

R2 Cyber has prepared the following report for use in the litigation styled *VPN.com LLC v. George Dikian*, pending in the Central District of California. Rod Rasmussen, the principal consultant at R2 Cyber, prepared this report and attaches his *curriculum vitae* to this report, which includes a list of all publications that he has authored in the previous 10 years. Mr. Rasmussen has not testified as an expert by deposition or at trial in any other case in the previous 4 years.

Mr. Rasmussen is an expert in cybersecurity operations and policy. He founded an early cybersecurity company, Internet Identity, in May 2000. He was President and Chief Technical Officer of that company for nearly sixteen years. Internet Identity provided cybersecurity software and services to a large array of companies all over the world. In particular, Mr. Rasmussen advised companies as to cybersecurity threats such as business email compromise, and built teams and systems designed to investigate and mitigate phishing and fraud scams.

In 2012, Mr. Rasmussen was appointed to the Security & Stability Advisory Committee of ICANN. The SSAC is tasked with analyzing internet security threats and providing advice to the ICANN Board, and to the internet community at large, as to how such threats should be analyzed, investigated, and mitigated. Mr. Rasmussen was elected Chair of the SSAC in 2017, and is currently serving his second three-year term in that role. Mr. Rasmussen joined the Messaging, Malware, and Mobile Anti-Abuse Working Group M3AAWG in 2004, and has served as an Expert Advisor to M3AAWG since 2020. M3AAWG is a worldwide industry organization that focuses on the abuse of various messaging systems, with a particular emphasis on email and Mr. Rasmussen has routinely contributed to M3AAWG publications on such topics. Mr. Rasmussen has been a member of the Anti-Phishing Working Group (APWG) since 2004, serving in a variety of leadership positions and publishing fundamental research on phishing activities and techniques over many years. Mr. Rasmussen has been a contributing member of several other industry organizations including the Forum for Incident Security Teams (FIRST), Online Trust Alliance (OTA), and the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC).

Mr. Rasmussen is compensated at the rate of \$500/hour for the study and preparation of this report, and for any testimony to be given by deposition and/or at trial of this matter. To date, Mr. Rasmussen has worked 12.5 hours in this matter.

Mr. Rasmussen's analysis and opinions are as follows:

Business Email Compromise Fraud Definition and Prevalence

Opinion: Business Email Compromise Fraud is extremely common.

Analysis: According to the Federal Bureau of Investigation's 2022 Report to Congress entitled "Business Email Compromise and Real Estate Wire Fraud", Business Email Compromise Fraud

(BEC) is the single most costly crime: “[f]or the past several years, BEC has consistently been the largest dollar loss by victim crime typology reported to IC3, with over \$2.4 billion of adjusted losses in the calendar year 2021.” (Attachment 1, FBI report, pg. 7). BEC has become incredibly common, with 241,206 reported BEC incidents between 2016 and 2021 totaling over \$43 billion in stolen funds. (FBI pg. 13). Furthermore, “IC3 has received an increased number of BEC complaints involving the use of cryptocurrency.” (FBI pg. 13). The FBI explains BEC/EAC as follows:

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests. The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds. (FBI pg. 12).

Business Email Compromise Fraud Against VPN.com

Opinion: The evidence revealed by internet service records and email records proves to a reasonable certainty that the gdikian@yahoo.com Yahoo! Mail address was compromised by an unauthorized actor. Once that account was compromised, the fraudster had access to previously sent emails which included login credentials for Dikian’s HostGator webhosting account. Both accounts then were used in furtherance of the alleged fraud on VPN. Once Dikian was alerted that the Yahoo! Mail address was compromised, he closed off unauthorized access to it by changing the password and deploying two-factor authentication for the account. Shortly thereafter, a new Gmail address was created, george.dikian@gmail.com, which was then used to complete the fraud. Clear evidence from Yahoo!, Google and HostGator shows access at critical times to the Yahoo! Mail and HostGator accounts from two foreign ISPs (one in Portugal, the other an international VPN service), which were also used to create the new Gmail address, and later to delete both that address and rhwdomains@gmail.com within twelve minutes of one another. This proves to a reasonable certainty that the same actor was responsible for all of that activity. It also proves to a reasonable certainty that this activity was performed from within Portugal.

