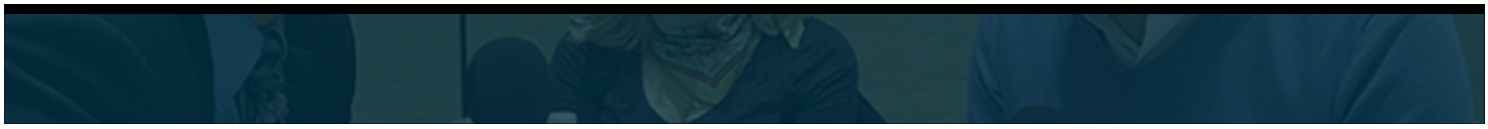


March 23, 2017

The ghost in the machine: Darknet evolves as portal into hacker's targets

Organizations would be wise to monitor hidden network's forums to shield themselves from attack

PODCAST BY BYRON ACOHIDO, THIRDCERTAINTY

00:00 00:00

Download Podcast

~~Office of Personnel Management. The Democratic National Committee. The one~~ thing all successful network hacks have in common is the Darknet.

The Darknet is a vast part of the internet where most ordinary citizens will never tread. Google, Bing and GoDuckGo do not keep track of anything in the Darknet. Its web locations can only be reached if you're versed in using nonstandard communications protocols.

With this in mind, I attended a talk by Andrew Lewman, chief revenue officer of Farsight Security at the RSA 2017 in San Francisco. The title of his talk: "Tracking Darknet: A Window into Attackers' Motives, Methods and Targets." A few eye-opening takeaways:

• **The commons.** The Darknet is where the cyber underground convenes. Network breaches now cause a phenomenal $600 billion in damages annually, a level of crime intensifying at a rate that will drive corporate losses to $2.5 trillion by 2020, according to British consultancy Juniper Research. The Darknet functions as the commons where all of the intricate horse trading underlying the complex, amazingly efficient cyber crime economy takes place.

• **It takes a village.** Want to hack a high visibility target? Head to the Darknet forums. It won't take you long to find parties knowledgeable about the systems your target uses, and, more importantly, the unpatched vulnerabilities therein waiting to be exploited. You can then shop for malware that will get you inside, and help you stealthily copy and exfiltrate entire databases. Now you need to market what you stole. One tried and true way is to post a sample of the stolen data on a Darknet location monitored by hacktivists and reporters. Voila, your breach hits the headlines. Expect purchase queries to follow via the forums.

pay the mortgage or buy a Maserati with Bitcoin. What's more, U.S. and European anti-laundering laws can snare you at legitimate exchanges. Luckily, on the Darknet faked passports are readily available, Bitcoins accepted for payment. It's simple to set up an alter ego, with a passport of good enough quality to be used as accepted ID at online currency exchanges. What color would you like your Maserati?

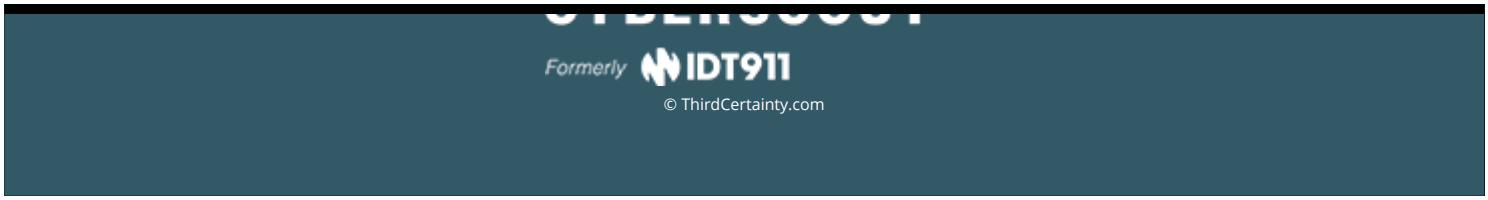
Another fascinating theme Lewman spoke about was why organizations should consider assigning someone to gain a working knowledge of the Darknet. Self-education is straight forward with lots of tutorial material available online.

Why would a company do this? The same reason law enforcement does it: to understand and monitor deal making and the movement of stolen data and criminal payoffs. From a company's standpoint, it's possible to monitor Darknet forums to see if your company's name appears in a way that should send up a red flag. And if your company gets breached or sustains a ransomware hit, following the bread crumb trail of the attacks can be acutely valuable.

More related stories:

Norse discovers stunning Dark Net attack patterns

How to operate in a world without any secrets


Formerly IDT911
© ThirdCertainty.com