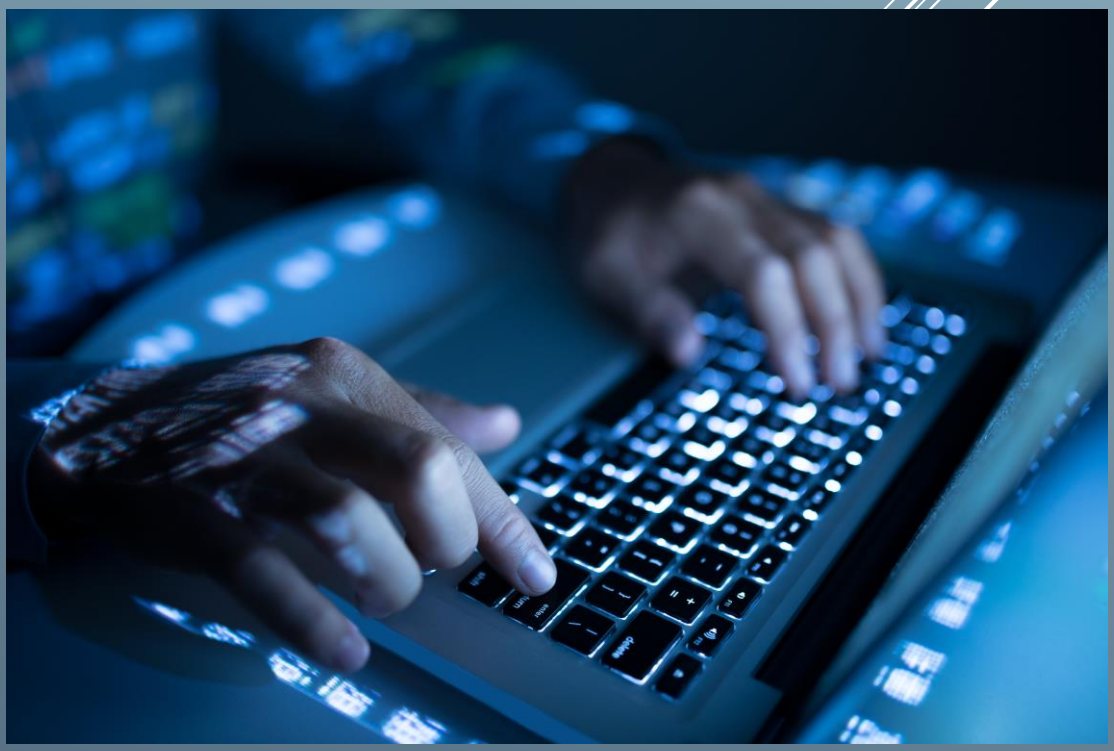

THE DARK WEB: 5 THINGS TO KNOW

How to Search for Your Organization's Data

An Interview Transcript from Terbium Labs' Danny Rogers and Information Security Media Group's Tom Field

The Dark Web:

5 Things to Know

Terbium CEO Danny Rogers on How to Search for Your Organization's Data: Interviewed by Information Security Media's Tom Field, VP of Editorial

What's required to access the Dark Web? And how does one separate fact from fiction? These are two of the five things Dark Web users need to know, says Danny Rogers, cofounder and CEO of Terbium Labs.

"Through our original research, we've found that actually half the content floating around on [the Dark Web] is perfectly legal and benign," Rogers says. "It's the other half you really have to worry about - a lot of it is illegal drugs; a lot of it is stolen credit cards, other stolen data, and those are the parts that one specifically has to worry about."

In this interview transcript about how to use the Dark Web, Rogers discusses:

- Common misconceptions about the Dark Web;
- The five things everyone needs to know;
- How Terbium Labs helps customers search data on the Dark Web.

Rogers is the co-founder and CEO of Terbium Labs, an information security and data intelligence startup based in Baltimore, Maryland. He is a computational physicist with experience supporting defense and intelligence community cyber operations, as well as startup experience in the defense, energy, and biotechnology sectors. He is an author and expert in the field of quantum cryptography and has published numerous patents and papers on that and other subjects. Prior to co-founding Terbium Labs, he managed a portfolio of physics and sensor research projects at the Johns Hopkins University Applied Physics Laboratory.

Interview Transcript

Field: Hi, I'm Tom Field, Vice President of Editorial with Information Security Media Group. I'm talking today about searching the dark web for your data: the five things that you need to know. It's my pleasure to be speaking with Danny Rogers. He's the co-founder and CEO with Terbium Labs. Danny, thanks so much for joining me today.

