THAT'S YOUR PROOF??

Evaluating Attributions Made in Hunting Cyber Criminals

ABSTRACT

Vinny Troia named individuals as being members of thedarkoverlord, GnosticPlayers, and ShinyHunters. Does he have sufficient evidence to support his attributions?

DataBreaches.net

THAT'S YOUR PROOF??

EVALUATING ATTRIBUTIONS MADE IN HUNTING CYBER CRIMINALS

"Extraordinary claims require extraordinary evidence." — **Carl Sagan**
"Exceptional claims demand exceptional evidence." — **Christopher Hitchens**
"Troia makes extreme claims with unsatisfactory evidence." -- **"Dissent Doe"**

INTRODUCTION

When *Hunting Cyber Criminals* was published by Wiley several months ago, its author, Vinny Troia, promised to release a technical report with proof supporting attributions he had made – attributions that named several people as criminals. According to Troia, he had managed to identify the core members of not just one, but **three**, threat actor groups: thedarkoverlord ("TDO"), GnosticPlayers, and ShinyHunters. And as if that wasn't enough to grab headline news, he also claimed that the same individuals were involved in all three groups and that two of the threat actors account for more than 40% of all non-credit card breaches between 2017 until now.[1]

Troia released the promised technical report this past week. But does it contain sufficient proof or even build a strong enough circumstantial case to support accusing named people of being criminals? In my opinion: no.

Attribution is difficult and should involve multiple types and sources of information. Troia tries to find connections between different threat actors and clearly spent time going back through defunct forums to try to determine who knew whom and who may have worked together or with TDO in the past. That is all to his credit. But he relies heavily on chat logs and forum posts by people who obviously may not be telling the truth. The report also contains some interesting IP address data for GnosticPlayers and ShinyHunters, but he does not appear to have clear evidence of any individual actually being a hacker for TDO other than some early posts by "Arnie" or later forum posts by TDO as a group claiming responsibility for hacks. If you are going to claim that a threat actor is the "lead hacker" for TDO, then there should be something that shows he committed at least one hack that has been linked to them. Troia does not seem to meet even that low bar, unless you agree with him that he has successfully linked one Canadian man to the threat actor who used the NSA@rows.io Jabber ID. But even then, he seems unable to prove NSA actually hacked anything for TDO. And he has even less evidence linking that person to GnosticPlayers or ShinyHunters.

[1] DataBreaches.net is not linking to any of Troia's publications precisely because he does accuse named individuals of criminal conduct. Nor will any of those he accuses be named in this report.

While I always enjoy a good conspiracy story, and love having things tied up neatly with bows, Troia's report leaves me thinking that although I know what Troia believes, I have not seen enough evidence to agree that his beliefs are justified.

Because I found so much of his presentation and analyses problematic, I will not go through his report section by section or point by point. Instead, I have selected just some of my concerns or disagreement with his attributions.[2] Quoted material in this paper is drawn from his book, a recent keynote presentation, and his technical report.

I will start by noting claims where I think Troia *has* provided reasonable evidence to support at least part of his claims:

1. Troia identifies a young man in Canada as someone who had been arrested for computer-related crimes. Troia claims that when the police seized the youth's devices, they found indications that this teenager might be "Ping." Someone in Canadian law enforcement with knowledge of the case who was not authorized to speak publicly did confirm for me the arrest, the reported link to "Ping," and the real identity of the youth. But of course, even establishing that this teen was likely "Ping" is a far cry from establishing that he was part of TDO, or GnosticPlayers, or ShinyHunters – or all three. We have to look at other evidence Troia presents for that to see if he builds a solid case or a weaker circumstantial case.
2. Troia claims that "Cr00k" was a seller of TDO databases and used at least two jabber accounts on Jabber and as contact links in posts on forums. I agree with that attribution I also agree with Troia's claim that F3ttywap is an alias of Cr00k. Somewhat confusingly, though, in another part of his report, Troia suggests that Cr00k and F3ttywap are different people: "These posts reveal Arnie, Cr00k, and F3ttywap as the initial set of TDO threat actors." He likely had it right the first time when he said that it was the same person using different aliases.
3. Troia correctly notes that there was some change in 2017 in TDO in the sense that the original spokesperson was no longer the spokesperson and TDO's tone and communications became more aggressive. Several journalists had noted the change, too, and it is certainly the case that whoever was handling communications did not appear to know things that the previous TDO would have known. They even admitted as much to me on several occasions.
4. Troia correctly identifies Nathan Wyatt of the U.K. as being associated with thedarkoverlord. That is undisputed. But pretty much almost everything else Troia claims about Wyatt has been disputed by DataBreaches.net, as detailed later in this article.[3]

[2] Because of arrests made in the case of GnosticPlayers hacks, attributions involving those threat actors have more actual support. When it comes to TDO, however, there has been only one arrest revealed to date, and that individual was not charged with hacking.