Analysis: On January 28, 2022, access to the Yahoo! Mail account g.dikian@yahoo.com was evidenced by the Yahoo! IP Login Report, which shows the IP address 88.214.185.175 was used to login. (Attachment 2, Yahoo! Subpoena Response).

Those records show use of two foreign ISPs to access that account. The Portuguese internet service provider “MEO - Servicos de Comunicacoes e Multimedia S.A.” (no VPN used with MEO) and the internet service provider “Packethub S.A.” (also known as NordVPN). (Attachment 2, Yahoo! Subpoena Response). The internet IP addresses from the Yahoo! Account have been checked against <https://whatismyipaddress.com/> to determine the ISP and location of each respective IP address, and logged to Attachment 3, “Dikian - Yahoo Google HostGator ISP Analysis”. The orange and red lines represent logins from the two foreign ISPs.

108.177.66.158	March 17 2022 09:44:47	ISP: Google LLC	Services: Datacenter	Country: United States	State/Region: California	City: Mountain View
108.177.68.125	March 17 2022 08:47:16	ISP: Google LLC	Services: Datacenter	Country: United States	State/Region: California	City: Mountain View
94.140.11.103	March 17 2022 08:47:07	ISP: Packethub S.A.	Services: VPN Server	Country: United States	State/Region: Florida	City: Miami
35.211.30.191	March 17 2022 08:44:12	ISP: Google LLC	Services: Datacenter	Country: United States	State/Region: South Carolina	City: North Charleston
94.140.11.103	March 17 2022 08:32:15	ISP: Packethub S.A.	Services: VPN Server	Country: United States	State/Region: Florida	City: Miami
94.140.11.103	March 17 2022 08:11:38	ISP: Packethub S.A.	Services: VPN Server	Country: United States	State/Region: Florida	City: Miami
94.140.11.103	March 17 2022 06:21:52	ISP: Packethub S.A.	Services: VPN Server	Country: United States	State/Region: Florida	City: Miami
2601:6c0:c202:3430:5bd:1b49:ca53:a4c9	March 16 2022 14:48:08	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:5bd:1b49:ca53:a4c9	March 16 2022 14:48:07	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:5bd:1b49:ca53:a4c9	March 16 2022 14:48:07	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:3c46:765f:a03d:751e	March 16 2022 13:02:41	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:3c46:765f:a03d:751e	March 16 2022 13:01:17	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
185.216.74.163	March 16 2022 07:09:10	ISP: Packethub S.A.	Services: VPN Server	Country: United States	State/Region: California	City: Los Angeles
2601:6c0:c202:3430:535:baeb:7a05:c024	March 16 2022 04:49:04	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:535:baeb:7a05:c024	March 16 2022 04:48:02	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
88.214.186.213	March 16 2022 02:26:43	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Porto	City: Maia
2600:387:9:3::1b	March 15 2022 19:12:12	ISP: AT&T Mobility LLC	Services: None detected	Country: United States	State/Region: Washington	City: Redmond
2600:387:9:3::49	March 13 2022 03:23:14	ISP: AT&T Mobility LLC	Services: None detected	Country: United States	State/Region: Washington	City: Redmond
2601:6c0:c202:3430:3d07:f13c:be6e:a6d6	March 08 2022 18:30:24	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:201a:7805:bcd:e452	March 08 2022 17:52:49	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
88.214.160.194	March 08 2022 16:16:09	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Viana do Castelo	City: Viana do Castelo
2600:387:9:3::c1	March 06 2022 19:53:09	ISP: AT&T Mobility LLC	Services: None detected	Country: United States	State/Region: Washington	City: Redmond
2600:387:9:3::46	March 01 2022 18:00:33	ISP: AT&T Mobility LLC	Services: None detected	Country: United States	State/Region: Washington	City: Redmond
88.214.163.17	March 01 2022 11:23:19	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Porto	City: Porto
2601:6c0:c202:3430:3d07:f13c:be6e:a6d6	February 28 2022 11:46:03	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:44a:a9:eb77:629f	February 22 2022 16:30:27	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:44a:a9:eb77:629f	February 22 2022 00:58:45	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
88.214.186.154	February 18 2022 08:42:58	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Porto	City: Maia
2601:6c0:c202:3430:9c65:dedd:bb2:f289	February 15 2022 16:23:59	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:3430:9c65:dedd:bb2:f289	February 15 2022 14:33:04	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
88.214.184.195	February 11 2022 01:39:40	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Vila Real	City: Vila Real
2601:6c0:c202:3430:9c65:dedd:bb2:f289	February 09 2022 03:04:16	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2600:387:9:3::28	February 08 2022 15:38:25	ISP: AT&T Mobility LLC	Services: None detected	Country: United States	State/Region: Washington	City: Redmond
2601:6c0:c202:3430:b079:940b:aa0c:77ca	February 02 2022 19:46:27	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
2601:6c0:c202:ccc0:873a	February 01 2022 15:30:01	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
73.156.249.50	February 01 2022 15:12:41	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Cape Coral
2601:6c0:c202:ccc0:873a	January 31 2022 01:17:09	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
88.214.185.175	January 28 2022 01:39:04	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Viana do Castelo	City: Viana do Castelo
2601:6c0:c202:ccc0:6486:af6b:48cb:401e	January 27 2022 09:40:03	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Naples
73.156.249.50	January 25 2022 14:29:01	ISP: Comcast Cable Communications LI	Services: None detected	Country: United States	State/Region: Florida	City: Cape Coral

