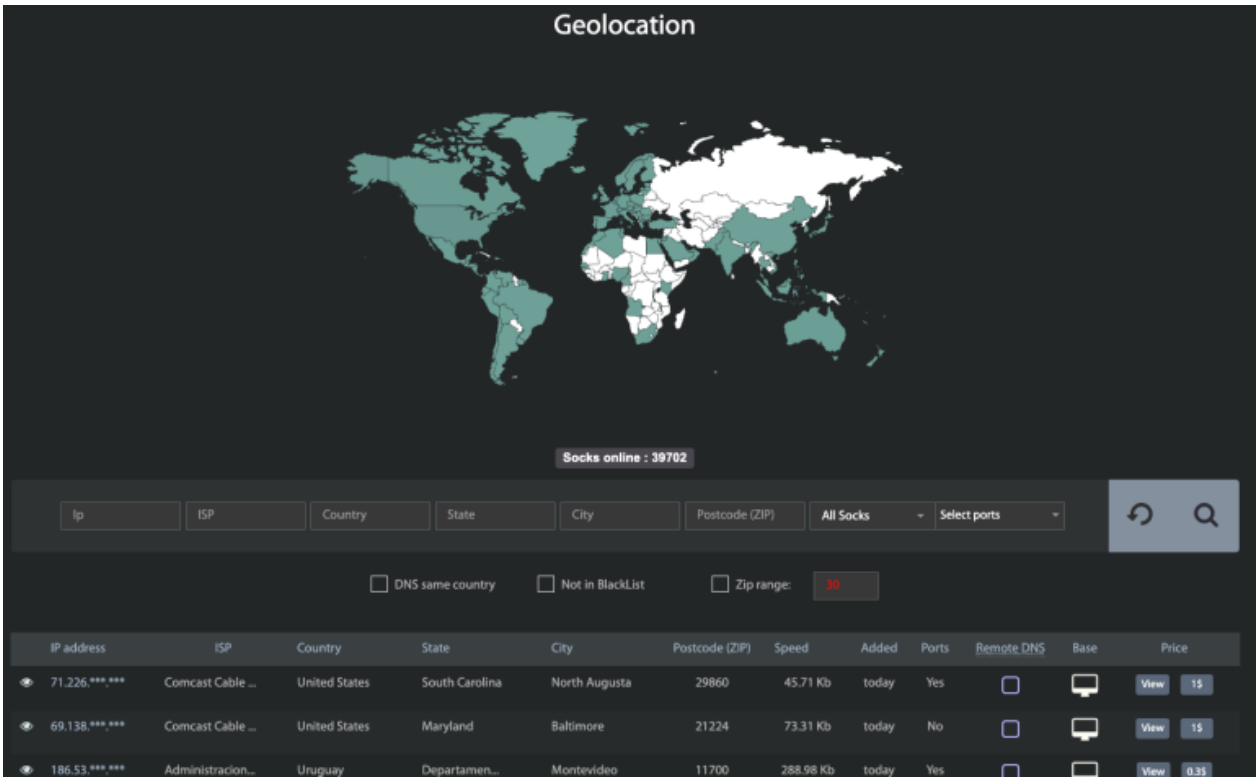
Giving a Face to the Malware Proxy Service ‘Faceless’

krebsonsecurity.com/2023/04/giving-a-face-to-the-malware-proxy-service-faceless/

For the past seven years, a malware-based proxy service known as “**Faceless**” has sold anonymity to countless cybercriminals. For less than a dollar per day, Faceless customers can route their malicious traffic through tens of thousands of compromised systems advertised on the service. In this post we’ll examine clues left behind over the past decade by the proprietor of Faceless, including some that may help put a face to the name.