[3] Of concern, Troia continues to repeat claims he has been advised are incorrect without even mentioning that there is evidence to refute his claims, suggesting that he locked into one theory and failed to remain objective or share relevant data with readers in his report.

The remainder of this article describes some of my concerns about Troia's methods and report, with specific examples drawn from his writings and work.

Concern: Weasel Words

Troia often makes claims such as, "It is believed" or "Evidence suggests" without providing any sense of who believes something or what evidence he is referring to as suggestive. Consider the section of his book on "Arnie," a section that Troia accompanies with a picture of Nathan Wyatt declaring Wyatt "Arnie." Troia writes:

> *Evidence suggests that Arnie is Nathan Wyatt (aka CraftyCockney), a 30 year old resident of the United Kingdom*

Given that statement, I would expect to see some evidence that Wyatt (who is 39) is "Arnie." But at no time in any chat or communications seen by this site did Wyatt ever suggest or claim that he was "Arnie," and his writing is distinctly different from the first TDO's writing.[4]

Wyatt was extradited here for his role in early TDO attacks in Georgia and Missouri. His guilty plea and sentencing are scheduled for September, 2020. Of note here, the federal case does not accuse Wyatt of being Arnie. In fact, Wyatt is not accused of hacking anything in the U.S. "Arnie," however, had claimed to hack the medical clinics. If Wyatt was "Arnie," and if there was evidence that Wyatt was "Arnie," prosecutors would probably have charged him with hacking.

From Troia's technical report:

> *…. Wyatt was one of the original personas behind the Dark Overlord, and also acted as the group's original lead figure under the alias Arnie*

Wyatt was undoubtedly involved with TDO in 2016, by his own admission to this site, and by the fact that he is pleading guilty to charges involving TDO hacks in Missouri and Georgia. But it is highly unlikely Wyatt was the main TDO jabber channel communicator for journalists in 2016. That person, who I refer to as TDO-1, wrote in decent English while faking broken English as a drunken Russian. Wyatt reportedly quit school at age 15, and it is doubtful he would have included the literary references TDO included in their tweets and posts. Wyatt might have registered TDO's Twitter account, but his writing does not seem consistent with the individual who tweeted for TDO. THAT individual seemed to be the same person running the Jabber channel for journalists.

Furthermore, if, as Troia maintained, "Arnie" was TDO-1 and handled press communications and their Twitter account, then Wyatt *could not have been* Arnie. I had lengthy chats with TDO-1 *while Wyatt was in police custody and could not have been online or on Jabber at all.*[5]

[4] DataBreaches.net had extensive Jabber chats with both the first TDO spokesperson and Wyatt. Their writing and style was significantly different.

[5] I had informed Troia of this in the past, so his continued claims that Wyatt was both "Arnie" and TDO's spokesperson in September 2016 are puzzling, at best.

Troia also tries to paint Wyatt as a patsy for TDO. Troia seems to think he has identified a common pattern that these threat actors use – they hang everything on a patsy who is presented as the public-facing head of the group. Troia claims that they did the same thing with GnosticPlayers. But apart from evaluating the claim about GnosticPlayers, is there any actual evidence that Wyatt was ever TDO's patsy?

In his book, Troia writes:

> *The indictment states that Wyatt willingly used bank accounts in his and his girlfriend's name, which were to be used to cash out money earned from the group's extortion schemes. This is the one charge that I personally find a bit hard to believe. According to the indictment, the account numbers were used in a TDO extortion email. Given the MO of the other group members, it is very possible they were able to find his account numbers and intentionally include them in an email to a victim.*

In his technical report, he writes:

> *It is our opinion that, NW was ultimately setup to take the fall for the group's crimes. This theory is supported by the fact that Wyatt allegidly opened bank accounts in both his and his girlfriend's name which were used to withdraw funds from TDO extortions.* [18]

I agree with Troia that it is difficult to believe that an experienced fraudster like Wyatt could be so sloppy or careless as to open bank accounts in his own name and his fiancée's name. But consider the following:

- Wyatt used his well-known nicks and accounts when trying to sell hacked Pippa Middleton photos to the media. Given that he was trying to sell stolen material belonging to a member of the royal family, wouldn't you think he would use heightened opsec and would try to mask his identity? He did not. As he told me in that interview, he wanted to use the opportunity to promote himself. Wyatt is apparently not totally averse to being easily associated with criminal activity if it helps build his reputation "in the community."
- Also: if Troia thinks TDO set up Wyatt as a patsy, did Troia try contacting the banks in the UK about their security and requirements to open those accounts? I had contacted them and was assured that the banks had verified who was opening the accounts, although for security reasons, they would not give me a detailed answer about their verification controls. I would expect that because the U.S. federal complaint included those bank accounts as evidence against Wyatt, that law enforcement would have checked to make sure that the banks could document how they verified Wyatt had opened the account and not an impostor.

