun 10, 2019, 2:39 AM | Jul 2, 2019, 11:28 AM |
| auth-mail[.]email | Jun 10, 2019, 1:57 AM | Jun 19, 2019, 4:20 AM |
| voice98765[.]online | Jun 10, 2019, 1:39 AM | Jun 12, 2019, 4:47 AM |
| mail-google[.]email | Jun 10, 2019, 1:39 AM | Jun 15, 2020, 1:12 AM |
| myaccount-support[.]top | Jun 10, 2019, 1:36 AM | Apr 20, 2020, 11:06 AM |
| gmail-warning[.]top | Jun 10, 2019, 1:36 AM | May 20, 2020, 12:55 AM |
| www.auth-google[.]site | Jun 9, 2019, 8:25 AM | Jun 20, 2019, 2:03 AM |
| auth-google[.]site | Jun 9, 2019, 8:21 AM | Jun 20, 2019, 2:03 AM |
| rc-room[.]com | Jun 6, 2019, 3:34 AM | Jun 18, 2019, 12:43 AM |

Table B.3. Passive DNS for IP address 51.83.97.40

The public SSH key of IP address 51.83.97[.]40 had the fingerprint cc:97:53:b8:51:52:d8:5f:fa:1e:39:db:2c:ce:12:6b between June 4, 2019 and June 24, 2019. A couple of these websites moved to the IP address 134.209.86[.]7 later in 2019 (this IP address also hosted google-activity[.]pw, which we have previously related to Void Balaur in Appendix A). This establishes a direct link between the Amnesty International report, the eQualitie report and our research on Void Balaur.

Besides this, we found that in 2020, Void Balaur targeted the editor-in-chief of one of the websites that was attacked in 2018 and 2019, according to the eQualitie report.

Appendix C

This appendix shows how we traced the activities of Void Balaur to the year 2015. We started with some of the indicators that were published originally in the eQuality and Amnesty International report: my-cabinet[.]com, mail-help-support[.]info, auth-mail[.]me, auth-mail[.]com, and mail-support[.]info. We can relate these domain names to mx-delivery[.]com by looking at the pattern of hostnames in a large database of passive DNS data. We found that at least two forms of hostnames are virtually unique in that database, when we discard one or two for obvious false positives.

| Hostname | IP address | First accessed | Last accessed |
|--|-----------------|----------------|---------------|
| resize.google.com.my-cabinet[.]com | 139.60.163[.]29 | Nov 20, 2017 | Feb 27, 2018 |
| resize.google.com.mx-delivery[.]com | 80.79.125[.]120 | Jan 22, 2016 | Mar 7, 2016 |
| resize.google.com.mail-help-support[.]info | 46.45.137[.]74 | Nov 14, 2016 | Nov 19, 2016 |

Table C.1. Passive DNS data of hostnames starting with resize.google[.]com

| Hostname | IP address | First | Last |
|---------------------------------------|-------------------|--------------|--------------|
| see.document.plus20.slack[.]com | 205.251.219[.]142 | Jun 11, 2019 | Jun 11, 2019 |
| see.document.autohome.com[.]cn | 219.148.35[.]254 | Sep 15,2020 | Sep 15, 2020 |
| see.document.auth-mail[.]me | 46.45.137[.]74 | Aug 11, 2017 | Aug 11, 2017 |
| see.document.auth-mail[.]com | 46.45.137[.]74 | Aug 25, 2017 | Sep 21, 2017 |
| see.document.my-cabinet[.]com | 139.60.163[.]29 | Nov 17, 2017 | May 7, 2018 |
| see.document.mx-delivery[.]com | 80.79.125[.]120 | Jan 22, 2016 | Mar 7, 2016 |
| see.document.mx-delivery[.]com | 107.150.171[.]182 | May 19, 2016 | May 19, 2016 |
| see.document.mail-support[.]info | 46.45.137[.]74 | Apr 11, 2017 | Apr 11, 2017 |
| see.document.mail-help-support[.]info | 46.45.137[.]74 | Nov 14, 2016 | Nov 19, 2016 |

Table C.2. Passive DNS data of hostnames starting with see.document

This offers a clear correlation between Void Balaur and the domain name mx-delivery[.]com — though this is not 100% foolproof. The domain name mx-delivery[.]com was registered on September 16, 2015; therefore, we think that Void Balaur has been active since at least 2015.