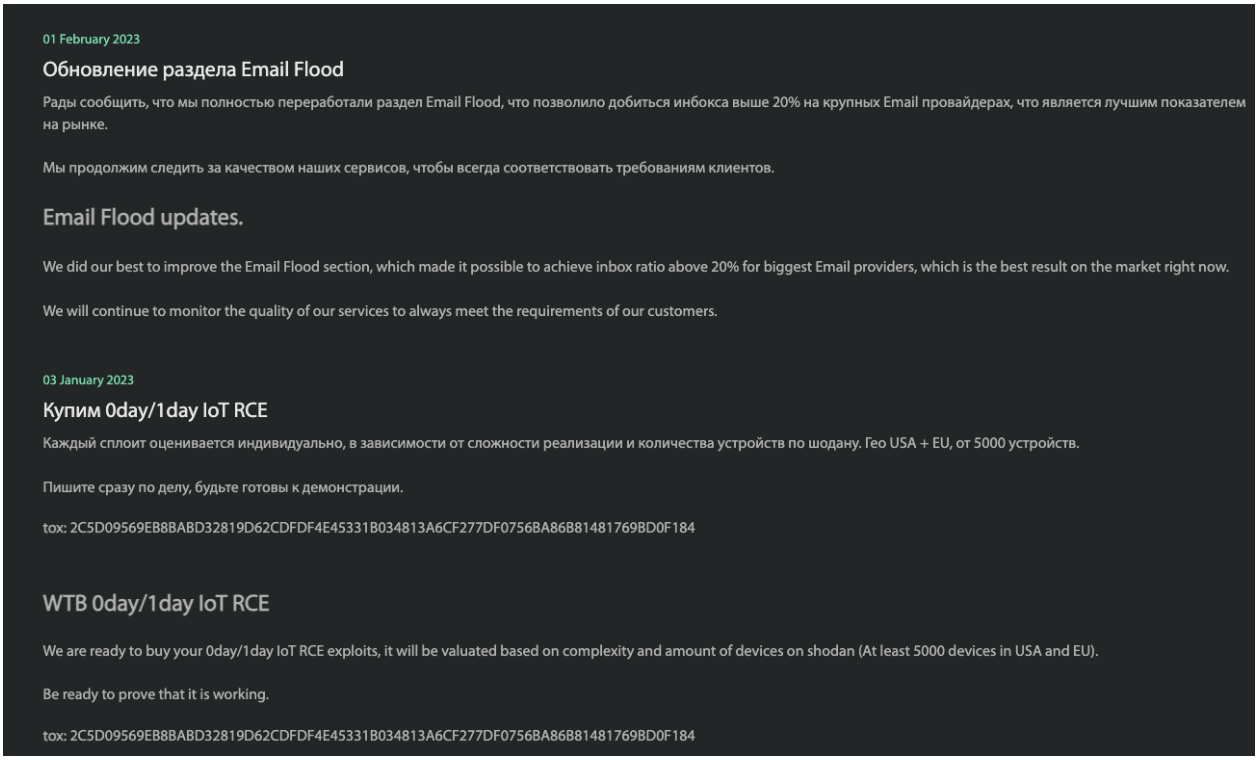
The proxy lookup page inside the malware-based anonymity service Faceless. Image: spur.us.

Riley Kilmer is co-founder of Spur.us, a company that tracks thousands of VPN and proxy networks, and helps customers identify traffic coming through these anonymity services. Kilmer said Faceless has emerged as one of the underground’s most reliable malware-based proxy services, mainly because its proxy network has traditionally included a great many compromised “Internet of Things” devices — such as media sharing servers — that are seldom included on malware or spam block lists.

Kilmer said when Spur first started looking into Faceless, they noticed almost every Internet address that Faceless advertised for rent also showed up in the IoT search engine Shodan.io as a media sharing device on a local network that was somehow exposed to the Internet.

“We could reliably look up the [fingerprint] for these media sharing devices in Shodan and find those same systems for sale on Faceless,” Kilmer said.

In January 2023, the Faceless service website said it was willing to pay for information about previously undocumented security vulnerabilities in IoT devices. Those with IoT zero-days could expect payment if their exploit involved at least 5,000 systems that could be identified through Shodan.



01 February 2023

Обновление раздела Email Flood

Рады сообщить, что мы полностью переработали раздел Email Flood, что позволило добиться инбокса выше 20% на крупных Email провайдерах, что является лучшим показателем на рынке.

Мы продолжим следить за качеством наших сервисов, чтобы всегда соответствовать требованиям клиентов.

Email Flood updates.

We did our best to improve the Email Flood section, which made it possible to achieve inbox ratio above 20% for biggest Email providers, which is the best result on the market right now.

We will continue to monitor the quality of our services to always meet the requirements of our customers.