The cybercriminal gained access to Dikian’s account at Hostgator.com between April 4, 2022 and May 2, 2022. The compromised Yahoo! Mail account contained a 2017 sent email from that account to Dikian’s web developer at that time (Daniel Rapaport), which contained login info for the Hostgator account. (Attachment 7). This account also was accessed through the same foreign ISPs, MEO Wifi Customers NAT and Packethub S.A., along with one login from LVNET Ltd., which is listed as a “public proxy server” on whereismyip.com:

Hostgator				
Danial Rapaport (info@networkprograms.net)	88.214.161.103	[2022-04-04 08:46:02]	ISP: MEO Wifi Customers NAT	Services: None detected
Danial Rapaport (info@networkprograms.net)	185.203.218.190	[2022-04-24 07:38:31]	ISP: Packethub S.A.	Services: VPN Server
Danial Rapaport (info@networkprograms.net)	185.203.218.188	[2022-04-25 08:49:39]	ISP: Packethub S.A.	Services: VPN Server
Danial Rapaport (info@networkprograms.net)	185.216.74.163	[2022-04-27 07:18:35]	ISP: Packethub S.A.	Services: VPN Server
Danial Rapaport (info@networkprograms.net)	88.214.163.170	[2022-04-28 20:10:47]	ISP: MEO Wifi Customers NAT	Services: None detected
Danial Rapaport (info@networkprograms.net)	45.15.176.211	[2022-05-01 17:35:59]	ISP: LVNET Ltd	Services: Datacenter
Danial Rapaport (info@networkprograms.net)	185.216.74.162	[2022-05-02 02:06:07]	ISP: Packethub S.A.	Services: VPN Server

After the account was accessed, the subdomain intermediar.89.com was created within Dikian’s 89.com domain name, which subdomain was later used to further the alleged fraud.