References

- 1 Amnesty International. (Oct. 19, 2019). *Amnesty International*. “Moroccan human rights defenders targeted using malicious NSO Israeli spyware.” Accessed on Oct. 14, 2021, at <https://www.amnesty.org/en/latest/press-release/2019/10/moroccan-human-rights-defenders-targeted-using-malicious-nso-israeli-spyware/>.
- 2 Jack Stubbs and Christopher Bing. (Oct. 3, 2019). *Reuters*. “Uzbek spies attacked dissidents with off-the-shelf hacking tools.” Accessed on Oct. 14, 2021, at <https://www.reuters.com/article/us-uzbekistan-cyber-idUSKBN1W10YL>.
- 3 Gabrielle Tétrault-Farber. (July 27, 2020). *Reuters*. “Self-exiled Belarus presidential contender pins hopes on new ‘Joan of Arc’.” Accessed on Oct. 14, 2021, at <https://www.reuters.com/article/us-belarus-election-idUSKCN24R0QG>.
- 4 Trend Micro. (July 21, 2015). *Trend Micro*. “The Hacking Team Leak, Zero-Days, Patches, and More Zero-Days.” Accessed on Oct. 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-hacking-team-leak-zero-days-patches-and-more-zero-days>.
- 5 United Nations. (July 28, 2020). *United Nations*. “Use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination.” Accessed on Oct. 14, 2021, at <https://undocs.org/en/A/75/259>.
- 6 United Nations. (Feb., 2021). *United Nations*. “Working Group on the Use of Mercenaries Call for Input: Report on the provision of military and security cyber products and services by ‘cyber mercenaries’ and its human rights impact.” Accessed on Oct. 14, 2021, at <https://www.ohchr.org/Documents/Issues/Mercenaries/WG/CyberMercenaries/AccessNow.pdf>.
- 7 Feike Hacquebord. (April 25, 2017). *Trend Micro*. “Two Years of Pawn Storm: Examining an Increasingly Relevant Threat.” Accessed on Oct. 14, 2021, at <https://documents.trendmicro.com/assets/wp/wp-two-years-of-pawn-storm.pdf>.
- 8 Raphael Satter. (May 8, 2018). *Associated Press News*. “Russian hackers posed as IS to threaten military wives.” Accessed on Oct. 14, 2021, at <https://apnews.com/article/mi-state-wire-or-state-wire-russia-co-state-wire-north-america-4d174e45ef5843a0ba82e804f080988f>.
- 9 Amnesty International. (Oct. 19, 2019). *Amnesty International*. “Moroccan human rights defenders targeted using malicious NSO Israeli spyware.” Accessed on Oct. 14, 2021, at <https://www.amnesty.org/en/latest/press-release/2019/10/moroccan-human-rights-defenders-targeted-using-malicious-nso-israeli-spyware/>.
- 10 Jack Stubbs and Christopher Bing. (Oct. 3, 2019). *Reuters*. “Uzbek spies attacked dissidents with off-the-shelf hacking tools.” Accessed on Oct. 14, 2021, at <https://www.reuters.com/article/us-uzbekistan-cyber-idUSKBN1W10YL>.
- 11 Etienne. (May 9, 2019). *eQualitie*. “Deflect Labs Report #6: Phishing and Web Attacks Targeting Uzbek Human Right Activists and Independent Media.” Accessed on Oct. 14, 2021, at <https://equalit.ie/deflect-labs-report-6/>.
- 12 Andrei Zakharov. (May 27, 2019). *BBC News*. “Russian data theft: Shady world where all is for sale.” Accessed on Oct. 14, 2021, at <https://www.bbc.com/news/world-europe-48348307>.
- 13 Joshua Yaffa. (March 31, 2021). *The New Yorker*. “How Bellingcat Unmasked Putin’s Assassins.” Accessed on Oct. 14, 2021, at <https://www.newyorker.com/news/dispatch/how-bellingcat-unmasked-putins-assassins>.
- 14 Etienne. (May 9, 2019). *eQualitie*. “Deflect Labs Report #6: Phishing and Web Attacks Targeting Uzbek Human Right Activists and Independent Media.” Accessed on Oct. 14, 2021, at <https://equalit.ie/deflect-labs-report-6/>.
- 15 Amnesty International. (March 12, 2020). *Amnesty International*. “Targeted Surveillance Attacks in Uzbekistan: An Old Threat with New Techniques.” Accessed on Oct. 14, 2021, at <https://www.amnesty.org/en/latest/research/2020/03/targeted-surveillance-attacks-in-uzbekistan-an-old-threat-with-new-techniques/>.
- 16 BBC News. (Dec. 29, 2017). *BBC News*. “Exmo Bitcoin exchange manager freed by kidnappers.” Accessed on Oct. 14, 2021, at <https://www.bbc.com/news/business-42518235>.
- 17 Feike Hacquebord et al. (Sept. 17, 2019). *Trend Micro*. “Ready or Not for PSD2: The Risks of Open Banking.” Accessed on Oct. 14, 2021, at https://documents.trendmicro.com/assets/white_papers/wp-PSD2-The-Risks-of-Open-Banking.pdf.
- 18 strazzer. (Jan. 22, 2021). *GitHub*. “anti-emulator.” Accessed on Oct. 14, 2021, at <https://github.com/strazzer/anti-emulator/tree/master>.
- 19 blikoon. (Dec. 2, 2019). *GitHub*. “Rooster.” Accessed on Oct. 14, 2021, at <https://github.com/blikoon/Rooster>.

- 20 Feike Hacquebord. (March 19, 2020). *Trend Micro*. "Pawn Storm in 2019: A Year of Scanning and Credential Phishing on High-Profile Targets." Accessed on Oct. 14, 2021, at https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf.
- 21 Bill Marczak et al. (Dec. 20, 2020). *The Citizen Lab*. "The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit." Accessed on Oct. 14, 2021, at <https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/>.
- 22 Tom Burt. (Dec. 21, 2020). *Microsoft*. "Cyber mercenaries don't deserve immunity." Accessed on Oct. 14, 2021, at <https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/>.
- 23 Craig Gibson et al. (July 29, 2021). *Trend Micro*. "Islands of Telecom: Risks in IT." Accessed on Oct. 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/islands-of-telecom-risks-in-it>.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com



| research 