Rogers: Thanks so much, Tom, for having me.

Field: Danny, I know you've given the dark web a lot of time and energy. What do you find to be some of the popular misconceptions of the dark web and what really happens on it?

Rogers: That's really a great question because the term dark web is so loosely defined. We, through our original research, found that actually over half of the content floating around on these anonymous, hidden services and other places on the internet is actually perfectly legal and benign. It's sort of the other half that you really have to worry about, and that other half is split. A lot of it is illegal drugs. A lot of it is stolen credit cards, other stolen data, and I think those are the parts that typically one needs to worry about.

We haven't seen a lot of terrorism out there. I think a lot of that is overblown. I think a lot of the more well-publicized scams around things like assassination services and weapons, a lot of that is mostly mythology. The truth is, like I said, it's a lot of drugs, but also a lot of fraud and stolen data, too. Those are the parts – especially the fraud and stolen data – where we tend to focus.

Field: Well, let's go through the five things that you need to know about the dark web, and let's start with this: What's required to access the dark web?

Rogers: That's a great question. So, for starters, it's a little bit hard to define what the dark web is. It's pretty loosely defined, like I said, if you're talking about

accessing Tor hidden services, for example. For starters, the Tor network is an anonymous proxy overlay network, and it requires special software from the Tor project to even access. There's a special web browser and other software underneath that that connects you into this proxy network. Once you're there, you're able to access, for example, what are called hidden services, which are websites that are anonymously hosted within this Tor network. The URL is often in .onion. There are other proxy overlay networks, such as I2P and Freenet, things like that. But, the overwhelming mass of content and data are on Tor, so you need special software to start.

Now, that said, there are sites on the clear web, whether it's carding forums or stolen information marketplaces or even paste sites that don't technically require Tor to access, but then you can get into some sort of dangerous territory where you're potentially accessing sites and giving away who you are to the folks that operate these sites, and you may not want them to know that you are looking. That's where these anonymization technologies come in. From a technical perspective, at the very least, one of these anonymization services like Tor is the minimum requirement to even be able to view this part of the internet.

Field: You talked a few minutes ago about mythology about the dark web, how do you separate fact from fiction?

Rogers: You know, it's difficult unless you have access to the actual specific data you are searching for. It’s like that famous New Yorker cartoon on the internet: “Nobody knows you're a dog.” It's kind of important to remember that a lot of the people out there claiming to have breached certain organizations, claiming to be capable of certain things, a lot of them are scammers. Sometimes it's trying to pump themselves up to look more elite than they are. Sometimes it's perpetrating scams to steal bit coin from other people on the dark web. The way we do it is really by ... we're talking to our search technologies to specific data on behalf of our clients, through our data fingerprinting techniques. Verifying a data breach, whether it's through some automated technique like we use, or manually the way some security researchers do, it's really important to be able to tell what's a scam and what's real.

There's been a number of notable examples over the past couple of years of publicized data breaches that turned out to be false, or pieced together from historical events, or claims that were made that were just flat out not true. It is a challenge, and it's something that – whether you do it by hand or build in automated systems as we do – it's definitely something that's sort of a "must have" to be able to tell the difference between what's fake and what's real.

Field: The third thing individuals need to know: What are the legal considerations they need to weigh?

Rogers: That's a really important issue. There's a lot of content out there that is illegal to even just access, certain kind of illegal pornography and child abuse imagery that is prevalent out there that is really kind of important to combat, but illegal as a private citizen to even just access. Having a procedure in place to filter it out and avoid it and to report it when you do find it is critical, and we have obviously all of that in place.

Then, just storing and accessing other kinds of stolen information – technically, it's always important to remember that when you're looking at this data breach stuff, you're touching stolen property. How do you provide this search capability, or how do you search this part of the internet without accidentally trafficking in stolen goods, whether that's through bit torrents, or just in the process of indexing these parts of the internet? It is really important because I think more and more there's going to be attention paid and enforcement activity around accidentally both proliferating this material and incentivizing the people who are doing the stealing to put it out there.

Field: Danny, the fourth item. We talked about the legal considerations, what about technical and even trade craft considerations?

Rogers: Yeah, that's also incredibly important. A lot of these forums are run by hostile actors… Let's say you download a guide or a pdf, or something like that, it's very likely and possible that that document or that file can be infected with some kind of malware. Thinking about how you handle materials that you pull from that part of the internet is very, very important.