The Gmail addresses rhwdomains@gmail.com and george.dikian@gmail.com were used in furtherance of the alleged fraud. First, rhwdomains@gmail.com was used as the address of a potential buyer of 89.com. Later, george.dikian@gmail.com was used as the purported seller’s email address, after Dikian was alerted to the compromise of g.dikian@yahoo.com and changed the password to lock out the hacker, as set forth further below. Records subpoenaed from Google show the creation date and the deletion date – just twelve minutes apart -- of each of these Gmail addresses as follows:

R2 Cyber

PO Box 88815
Steilacoom, WA 98388
info@r2cyber.com

e-Mail: rhwdomains@gmail.com
Alternate e-Mails:

Created on: 2019-05-24 16:13:50 Z
Terms of Service IP:
Terms of Service Language:
Provider for Consumer Services: Google Ireland Limited
Birthday (Month Day, Year): - -, -

Services: Gmail, Google Hangouts, Web & App Activity, C
Unregistered Services: Is Ams Half Created

Deletion Date: 2022-10-13 17:01:35 Z

e-Mail: george.dikian@gmail.com
Alternate e-Mails:

Created on: 2022-03-17 08:42:27 Z
Terms of Service IP:
Terms of Service Language:
Provider for Consumer Services: Google LLC
Birthday (Month Day, Year): - -, -

Services: Gmail, Google Hangouts, Web & App Activity
Unregistered Services: Is Ams Half Created

Deletion Date: 2022-10-13 16:49:52 Z

(Attachments 4 and 9, from Google Subpoena Response).

Given that the two email addresses were deleted within just twelve minutes of each other, after VPN.com and Dikian began investigating this matter, it is obvious that those two Gmail addresses were almost certainly controlled by the same person -- who impersonated both the fake buyer and seller in the alleged fraudulent transaction.

VPN.com was approached through rhwdomains@gmail.com on March 7, 2022, asking that VPN.com act as broker to purchase the domain name 89.com. VPN.com then sent email to g.dikian@yahoo.com, which was listed in the public WHOIS record for that domain name. Additionally, the fact that VPN.com requested a phone call with Dikian multiple times, but was refused, could have alerted VPN.com to the fact that they were the victim of a Business Email Compromise scheme, as this is another very common tactic used in furtherance of such scams. On March 7, 2022, Sharjil Saleem of VPN.com wrote "George, Can you give me a call at +1 315

R2 Cyber

PO Box 88815
Steilacoom, WA 98388
info@r2cyber.com

675 4078, We can discuss it over phone?”, to which the cybercriminal replied that he would only use email:

From: George Dikian <g.dikian@yahoo.com>
Sent: Tue, 08 Mar 2022 02:31:59 +0000
To: Sharjil Saleem <sharjil@vpn.com>
Subject: Re: 89.com Domain Purchase Inquiry

Sorry email is the option to negotiate

If I would be accepting phone calls I'd be spending the whole day speaking with people.

You contacted me because you said you have a buyer, I gave you my offer and terms.

You should get bak to the buyer if he really is interested.

(Attachment 10).

Between March 7, 2022 and March 11, 2022 that Yahoo! Mail address was used to communicate with VPN.com, pretending to negotiate terms for the sale of 89.com, with a final email to VPN.com sent from g.dikian@yahoo.com on March 11, 2022. That email stated as follows:

R2 Cyber

PO Box 88815
Steilacoom, WA 98388
info@r2cyber.com

From: George Dikian <g.dikian@yahoo.com>
Sent: Fri, 11 Mar 2022 06:41:06 +0000
To: Sharjil Saleem <sharjil@vpn.com>
Subject: Re: 89.com Domain Purchase Inquiry
Attachments:
· Screen Shot 2022-03-08 at 1.24.37 PM.png (625 kb)

No USD please. I mean not for big amounts.

I do receive USD on intermediar.com but only when the sale amount is low.

See the screenshot attached so you understand what I mean.

On Friday, March 11, 2022, 01:22:08 AM EST, Sharjil Saleem <sharjil@vpn.com> wrote:

George.