03 January 2023

Купим 0day/1day IoT RCE

Каждый сплоит оценивается индивидуально, в зависимости от сложности реализации и количества устройств по шодану. Гео USA + EU, от 5000 устройств.

Пишите сразу по делу, будьте готовы к демонстрации.

tox: 2C5D09569EB8BABD32819D62CDFDF4E45331B034813A6CF277DF0756BA86B81481769BD0F184

WTB 0day/1day IoT RCE

We are ready to buy your 0day/1day IoT RCE exploits, it will be valuated based on complexity and amount of devices on shodan (At least 5000 devices in USA and EU).

Be ready to prove that it is working.

tox: 2C5D09569EB8BABD32819D62CDFDF4E45331B034813A6CF277DF0756BA86B81481769BD0F184

Notices posted for Faceless users, advertising an email flooding service and soliciting zero-day vulnerabilities in Internet of Things devices.

Recently, Faceless has shown ambitions beyond just selling access to poorly-secured IoT devices. In February, Faceless re-launched a service that lets users drop an email bomb on someone — causing the target's inbox to be filled with tens of thousands of junk messages.

And in March 2023, Faceless started marketing a service for looking up Social Security Numbers (SSNs) that claims to provide access to "the largest SSN database on the market with a very high hit rate."

Kilmer said Faceless wants to become a one-stop-fraud-shop for cybercriminals who are seeking stolen or synthetic identities from which to transact online, and a temporary proxy that is geographically close to the identity being sold. Faceless currently sells this bundled product for $9 — $8 for the identity and $1 for the proxy.

"They're trying to be this one-stop shop for anonymity and personas," Kilmer said. "The service basically says 'here's an SSN and proxy connection that should correspond to that user's location and make sense to different websites.'"

MRMURZA

Faceless is a project from **MrMurza**, a particularly talkative member of more than a dozen Russian-language cybercrime forums over the past decade. According to cyber intelligence firm Flashpoint, MrMurza has been active in the Russian underground since at least September 2012. Flashpoint said MrMurza appears to be extensively involved in botnet activity and “drops” — fraudulent bank accounts created using stolen identity data that are often used in money laundering and cash-out schemes.

Faceless grew out of a popular anonymity service called **iSocks**, which was launched in 2014 and advertised on multiple Russian crime forums as a proxy service that customers could use to route their malicious Web traffic through compromised computers.

Flashpoint says that in the months before iSocks went online, MrMurza posted on the Russian language crime forum **Verified** asking for a serious partner to assist in opening a proxy service, noting they had a botnet that was powered by malware that collected proxies with a 70 percent infection rate.

MrMurza’s Faceless advertised on the Russian-language cybercrime forum ProCrd. Image: Darkbeast/Ke-la.com.

In September 2016, MrMurza sent a message to all iSocks users saying the service would soon be phased out in favor of Faceless, and that existing iSocks users could register at Faceless for free if they did so quickly — before Faceless began charging new users registration fees between $50 and $100.

Verified and other Russian language crime forums where MrMurza had a presence have been hacked over the years, with contact details and private messages leaked online. In a 2014 private message to the administrator of Verified explaining his bona fides, MrMurza said he received years of positive feedback as a seller of stolen Italian credit cards and a vendor of drops services.

MrMurza told the Verified admin that he used the nickname **AccessApproved** on multiple other forums over the years. MrMurza also told the admin that his account number at the now-defunct virtual currency Liberty Reserve was **U1018928**.

According to cyber intelligence firm Intel 471, the user AccessApproved joined the Russian crime forum **Zloy** in Jan. 2012, from an Internet address in Magnitogorsk, RU. In a 2012 private message where AccessApproved was arguing with another cybercriminal over a deal gone bad, AccessApproved asked to be paid at the Liberty Reserve address U1018928.

In 2013, U.S. federal investigators seized Liberty Reserve and charged its founders with facilitating billions of dollars in money laundering tied to cybercrime. The Liberty Reserve case was prosecuted out of the Southern District of New York, which in 2016 published a list of account information (PDF) tied to thousands of Liberty Reserve addresses the government asserts were involved in money laundering.

That document indicates the Liberty Reserve account claimed by MrMurza/AccessApproved — U1018928 — was assigned in 2011 to a "**Vadim Panov**" who used the email address **lesstroy@mgn.ru**.