Thinking about the browser configurations, whether it's enabling Java script or not, things like that, that open up attack surface to these hostile pages. There's no honor among thieves, and the people that operate these pages are just as much out to steal from the people who are visiting them as they are to other third parties. It's super important to have a technical setup that protects you. The Tor browser does, in some ways, try to help, although there's a lot of room for improvement there. I think the community will agree.

Just from a technical perspective, like I said, protecting yourself from potentially hostile site operators is one thing. The other big thing is trade craft considerations. Folks very widely say that encryption and anonymity technologies will only go so far as your trade craft, or lack thereof. It's much more important to have good trade craft in whatever technology you can handle, than the best technology and poor trade craft. You can anonymize yourself using Tor and then accidentally type your real email address or name into a form, and suddenly all of that anonymization doesn't really help.

There's a lot of art and knowledge and expertise in not accidentally leaking your identity or anything sensitive about yourself. I know of organizations out there that when they claim to "search the dark web," they're actually going and entering your sensitive data into the dark web search engine – search engines on the market places – and thus inadvertently revealing those sensitive queries to the market place operators, which is a really, really big risk, and a really big no-no. I think that there is always a lot of attention that needs to be paid to how you interact with these parts of the internet so as to not give yourself away – as to not put your own data or your own organization at risk.

Field: Danny, last point. The dark web is constantly changing. Why is this a key bit of information for users to know?

Rogers: Yeah, it *really is* constantly changing. The sites go up and down as researchers or law enforcement pay more or less attention to them. They move around to different URLs, often in rotation or randomly, in response to the hostile environment in which they operate. Sites merge and split regularly. Different

groups show up and start their own marketplaces. Other groups exit scam and close down marketplaces, so these things change pretty dynamically, and it's really a challenge to try to keep up with them by hand.

This is why we're so focused at Terbium on automation, just because keeping up with that frontier: where are the latest forums? Where are people posting the latest information? Where are they putting up your W2 information for sale?

All these sites come and go so quickly that you really need an automated system to at least stay ahead of that and discover the new ones. Often you can still have human follow up behind and fill in the gaps, but it's just so dynamic and so word-of-mouth that unless yours are really in the community, you're never going to be able to keep up. Even if you are, you can never really keep up with all the different communities, whether that's the carding forums, the identity theft marketplaces, the drug marketplaces, and all of these places that are their own specific sub-communities. There's no way by hand to keep up. If you try, it's just going to scale to where it becomes prohibitively expensive. That's why we think automation is one of the absolute keys to be able to do this effectively.

Field: Well, Danny, to wrap up our conversation, tell me a little bit about Terbium Labs. What are you doing to help your customers monitor and use the dark web appropriately?

Rogers: Absolutely, and thanks for asking. We really focus on fully private, fully automated dark web data intelligence. What that means is that we use our automated systems to keep up with this part of the internet and to stay ahead of it. Our machines read the internet faster than any human could. We use that advantage to stay ahead of this dynamic environment. At the same time, we use this privacy protected data fingerprinting to monitor this part of the internet for our customers' sensitive information, and we do so in a way that doesn't require them to reveal that information to us but can still tie it back to that original data.

Tying it back to the point earlier about how do you tell what's real and what's fake, we tie our matching directly to the customer information itself, whether that's employee personal information, or customer data, or specific identifiers, we know the data is real because the fingerprints match. We don't have to do nearly as much manual evaluation or vetting of is this real or fake. In fact, we don't even have to rely on things being labeled. If there's just sort of a big dump of PII on our unsecured pay site, if those fingerprints overlap and match what we have on file for our customers, they're automatically alerted when that shows up. Really focusing on bringing that breach discovery time down from months that it is now, down into the minutes. In some cases, we're able to alert our customers that their data has popped up somewhere it shouldn't have within a matter of minutes of it appearing.

That's really kind of an overview of what we do, and we try to do that in a way that is much more affordable than others in this space. Again, coming down to this automation; we're not trying to scale up human beings trying to keep ahead of this frontier, and we can do it at a much more affordable price point. Really, that's what it comes down to, full privacy, full automation, the action ability of tying it to the real data, and the affordability of our offering.

Field: Very good, Danny. I appreciate your time and insight today. Thank you.

Rogers: Absolutely. Thanks so much for having me. Good luck out there on the dark web.

Field: The topic has been searching the dark web for your data: five things you need to know. I've been speaking with Danny Rogers, co-founder and CEO of Terbium Labs. For Information Security Media Group, I'm Tom Field. Thank you very much.