**The Dark Web: Insights From A Cybersecurity Professional**

How much do you and your students know about the dark web?

The National Convergence Technology Center (CTC) at Collin College attended a virtual presentation by Information Security Systems Association on cybercrime and the dark web. The presentation was by Michael Mayes, an executive from the global cybersecurity company, Armor.

* While there may be over 1.5 billion URLs on the indexed “surface web,” there are over 8000 active links and over 100 markers on the “dark web” that can only be accessed by specific means.
* Anonymous marketplaces provide specialized platforms for the sale of hacker exploit kits, downloadable malware, and infected AWS and Azure servers. These tools and resources are “readily available” to cybercriminals on the dark web. Anonymous marketplaces are the “most significant development in e-commerce and cybercrime.”
* The dark web also offers “cybercrime as a service” that provides subscription models, robust customer service, pre-packaged software tools, and simple plug-and-play tools. It’s a criminal mirror image of familiar cloud-style services, all of it designed to make it easy for novice cybercriminals to do business. One example: A Distributed Denial of Service attack runs $60/hour or $2000/month.
* Forty-six percent of all bitcoin transactions – which total $76 billion – involve cybercrime. Cryptocurrency funnels through thousands of exchanges.
* The dark web has provided a boom to COVID-19 fraud as phony businesses collect relief money and merchants sell scare supplies like black-market PPE and testing kits and also phishing strategies and tools to leverage health fears.
* Ransomware continues to be a low-cost, high-reward pursuit – driven by RaaS Ransomware-as-a-Service – that rarely results in arrest or prosecution. Companies typically pay the ransom. It’s a threat that continues to grow and evolve.
* A recent survey of 150 security executives commissioned by IDG’s CIO and CSO magazines reported an overall 26% uptick (37% for those in the financial industry) in cybersecurity attacks. That same survey reported that 61% of the executives were concerned about the new security risks presented by the [“work from home”](https://www.idg.com/news/latest-research-shares-how-it-and-security-leaders-are-addressing-the-current-social-economic-landscape/) trend caused by COVID-19.

Michael Mayes is a senior writer and researcher at Armor, a cloud security-as-a-service provider in Richardson, Texas. His career in technology communications includes work with the Human Genome Project, handheld software during the Palm and Pocket PC era, blockchain development and cybersecurity. He began his research in black markets in 2013 during a PhD year in professional and technical writing at the University of Memphis where he wrote on the early days of Bitcoin and its defining proof of concept, the Silk Road.

To learn more, you can download Armor’s 2019 Black Market Report [here.](https://www.armor.com/resources/the-black-market-report/)

<https://connectedtech.org/blog/the-dark-web-insights-from-a-cybersecurity-professional/>