

Expert Report on Evidence Examination

VPN.com LLC v. George Dikian et al, 2:2022cv04453

Performed by Mark Seiden, mis@msbit.com

I was retained by Counsel for [REDACTED] ka George Dikian to examine the record of online activity relating to the fraudulent transfer of [REDACTED] domain names that took place in March 2022. My analysis in this matter has so far taken 24.5 hours at an hourly rate of \$350.

I have investigated numerous account compromises and online frauds over more than the last 20 years. I have been a programmer and software engineer since the 1960s and have taught these subjects at several universities. My cv appears as Appendix A.

The fraud, which required planning and preparation took the form of an advance funding scheme, where a phony buyer contacted VPN, a broker, expressing interest in the domain name 89.com, owned by [REDACTED]. VPN unwisely failed to verify the identity of either the purported buyer, or the purported seller, and did not apparently even speak with them on the telephone. However VPN sent an advance payment in the form of bitcoin to a phony escrow company (intermediar) set up by the fraudsters. The funds were then rapidly disbursed into an assortment of accounts, while the fraudsters played delaying games with VPN, and then deleted both buyer and seller email accounts. The Complaint alleges that the [REDACTED] was involved in the fraud.

OPINION: My findings based on what I have so far examined is that there is no evidence that [REDACTED] was personally involved. To the contrary, there is ample evidence to prove that he was not.

ANALYSIS:

The most important materials that I have reviewed include

- A timeline of events, represented as having been prepared by Rod Rasmussen, whom I have known for approximately 15 years as a colleague on and Chair of the Security and Stability Advisory Committee of ICANN. Rasmussen is a skillful examiner of Internet artifacts and a recognized expert in email fraud.
- Dikian - fact memo (summary of facts prepared by Counsel)
- Yahoo Response to Production Request Feb 6 2023
- Dikian - Yahoo Google Hostgator ISP Analysis
- Google Subpoena Responses (two of them for subscriber information for rhwdomains@gmail.com and account george.dikian@gmail.com)
- Phone Call Request Email – Re 89.com_Domain_Purchase_Inquiry started Mar 7, 2022
- Last Email sent from G.Dikian@Yahoo.com, a continuation of the same thread ending Mar 11, 2022
- Yahoo response to Subpoena 5/5/2023

The General Methodology and Scope of this Examination:

The evidence in this case is primarily a series of emails in text form purporting to be from Defendant, both from his longtime yahoo account (g.dikian@yahoo.com) and from a similarly named separate Gmail account (George.dikian@gmail.com) set up only on 2022-03-17.

The main question is whether Defendant was involved in sending or receiving the emails facilitating the fraud.

I have examined documents provided by Counsel which are the products of discovery from various providers and email contents. I have diligently examined what was provided by Counsel, but this is not the complete evidence in its original context. As a general comment, it is always more difficult to prove a negative, i.e. that someone did *not* do something, than that someone *did* do something. Still, from examined evidence, along with extensive experience of the behavior of malefactors who compromise accounts, conclusions can be drawn in which confidence can be put.

CONCLUSIONS:

1. The g.dikian@yahoo.com account (Dikian's working account) was compromised on or before 1/28/2022 by currently unknown malefactors. (That was the date of the first anomalous login shown in the Yahoo! subpoena response). This could most easily have been accomplished by a targeted phishing attack against the accountholder in which he was tricked into typing his login password into a web site constructed to resemble that of yahoo.com. Another possibility is that targeted malware was used to compromise his laptop or phone, and leak his password to the malefactor.

██████ did not, at the time, use a second factor to protect any of his accounts, so the password alone would have sufficed to impersonate him.

The account compromise is evidenced by a series of logins starting in January from WIFI connection of an Internet provider in Portugal, and separate connections from a VPN provider while ██████ was normally logging in from his usual locations in Florida and/or via his cellphone.

There were also multiple successful attacks on that account's recovery information, which resulted in email addresses being added to the account records that could be used to change password. (See below for more detail).

The long email thread, Subject: 89.com Domain Purchase Inquiry showed a Portugal WIFI login by the fraudster (on Mar 8, 2022, 16:16 Z = 8:16am PST), around the beginning of the first reply (Mar 8, 2022, 7:03 am). There were also logins by ██████ slightly later on that day using ATT. None of the emails sent by fraudsters using the yahoo account appear in received or sent email folders. (They cleaned up after themselves).

2. The g.dikian@yahoo.com account contained sent mail (from 2017) to ██████ web contractor containing the hostgator password, still unchanged in 2022.

Malefactors typically inspect the sent and received email in compromised accounts to find credentials, pending deals, or transactions they can monetize. This is a plausible hypothesis for

the way the intruder gained control over the hostgator account, which shows logins from the same ip addresses as other malefactor activities.

3. The malefactors set up one short-lived account at gmail, George.dikian@gmail.com one long-lived account: rhwdomains@gmail.com, both of which were used substantially or entirely for engineering fraud. George.dikian was set up at 2022-03-17 08:42:27 Z and rhwdomains was set up on 2019-05-24 16:13:50 Z. However, both accounts were deleted within the same 12 minute period, one at 2022-10-13 17:01:35 Z and one at 2022-10-13 16:49:52 Z. This is extremely unlikely to be a coincidence.
4. My belief is that there were two malefactors, since they habitually used different login mechanisms. The IP addresses used to log on to the gmail account were closely related to those used to log on to the compromised yahoo account (same Portugal ISP and same VPN).