Sometimes, a cigar is just a cigar. Of course, it is possible that Troia is right in his attributions and claims about Wyatt and that I am wrong. But it is his failure to include all the evidence about Wyatt or at least acknowledge that there is evidence refuting his beliefs that should makes you wonder whether he is ignoring or withholding information that might change your mind as you read his report.

CONCERN: SUBSTITUTING NICKS/ALTS

Troia often attributes chats or actions to *aliases he believes are alts for the threat actor* instead of reporting the nicks that were used in the chat or situation. By substituting usernames/nicks, Troia may be biasing the reader to see a behavior as being demonstrably linked to one threat actor when it had been said by another persona who may or may not be the same individual.

Consider the following material from his book. On one page, Troia provides the following excerpt from a chat that describes as being with "NSA" (the one he calls NSA@rows.io). He tells the reader the speaker is NSA, and then uses XXX to indicate him:

> XXX I'm sorry man but you sound like you're either LE or a f***ing
> retard, probably the latter.
> VT why am i a retard?
> XXX you and your friends NightCat/jasonvoorhees/hafez asad and other
> d**kheads can go climb a wall of d**ks
> VT NightCat? Jasonvoorhees?
> XXX s u c k a d * * k

Later in the book, he cites the exact same chat but now identifies the speaker as "WhitePacket:"

> VT: so how do you know Bev?
> whitepacket: sorry not interested in discussing that
> whitepacket: are you in the law enforcement industry?
> VT: there's no money in being in LE
> whitepacket: I'm sorry man but you sound like you're either LE or
> a f***ing retard, probably the latter.
> VT: why am i a retard?
> whitepacket: you and your friends NightCat/jasonvoorhees/hafez asad
> and other d**kheads can go climb a wall of d**ks
> VT: NightCat?
> VT: jasonvoorhees?
> whitepacket: s u c k a d * * k

Troia may believe that "NSA" = "WhitePacket," but he biases the reader in the first instance by referring to the chat as being by "NSA." In addition to occasionally substituting nicks, he also occasionally omits nicks that should be included and/or edits logs to delete or redact information. In some cases, he offers no context and no explanation for why he is redacting material from a log. As a result, a reader may have no context to evaluate a chat log. Was the speaker communicating with a friend or fellow threat actor? Did they think they were talking to Troia? Did they think they were talking to a buyer? Troia omits important information at times.

CONCERN: BELIEVING THOSE MOTIVATED TO LIE

Troia seems to rely on statements by cybercriminals in making his claims, while realizing that criminals lie. So why does he seem to just blithely accept some of their claims as true? If Threat Actor #1 decides Troia is getting too close, he may throw Threat Actor #2 under the bus to disinform and misdirect Troia.

Troia realizes that type of thing does happen and that some threat actors are highly accomplished liars. Yet Troia may use what Threat Actor #1 says in the book or report it as supposed evidence of something. Why?

Indeed, one of the biggest concerns I have with Troia's analyses and attributions is that he appears to believe people who routinely lie as part of their opsec and much of his "evidence" relies on chats. Consider this bit from his report:

> *In the following private conversation, user Photon is revealed as also being NSFW, Ryder and Prometheus*
>
> *XX: NSFW == prometheus == ryder == photon*
> *XX: I don't understand why are you so confused it's so simple prometheus == script kiddy*
> *ME: NSFW is prometheus?*
> *XX: yes NSFW and prometheus are the same person*

Troia does not clearly indicate who the speaker is in the chat. Could they be lying to Troia? Of course. So why does he present this as being an accurate or truthful revelation about "Photon?" Why doesn't he tell the reader who made that claim? And does he know that at other times, Prometheus has been identified by others who do not claim that Prometheus was Ryder or Photon or NSFW? Was Troia so intent on trying to link Prometheus to NSFW that he just believed the claim? Believing claims that support your theory is understandable, but often a huge mistake.

THE ELEPHANT IN THE ROOM: DOES TROIA HAVE COMMERCIAL RELATIONSHIPS WITH THESE THREAT ACTORS?

Over the past few years, a number of people have questioned whether Troia has engaged in unethical or illegal conduct. After Verifications.io was recently leaked, more people have come forward and have accused him of buying, selling, and trading hacked data, leaking hacked databases that had not previously been public, encouraging others to hack or acquire stolen data for him, harassing or attempting to extort them to give him databases or information, and lying about how DataViper.io was hacked. Those are obviously serious accusations, and to be clear, because I have not investigated any of the claims, I certainly do not mention them for any truth value. I mention the accusations because they are the elephant in the room when it comes to evaluating Troia's credibility. **If** Troia has had any commercial interactions or information-sharing relationships with the threat actors he is reporting on (and at least a few of them have claimed that he has had such interactions), I believe that it is his ethical obligation to disclose those relationships and transactions.

CONCLUSION

Most of Troia's most important claims or attributions do not seem adequately supported to me, but I don't know what standards the field has for naming someone. If you are a professional in the field, I'd like to hear your thoughts on whether his report provides adequate support for his attributions. You can email me at breaches[at]protonmail.ch.