My buyer is ready to proceed at \$2.5m USD via Escrow.com and Intermediar.com, He pays the fee. and is ready to fund the escrow in 72 hours. Please let me know if there is any window for USD.

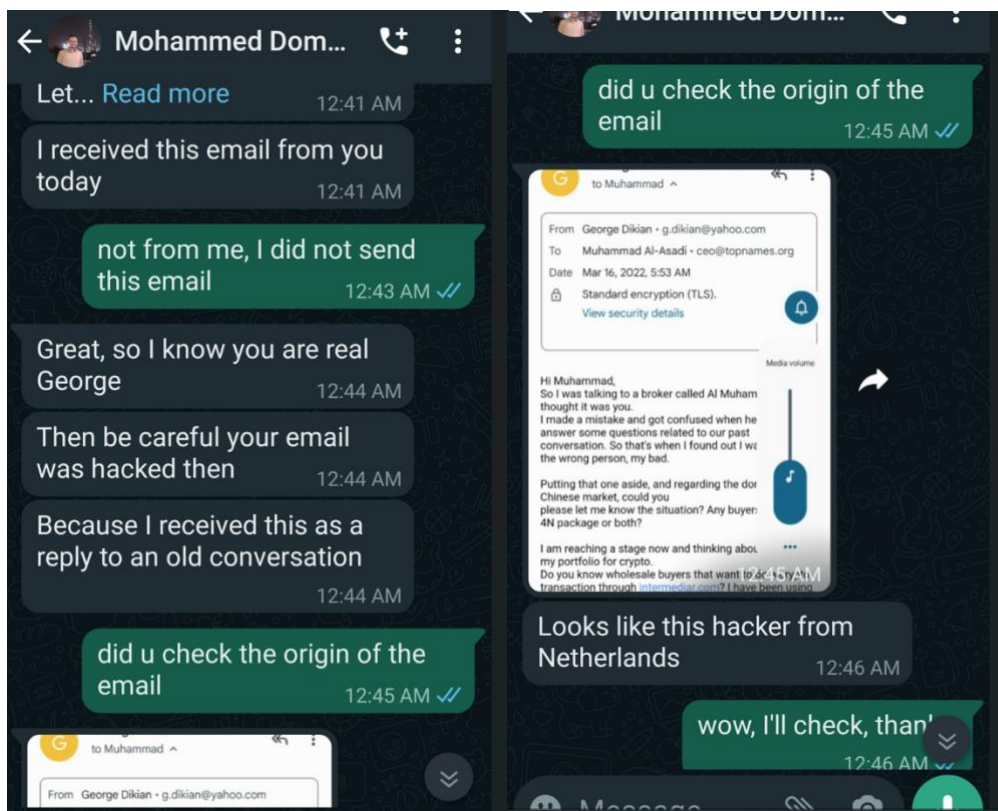
Regards

(See Attachment 5, produced by VPN.com).

However, on March 16, 2022, an acquaintance of Dikian sent a WHATSAPP message to him letting him know about suspicious activity from the g.dikian@yahoo.com address. (Attachment 6, WhatsApp Conversation).

R2 Cyber

PO Box 88815
Steilacoom, WA 98388
info@r2cyber.com



As a result of this conversation, Dikian immediately changed the password on the Yahoo! Mail address g.dikian@yahoo.com, as evidenced by the logs received in response to subpoenas to Yahoo!, which show the password was changed on March 16, 2022. According to www.whatismyip.com, the IP address <2601:6c0:c202:3430:3c46:765f:a03d:751e pw_chg>, which was used to change the password for g.dikian@yahoo.com is traceable to Naples, Florida, which is near Dikian's place of residence. By the next day, the cybercriminal's sessions with Yahoo! Mail had ended permanently. (See Attachments 2 and 3).

