SIXGILL REPORT

How Sixgill Solutions Help Minimize Your Cyber Risk

By David Strom

SIXGILL

July 2020

Every minute of every day, hackers are trying their best to penetrate our business networks. While this is nothing new, the depths of their determination is. Not satisfied with the open or public web to learn about your computing infrastructure, hackers have moved to use more hidden parts of the Internet called the dark or deep web.

Hackers use the dark web to share tips and techniques and ways to compromise your data without your knowledge. Once upon a time, the dark web was a den of porn, illegal drugs, and other questionable content. It has since evolved into a well-developed marketplace where exploit kits and credit card details are traded anonymously. Nowadays you can also find discussions of the obfuscation aspects of malware tools and the best methods to penetrate networks without giving away much evidence of the penetration.

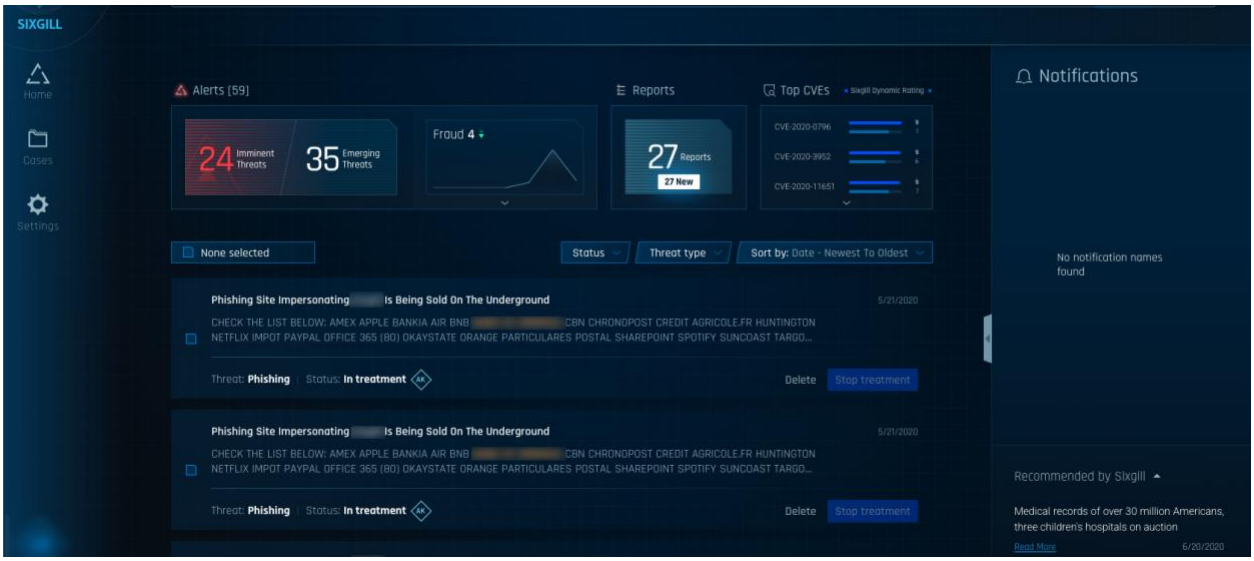
The dark web is also used to test out new penetration methods and discuss potential targets of opportunity before they are deployed on the public web. As an example, see this post on Brian Krebs' site about the city of Florence Alabama. Through dark web analysis, he tried to alert the city's IT manager about an impending ransomware threat last month. Despite repeated attempts, his warnings weren't heeded and the city was hit in early June with a ransomware request that shut down their email network and threatened to publish private data online.

Hackers use two basic tactics to try to get around your existing security infrastructure. First, **they limit the number of total packets in their intrusion**, hoping to avoid calling attention to themselves by lying dormant for weeks or months before doing any active damage. When Google rolled out its Chronicle security product several years ago, it found all sorts of network penetrations of its early customers that dated from several years back. It found just a few telltale packets in amongst the terabytes of historical data.