The Portugal logins were from MEO Wifi access points in multiple locations in Portugal. (Wifi access is obtained by buying a voucher delivered to a cell phone or by using prior account relationship, so it may be possible to circumstantially identify one malefactor although many foreign corporations do not cooperate with foreign civil discovery.)

The VPN logins are probably untraceable.

██████ states that he was in the US during the entire period and his history of logins from his cable modem at home in Naples, FL supports that claim. He also uses an ATT hotspot, and there are logins which anomalously show "Redmond, WA" as the location on approximately 4 dates in early 2022.

5. It was stated by ██████ that there were filters set up on the yahoo account so mail with certain properties (e.g. from particular parties or containing important words or phrases) would be filtered into folders so the true account owner would not see them. This is a standard practice for malefactors on compromised accounts. (I have not been able to verify that this was done -- Yahoo does not keep logs of filters set up or deleted in account records).

██████ represents that he uses a Windows laptop and (in 2022) a Samsung Note 9 (Android) (switched to a Samsung S23 Ultra in June 2023). He says he does not own any Apple hardware. Based on Google discovery, the user agent strings used to log in on the [George.dikian@gmail](mailto:George.dikian@gmail.com) account were Macintosh; Intel Mac OS X 10_15_7 on two occasions.

6. Based on my interview with ██████, he is not a particularly sophisticated user of computing. He uses his laptop and phone mainly as a communications device, for email and Whatsapp. He has multiple email addresses which forward mail to his Yahoo account. He does not download or use third party apps (not even Microsoft Office). His anti-virus software is the default Microsoft offering bundled with Windows. He was unaware what version of Windows he was running in 2022 or now. He said his machine received Microsoft patches regularly and applies them automatically. He did not use multifactor authentication until the fraud was pointed out to him. He said he has never used a VPN.

- The account rhwdomains@gmail.com is stylistically and operationally interesting. The communications from it to vpn.com are styled in Chinese/English hybrid language, full of typographical errors, and are both confused and confusing, perhaps deliberately. The discovery from Gmail did not contain login history or any ip addresses.

The discovery from yahoo pertaining to the gdikian@yahoo.com account shows several strange account recovery email addresses, including rhwdomains@gmail.com in December 2020, at least one year before the vpn domain fraud. These addresses could be used to take over the account at any point, by forcing a password change. (This would be detectable by the authentic owner because they could no longer log in.)

- Dikian disclaims any connection with these email accounts which were used to compromise his yahoo account:

spdwy@msn.com

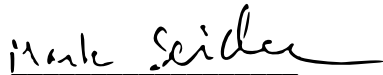
enprat on@gma .com

rhwdoma ns@gma .com

These were added as account recovery emails “by agent”, which suggests that social engineering of the call center was involved. They were all removed the same day when [REDACTED] was informed of the action. That this activity has been going on since 2020 shows that [REDACTED] has been under attack by at least one set of the same fraudsters for years.

Recovery Channel History			
Date	Channel	Action	IP
2023-01-05 21:42:12	+13107099449	ver fy by user	2601:6c0:c201:93c0:a444:1da3:e42e:61a0
2022-07-18 19:15:05	+13107099449	ver fy by user	2603:8001:9303:7000:a164:ce41:e163:b773
2022-04-27 23:44:26	+13107099449	ver fy by user	73.107.137.102
2022-04-27 22:03:00	+13107099449	ver fy by user	73.107.137.102
2022-03-21 10:44:02	+13107099449	ver fy by user	2601:6c0:c202:3430:15c:4bfe:cf43:62a2
2022-03-18 09:38:43	[REDACTED]@ve.com	ver fy by user	2601:6c0:c202:3430:44bf:58dc:222f:75e1
2022-03-18 09:38:20	[REDACTED]@ve.com	add by user	2601:6c0:c202:3430:44bf:58dc:222f:75e1
2022-03-18 09:37:20	[REDACTED]@yahoo.com	remove by user	2601:6c0:c202:3430:44bf:58dc:222f:75e1
2022-03-17 08:33:05	spdwy@msn.com	remove by user	94.140.11.103
2022-03-17 06:18:49	spdwy@msn.com	add by agent	10.195.119.39

Date	Channel	Action	IP
2020-12-16 12:25:34	enp rat on@gma .com	remove by user	2600:387:1:817::b5
2020-12-16 08:23:10	enp rat on@gma .com	add by agent	10.201.242.171
2020-12-11 07:34:31	██████@yahoo.com	remove by user	107.77.217.11
2020-12-11 06:27:08	██████@gma .com	remove by user	2600:387:a:3::18
2020-12-11 06:12:07	rhwdoma ns@gma .com	remove by user	2600:387:a:3::c3
2020-12-11 06:02:04	██████@yahoo.com	add by user	2600:387:a:3::18
2020-12-11 05:33:45	██████@gma .com	add by user	91.132.137.204
2020-12-11 05:32:45	██████@gma .com	remove by user	91.132.137.204
2020-12-11 05:32:45	██████@yahoo.com	add by user	91.132.137.204
2020-12-11 05:17:06	rhwdoma ns@gma .com	add by agent	10.201.242.169
2017-08-08 01:11:18	+13107099449	add by user	2605:e000:6083:f300:a87b:3deb:b2b3:2085
2017-08-07 23:59:02	+13107099449	remove by user	96.47.226.21
2015-06-28 00:00:22	██████@gma .com	add by user	98.139.244.166
2015-05-26 15:43:08	+13107099449	add by user	76.91.7.203



Mark Seiden

3 July 2023