PANOV

Constella Intelligence, a threat intelligence firm that tracks breached databases, says lesstroy@mgn.ru was used for an account "Hackerok" at the accounting service klerk.ru that was created from an Internet address in Magnitogorsk. The password chosen by this user was "**1232**."

In addition to selling access to hacked computers and bank accounts, both MrMurza and AccessApproved ran side hustles on the crime forums selling clothing from popular retailers that refused to ship directly to Russia.

On one cybercrime forum where AccessApproved had clothing customers, denizens of the forum created a lengthy discussion thread to help users identify incoming emails associated with various reshipping services advertised within their community. Reshippers tend to rely on a large number of people in the United States and Europe helping to forward packages overseas, but in many cases the notifications about purchases and shipping details would be forwarded to reshipping service customers from a consistent email account.

That thread said AccessApproved's clothing reshipping service forwarded confirmation emails from the address **panov-v@mail.ru**. This address is associated with accounts on two Russian cybercrime forums registered from Magnitogorsk in 2010 using the handle "**Omega^gg4u**."

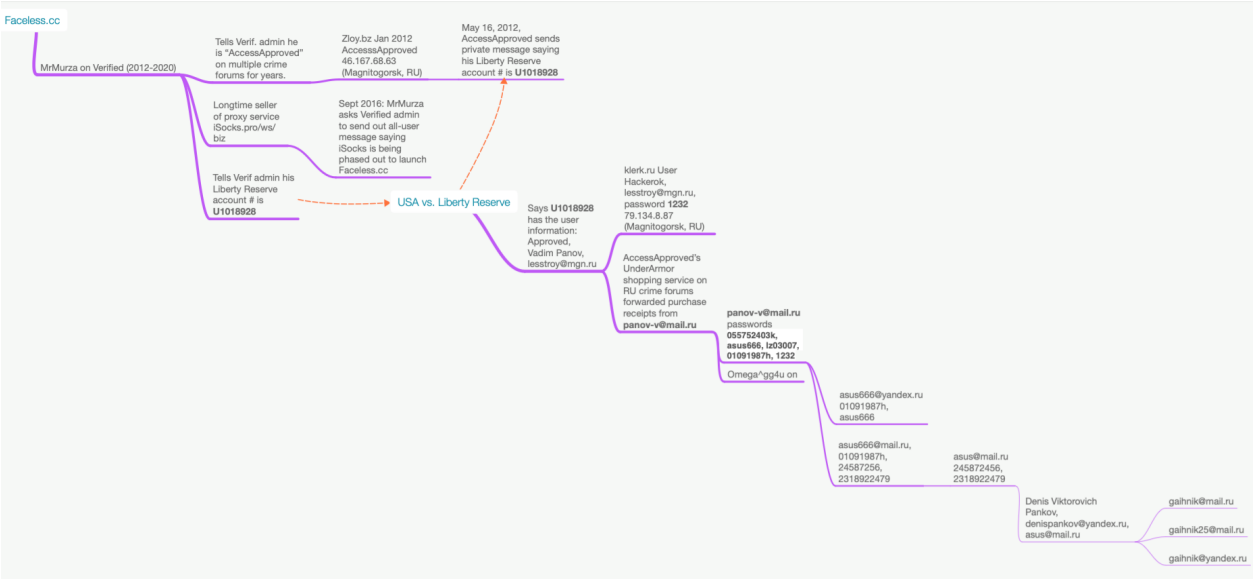
This Omega^gg4u identity sold software that can rapidly check the validity of large batches of stolen credit cards. Interestingly, both Omega^gg4u and AccessApproved also had another niche: Reselling heavily controlled substances — such as human growth hormone and anabolic steroids — from chemical suppliers in China.

A search in Constella on the address panov-v@mail.ru and many variations on that address shows these accounts cycled through the same passwords, including **055752403k**, **asus666**, **01091987h**, and the relatively weak password **1232** (recall that 1232 was picked by whoever registered the lesstroy@mgn.ru account at Klerk.ru).

Constella says the email address **asus666@yandex.ru** relied on the passwords asus666 and 01091987h. The 01091987h password also was used by **asus666@mail.ru**, which also favored the password **24587256**.