Additional IP Addresses:	Fri Mar 18 16:02:49 2022 GMT
	2601:6c0:c202:3430:6d38:4d15:c252:7a9a pw_chg
	Fri Mar 18 15:59:44 2022 GMT undefined enable_2sv
	Fri Mar 18 09:26:27 2022 GMT
	2601:6c0:c202:3430:44bf:58dc:222f:75e1 pw_chg
	Wed Mar 16 13:09:19 2022 GMT
	2601:6c0:c202:3430:3c46:765f:a03d:751e pw_chg

(Attachment 2, Yahoo Subpoena Response, pg. 4). This document shows the exact date, March 16, 2022, that Dikian first changed the password on his Yahoo! Mail account in effort to stop unauthorized access to the account. Two days later, he enabled two-factor authentication in the account. Had Dikian been behind this fraud, he would have had no reason to stop using

R2 Cyber

PO Box 88815
Steilacoom, WA 98388
info@r2cyber.com

g.dikian@yahoo.com. He likely would not have locked himself out of that account and then continued the fraud with a new email account.

Dikian discussed with Kris Hou on April 23, 2022 that he was the target of an identity theft scheme. (Attachment 8, Kris Hou Email).

As noted above, IP Analysis clearly indicates that there was substantial activity from “MEO – Servicos de Comunicacoes e Multimedia S.A.” and “Packethub S.A.” between January 28, 2022 and March 17, 2022. However, immediately after Dikian changed his password, all suspicious activity in his account stopped permanently. (See Attachment 3). Moreover, email to VPN.com from g.dikian@yahoo.com was last sent during login of a suspicious IP address on March 11, 2022, and never again were any suspicious email sent from that account after that. This IP data, along with the corroborating email and SMS communications, paints a clear picture that g.dikian@yahoo.com had been compromised.

After losing access to g.dikian@yahoo.com, the fraudster created the new Gmail address George.Dikian@gmail.com shortly thereafter on March 17, 2022. (See Attachment 9). Then email communications resumed with VPN.com from that email address on April 12:

From: George Dikian <george.dikian@gmail.com>
Sent: Tue, 12 Apr 2022 21:26:50 -0400
To: sharjil@vpn.com
Subject: 89.com

Hi

Is your client still interested in the domain?

The Google subpoena response indicates that that the same ISPs which were used to access g.dikian@yahoo.com were used to log into the newly minted george.dikian@gmail.com. This is clear proof that whoever compromised the Dikian Yahoo! Mail address also created this false Gmail account. Moreover, a comparison of the fake buyer’s email RHWDomains@gmail.com and George.Dikian@gmail.com show that they were deleted within twelve minutes of each other on October 13, 2022. This is obvious proof that both of these emails – both sides of the fraudulent transaction alleged by VPN.com – were created and controlled by the same actor.

That actor made frequent use of the ISP “MEO – Servicos de Comunicacoes e Multimedia S.A.” which is not a virtual private network and is located in Portugal. This is clear

evidence that the perpetrators of this fraud are most likely located in Portugal. Dikian’s travel records should prove that he did not visit Portugal during 2022.

Between April 4, 2022 and May 2, 2022, the cybercriminals logged into Dikian’s HostGator web hosting account seven times, using the credentials of Daniel Rapaport, Dikian’s former web developer. All activity during that period was performed through Rapaport’s credentials. This is explained by the fact that Dikian provided Rapaport those credentials by email in 2017, and these credentials were apparently acquired from the ‘Sent Items’ folder by the cybercriminal when the Yahoo! Account was compromised. (Attachment 7).

