NEWS

Q&A: Digging into darknet technology with Farsight's Andrew Lewman

by
Peter Loshin
Site Editor

Published: 17 Feb 2017

At RSAC, former Tor Project CEO Andrew Lewman explains the latest research into darknet technology and how that tech continues to evolve as an attack vector.

CONFERENCE COVERAGE:
RSA 2017: Special conference coverage »

+ Show More

SAN FRANCISCO -- While the Tor anonymity network may be the best-known darknet technology, it's not the only one. And while these darknet technologies are often portrayed as being impenetrable tools for heinous crimes, they aren't always evil -- and they aren't always impenetrable.

Andrew Lewman knows a lot about darknet technology. Before joining Farsight Security as chief revenue office, he was executive director and CEO at the Tor Project, and he continues to dig into the ways -- both good and bad -- anonymity tools are used.

Lewman, who presented a session at RSA Conference 2017, titled "Tracking Darknet: A Window into Attackers' Motives, Methods and Targets," sat down with SearchSecurity afterward to talk about how darknets can be used for and against enterprises, as well as what the future may hold for darknet technology.

Why should enterprises care about darknets? Are there benefits for enterprises from using them?

Andrew Lewman: Let's take the positive use first. Darknet technologies can be used to help investigations, to help have your team go and investigate something -- or someone -- without clearly screaming, 'You're from company.com.'

The negative uses are vast. The studies I reference talk about botnets using command and control over darknets. By design, most of these darknets bypass most corporate firewalls and [intrusion detection systems] and all the security apparatus you have in place. Someone goes and downloads it, comes in with a USB drive, pops the software on their computer, and now they have a two-way connection to the darknet that, likely, your corporate security apparatus just sees as encryption.

Unless you're actually doing deep packet inspection of every crypto packet to figure out, 'Does this look like SSL?' -- which could be legitimate -- or, 'Does this look like something else?' you're not going to see it, and you're not going to know. There are endpoint solutions that will scan if you're running executables, corporate desktop management apps that will say the following things are allowed to run or not allowed to run, and these are some basic ways to protect against darknets on your network.

However, what came to light a couple of weeks ago were a couple of forums were basically paying people inside organizations to leak data to their forum -- a sort of insider trading. And then, the people who are paying this are saying, 'I have access to 10, to 50, to 100,000 Twitter accounts or Instagram accounts,' and they can start doing sentiment analysis to tank your company's stock, or short it or trade against it. You just need to find one disgruntled employee, or one that just wants more money, and ... there you go.

It's the same situation you've had forever -- just now, they can do it completely and totally privately, through a darknet.

How did researchers learn about botnets using darknets?

Lewman: There were studies over the past couple of years where researchers had basically recorded hidden service traffic. And what they did was look for what addresses were being requested, and how often they were being requested and how long were these sites up. And what they found was, during the sample period, they found that botnets were by far the largest -- both in requests and popularity of what are the parts that were open [and used for botnet communication]. Port 55080 is associated with the Skynet botnet, and they found the most number of services were tied to a botnet, and the most requests were tied to a botnet.

Most of the hidden services with open ports were listening to the Skynet port. Does that mean they were all being used to control botnets?

Lewman: The belief was that it was command and control, so how does the botmaster control the millions of infected computers? They have to talk to them somehow. Traditionally, that has been done over IRC [Internet Relay Chat], or they've switched to Twitter, they've switched to Facebook, just to send out a command saying, 'Do this now,' [or] 'Do that now,' [or] 'Do this now.'

And that was one of the examples in there, with the cloud computing dashboard, one of the commands you could send was 'mine bitcoins.' So, you have access to 10 million computers, say, and what a great way to build your own mining farm to mine bitcoins and get free bitcoins.

Are a lot of these compromised systems communicating over the darknets?

Lewman: Whoever ran the botnet, the first thing they did was to install a minimal Tor client, which then would connect back to command and control, so they could control it and whatever else they did through it -- send email, fake webpages, steal credit card data, exfiltrate data, whatever. Just that Tor app, and you need a command-and-control point for that botnet.

You mentioned that some ports were opened for SSH. How were those used?

Lewman: A hidden service is just an address; whatever you put behind it is up to you. So, you get a .onion domain, and then you start looking at what ports are available. Some of them may be legitimate -- for example, if there's a corporate firewall in the way and you want to have SSH access to their machines. Because SSH is just Secure Shell, it lets you have an authenticated and encrypted conversation with a machine you control, hopefully, so that you can connect in remotely and do what you need to do, and then disconnect. Maybe you're a firewall administrator, and the firewall would not let you open the port while you're traveling, so you can go to this .onion and that's how it works.

There was no research into what was behind that. Like, was this legitimate or illegitimate, or was this some new kind of botnet thing where it uses SSH keys to hide the fact that it's command and control of a botnet? So, 'hide in the crowd' with a legitimate protocol. With Skynet, it's obvious, because it's port 55080 and it's screaming out, 'Hey, I'm a botnet!' So, you hide it inside SSH.

SARAH CORTES

Andrew Lewman at RSAC 2017

What's the next thing that's going to make us all crazy?

Lewman: All the darknets are too difficult to use. You still have to download something, you still have to go find the addresses, [and] you still have to figure out where they are. Think of movie piracy: You have to go download some BitTorrent thing, and then go find some movies and figure out how to piece it back together, and then you've got this giant movie file that you need to figure out how to play.

What was a huge leap for that was an app called Popcorn Time, which has since been taken down. But Popcorn Time was just like a Netflix interface, except it was all pirated movies and TV shows and music. You just point and clicked, and, magically, it started playing. You didn't have to work any of that stuff. And at some point, somebody will come up with a darknet that is that easy. And the real challenge is not so much the darknet itself -- you need to make it point-and-click easy.

I think that's what's next. Someone will come up with a way to host content -- whatever that is -- tie it to a darknet, and that will become the killer app.

Do you see anything like that being developed now?

Lewman: I2P has a lot of those technologies built into them; ZeroNet does, as well; and Tribler is another one that's sort of the same way. The idea is that you install it, and then you can start watching videos right away. It doesn't work quite that well in practice, but the potential is there.

As for your question, what's going to drive us crazy is that most corporate firewalls and firewall technologies are still on the level of, 'Is this IP [address] good or bad?' And they need to move up the stack and start to ask, 'Is this protocol good or bad?' Or, 'Is this traffic good or bad?' A lot of them are still based on IP addresses, [asking] 'What's the history of this IP address?' Or, 'What's the reputation?'

Peter I

What have your encounters with darknet technology in the enterprise been like?

Join the Discussion

Next Steps

Find out more about how attackers subvert SSH for use in botnets

Learn about how investors use sentiment analysis on social media

Read about why ad fraud botnets are so difficult to stop

Conference Coverage

RSA 2017: Special conference coverage

COVERAGE SECTIONS

1. **Cyberattacks and adversaries**
2. Emerging technologies
3. Government security
4. Video and podcasts
5. Chatter

Join the conversation

1 comment

Share your comment

Send me notifications when other members comment.

Add My Comment

Oldest ▾

[-] Peter Loshin

- 17 Feb 2017 12:56 PM

What have your encounters with darknet technology in the enterprise been like?

Reply

SearchCloudSecurity

How to make a cloud risk assessment easier with frameworks, standards

A cloud risk assessment can often fall by the wayside in an enterprise, but using a standard or framework can simplify it. Expert...

Tenable launches cloud-based vulnerability management platform

At RSA Conference 2017, Tenable Network Security introduced a cloud-based vulnerability management platform called Tenable.io ...