Constella further reports that whoever owned the much shorter address **asus@mail.ru** also used the password 24587256. In addition, it found the password **2318922479** was tied to both asus666@mail.ru and asus@mail.ru.

The email addresses asus@mail.ru, **asus2504@mail.ru**, and **zaxar2504@rambler.ru** were all used to register Vkontakte social media accounts for a **Denis ***@VIP*** Pankov**. There are a number of other Vkontakte accounts registered to asus@mail.ru and many variations of this address under a different name. But none of those other profiles appear tied to real-life identities.



A mind map simplifying the research detailed here.

PANKOV

Constella's data shows the email addresses **asus2504@mail.ru** and **zaxar2504@rambler.ru** used the rather unique password **denis250485**, which was also used by the email address **denispankov@yandex.ru** and almost a dozen variations at other

Russian-language email providers.

Russian vehicle registration records from 2016 show the email address denispankov@yandex.ru belongs to **Denis Viktorovich Pankov**, born on April 25, 1985. That explains the "250485" portion of Pankov's favored password. The registration records further indicate that in 2016 Pankov's vehicle was registered in a suburb of Moscow.

Russian incorporation records show that denispankov@yandex.com is tied to **IP Pankov Denis Viktorovich**, a now-defunct transportation company in the Volograd Oblast, a region in southern Russia that shares a long border with western Kazazkhstan.

More recent records for IP Pankov Denis Viktorovich show a microenterprise with this name in Omsk that described its main activity as "retail sale by mail or via the Internet." Russian corporate records indicate this entity was liquidated in 2021.

A reverse password search on "denis250485" via Constella shows this password was used by *more than 75 email addresses*, most of which are some variation of **gaihnik@mail.ru** — such as gaihnik25@mail.ru, or gaihnik2504@rambler.ru.

In 2012, someone posted answers to a questionnaire on behalf of Denis Viktorovich Pankov to a Russian-language discussion forum on Chinese crested dog breeds. The message said Pankov was seeking a puppy of a specific breed and was a resident of Krasnogorsk, a city that is adjacent to the northwestern boundary of Moscow.

The message said Pankov was a then 27-year-old manager in an advertising company, and could be reached at the email address gaihnik@mail.ru.

GAIHNIK

Constella Intelligence shows gaihnik@mail.ru registered at the now-defunct email marketing service **Smart Responder** from an address in Gagarin, which is about 115 miles west of Moscow.

Back in 2015, the user **Gaihnik25** was banned from the online game **World of Tanks** for violating the game's terms that prohibit "bot farming," or the automated use of large numbers of player accounts to win some advantage that is usually related to cashing out game accounts or inventory.

For the past few years, someone using the nickname Gaihnik25 has been posting messages to the Russian-language hacking forum **Gerki[.]pw**, on discussion threads regarding software designed to "brute force" or mass-check online accounts for weak or compromised passwords.

A new member of the Russian hacking forum **Nohide[.]Space** using the handle Gaihnik has been commenting recently about proxy services, credential checking software, and the sale of hacked mailing lists. Gaihnik's first post on the forum concerned private software for checking World of Tanks accounts.

The address gaihnik@mail.ru shows how so many email addresses tied to Pankov were also connected to apparently misleading identities on Vkontakte and elsewhere. Constella found this address was tied to a Vkontakte account for a **Dmitriy Zakarov**.

Microsoft's Bing search engine says gaihnik@mail.ru belongs to 37-year-old Denis Pankov, yet clicking the Mail.ru profile for that user brings up a profile for a much older man by the name **Gavril Zakarov**. However, when you log in to a Mail.ru account and view that profile, it shows that most of the account's profile photos are of a much younger man.

Many of those same photos show up in an online dating profile at dating.ru for the user Gaihnik, a.k.a "Denchik," who says he is a 37-year-old Taurus from Gagarin who enjoys going for walks in nature, staying up late, and being on the Internet.

Mr. Pankov did not respond to multiple requests for comment sent to all of the email addresses mentioned in this story. However, some of those addresses produced detailed error responses; Mail.ru reported that the users panov-v@mail.ru, asus666@mail.ru, and asus2504@mail.ru were terminated, and that gaihnik25@mail.ru is now disabled.

Messages sent to many other email addresses connected via passwords to Pankov and using some variation of asus####@mail.ru also returned similar account termination messages.