The cybercriminals used the same ISPs and IP addresses to log into the HostGator account as were controlling the George.Dikian@gmail.com account, and which had compromised g.dikian@yahoo.com:

Hostgator	IP	Date	ISP	Services	Country	State/Region	City
Daniel Rapaport (info@networkprograms.net)	88.214.161.103	[2022-04-04 08:46:02]	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Lisboa	City: Lisbon
Daniel Rapaport (info@networkprograms.net)	185.203.218.190	[2022-04-24 07:38:31]	ISP: PacketHub S.A.	Services: VPN Server	Country: United States	State/Region: Florida	City: Miami
Daniel Rapaport (info@networkprograms.net)	185.203.218.188	[2022-04-25 08:49:39]	ISP: PacketHub S.A.	Services: VPN Server	Country: United States	State/Region: Florida	City: Miami
Daniel Rapaport (info@networkprograms.net)	185.216.74.163	[2022-04-27 07:38:35]	ISP: PacketHub S.A.	Services: VPN Server	Country: United States	State/Region: California	City: Los Angeles
Daniel Rapaport (info@networkprograms.net)	88.214.163.170	[2022-04-28 20:10:47]	ISP: MEO Wifi Customers NAT	Services: None detected	Country: Portugal	State/Region: Porto	City: Porto
Daniel Rapaport (info@networkprograms.net)	45.15.176.211	[2022-05-01 17:35:59]	ISP: LVNET Ltd	Services: Datacenter	Country: United States	State/Region: New York	City: New York City
Daniel Rapaport (info@networkprograms.net)	185.216.74.162	[2022-05-02 02:06:07]	ISP: PacketHub S.A.	Services: VPN Server	Country: United States	State/Region: California	City: Los Angeles

(IP Analysis, Attachment 3).

HostGator support confirmed that user had created the subdomain “Intermediar.89.com” and then three days later suspended both that subdomain and 89.com, apparently in order to create the false impression to VPN.com that the names were in escrow at the fake escrow service Intermediar.com.



Hello Jack,

Thank you for contacting HostGator.

The user Daniel Rapaport (info@NetworkPrograms[.Net]) logged in on 4/24/22 from the IP address 185.203.218.190. During this login session, the user created the forwarding site 'intermediar.89.com'. Then, on 4/27/22, the user Daniel Rapaport logged in from the IP 185.216.74.163 and suspended both intermediar.89.com and 89.com. There do not appear to have been any filesystem changes during either of those logins.

Attached is a text file with Plesk session logs for the user for the month of April, 2022.

If these actions should not have occurred, please log in to Plesk and change the password for the user (or remove the user) as soon as possible.

Please let us know if we can be of further assistance.

Sincerely,

Jared T.
 Web Administrator
 HostGator.com

This HostGator support record is further corroborating proof that someone other than Dikian was able to access both the HostGator and Yahoo! Mail account, and also created the new Gmail account, in furtherance of the alleged fraud.

R2 Cyber

PO Box 88815
Steilacoom, WA 98388
info@r2cyber.com

Between March 11, 2022 and May 8, 2022, only 4 emails from the purported seller (using george.dikian@gmail.com) were copied to g.dikian@yahoo.com. It appears the fraudster was careful to omit that Yahoo! Mail address from correspondence that they initiated during that period. Sometime after discovering that his Yahoo! Mail account had been compromised, Dikian says that he discovered a number of email filters had been created to delete and/or obfuscate incoming emails. That is a common tactic to prevent such emails from being visible to the victim of a compromised account, and also would have prevented Dikian from responding to those emails.

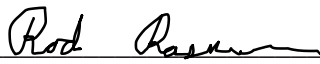
However, on May 8, 2022, Sharjil Saleem (from VPN.com) copied the g.dikian@yahoo.com address on a flurry of correspondence, and Dikian promptly alerted VPN.com to the hack on May 12, 2022:

From: George Dikian <g.dikian@yahoo.com>
Sent: Thu, 12 May 2022 02:10:09 +0000
To: "michael@vpn.com" <michael@vpn.com>
Subject: 89.com fake transaction

Hi,I received your email regarding some 89.com transaction that was never initiated or agreed by meSome of the other email addresses that were cc'd were created by imposters/scammersPlease provide your phone number so we can discuss further Thanks, George

I certify that I am competent to analyze the aforementioned factual information, and that my expertise in cybersecurity informs the above opinions.

Signed, this 26th day of June, 2023.

By: 
Rod Rasmussen
Principal, R2 Cyber