A second tactic is to **bury your intrusion detection equipment in a large number of fake alerts**, hiding the "real" intrusion deep inside this collection. The hackers are counting on overwhelming your security analysts with this pile of alerts that will make finding the actual threat more difficult. They are also counting on your analysts leaving tracks across the public web revealing important "tells" about your defensive equipment and tactics that they can use to avoid further detection.

A new way to level the playing field

There is only one way to make a more level playing field for defenders, and that is to **combine security automation backed with a large collection of deep and dark web content**. That is what Sixgill's Investigation Portal does, by providing threat intelligence teams with fully automated life cycle tools and actionable alerts along with the ability to conduct real-time cybersecurity investigations. It has near real-time access to threat data and these sources are enriched by machine learning techniques to provide contextual metadata that can drive actionable mitigations and improvements to make your infrastructure more resilient to these threats. (See the sample dashboard screenshot below.)



Sixgill's portal collects millions of daily threats that originate in thousands of both deep and dark web sources. These include content from QQ, Telegram and Discord, forums that are frequented by hackers these days. It also has a deep historical archive that can be easily searched. Because of these features, it can find early warnings of potential threats that haven't yet appeared across the public Internet, so you can be better prepared when these intrusions begin. And the Sixgill portal also hides your own investigations from the darkweb, something that makes them more covert and secure because your searches are anonymized. In addition, while most vendors rely on manual work of analysts to collect data, Sixgill collects up to 11.5x more through automation.

Looking to be master of my own domain

Let me show you a typical piece of threat intelligence that can be found on Sixgill's portal. I set up a search using my own "strom.com" domain, a domain that I have owned for decades and run both its web and email servers. Setting up this search term took seconds, and I began to receive periodic email notifications about potential abuses found on the dark web, including compromises that were first discovered several years ago and are still being exploited today.

What is curious about this entry is that it is a fictitious credential and shows a user that I know never existed on my domain. Given that I have owned the account, I know exactly the entire user list and kurt@strom.com has never been one of them. One possible explanation for this could be just a mistake on the part of a scammer, since my domain is just a few letters, it could also be a typo.

The alerts I received had copious details, including what credentials were used (including passwords) and recommended actions for defenders to take to prevent subsequent repeat attacks.

How is this content different from other threat intelligence providers? Many would only capture some of the deep and dark web and have major lag time in discovering new threat details about an attack. Sixgill not only collects and provides comprehensive data in real-time, but also enriches it with metadata, context and other actionable insights from a single pane of glass. These can be used to programmatically interact with other security tools such as SIEMs, SOARs, TIPs, Firewalls -- all of which Sixgill can integrate with. It can also enable the analysts to easily do smart analytics on the datasets, such as automatically compiling threat actor profiles so you can track where and what other related attacks have appeared in the underground. These automation features increase ROI as you can preemptively stop attacks and do a lot of threat analysis with just a few staffers, because they don't have to manually comb through alerts and log files to find specific threat evidence.

Evaluating a threat intelligence product

If you are looking for a great threat intelligence product, keep in mind these items:

- Where did this threat originate and who are the actors behind the threat?
- Does your threat intelligence include items from outside the public web?
- What actions were attributed to the threat?
- Which data structure was harmed, scanned or otherwise targeted?
- When did it happen?
- Why was this threat missed (if it was) by your other security apparatus?
- Does your threat intelligence collection integrate with other security tools programmatically?
- What automated methods are used to collect and augment the intelligence?

About Sixgill

Sixgill's fully automated threat intelligence solution helps organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response -- in real-time. Sixgill's investigative portal empowers security teams with contextual and actionable alerts along with the ability to conduct real-time, covert investigations. Rich intelligence streams such as *Darkfeed*™ harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include global 2000 enterprises, financial services, MSSPs, governments and law enforcement entities. Learn more at www.cybersixgill.com

About David Strom

David Strom (@dstrom, strom.com) is one of the leading experts on information security, network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, Internet applications, wireless and Web services for more than 35 years. He has held several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries,

including the editor-in-chief of *Network Computing*, DigitalLanding.com, and Tom's Hardware.com. He has also written two books on computer networking. He began his career working in varying roles in end user computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College and lives in St. Louis.