MITSloan
Management Review

Casting the Dark Web in a New Light

Magazine: Fall 2019 Issue • Research Feature • July 15, 2019 • Reading Time: 17 min

Keman Huang, Michael Siegel, Keri Pearlson, and Stuart Madnick

By examining cybercrime through a value-chain lens, we can better understand how the ecosystem works and find new strategies for combating it.

With cyberattacks increasingly threatening businesses, executives need new tools, techniques, and approaches to protect their organizations. Unfortunately, criminal innovation often outpaces their defensive efforts. In April 2019, the AV-Test Institute, a research organization that focuses on IT security, registered more than 350,000 new malware samples *per day*, and according to Symantec's 2019 Internet Security Threat Report, cyberattacks targeting supply chain vulnerabilities increased by 78% in 2018.[1]

Wide-scale attacks are becoming more common, too. In October 2016, a distributed denial-of-service (DDoS) attack that hit Dyn, a domain name system (DNS) provider, in turn brought down companies such as PayPal, Twitter, Reddit, Amazon, Netflix, and Spotify.[2] In 2017, the WannaCry and NotPetya ransomware attacks affected health care, education, manufacturing, and other sectors around the world. A report from the Department of Health in the U.K. revealed that WannaCry cost it 92 million pounds.[3] That same year, while the cyber-defense community was working out how to fight ransomware, cryptojacking — the hijacking of other people's machines to mine cryptocurrency — arose as a threat. Cryptojacking attacks they have a magical recipe for innovation that enables them to move more quickly? If, as is commonly believed, hackers operated mainly as isolated individuals, they would need to be incredibly skilled and fast to create hacks at the frequency we've seen. However, when we conducted research in dark web markets, surveyed the literature on cyberattacks, and interviewed cybersecurity professionals, we found that the prevalence of the "fringe hacker" is a misconception.

Through this work, we found a useful lens for examining how cybercriminals innovate and operate. The value chain model developed by Harvard Business School's Michael E. Porter offers a process-based view of business.[6] When applied to cybercrime, it reveals that the dark web — that part of the internet that has been intentionally hidden, is inaccessible through standard web browsers, and facilitates criminal activities — serves as what Porter called a value system. That system includes a comprehensive cyberattack supply chain, which enables hackers and other providers to develop and sell the products and services needed to mount attacks at scale. Understanding how it works provides new, more effective avenues for combating attacks to companies, security service providers, and the defense community at large.

The Dark Web's Marketplaces

The dark web hosts various cyberattack-as-a-service (CAaaS) marketplaces and forums that cater to a criminal ilk of technologists and businesspeople.[7] Rather than orchestrate a hack themselves, the technologists can use the dark web to develop and sell the components needed to launch an attack as well as offer expertise and other services needed to complete an attack. The businesspeople buy these services and combine them to orchestrate attacks.

For example, when we surveyed the dark web in June 2017, we found personal profiles (the more personal, the more valuable) for sale: In one case, a pharmacy database with more than 50,000 customer profiles including email addresses was available for $1,000. Silent bitcoin miners used for cryptojacking also were being sold for as little as 2.25 euros (then about $2). And criminals who wanted to launch phishing attacks needed to look no further than Dream Market, one of the largest dark web marketplaces, where they could purchase a phishing service, along with an SMTP server, to replicate phishing emails, an automated mailer application to send the emails, fraudulent websites, and high-quality email lists of individuals and businesses. The collective cost: around $100 per month.

Recently, artificial intelligence has been harnessed to create even more powerful CAaaS dark web offerings. With the help of AI, personal information collected from Twitter, Facebook, and other social media sites can be used to automatically generate phishing emails and posts with open rates as high as 60%.[8] This is a higher rate than found in so-called spear phishing campaigns, in which attackers manually research victims and create targeted messages. In another example, in 2018, cybersecurity firm Darktrace reported spotting a never-before-seen attack that used rudimentary machine learning to observe, learn, and mimic patterns

The authors analyzed service samples in dark web markets and surveyed academic literature and publicly available reports. (See K. Huang, M. Siegel, and S. Madnick, "Systematically Understanding the Cyber Attack Business: A Survey" for more details about the research method.)

They also interviewed more than 30 cybersecurity executives, managers, and researchers from Fortune 500 companies and key cybersecurity solution providers.

other dark web providers don't need to perform attacks to realize benefits from their innovations, and their customers don't need to be hackers to mount attacks. The "as a service" model distances developers from the attacks enabled by their products and services as they don't need to be directly involved in the specific cyberattack activity. It helps them evade the grasp of authorities, as well, because many services in CAaaS marketplaces are not fundamentally illegal. For instance, a service that creates emails might not break any laws on its own but can still be used as part of a process for illegal phishing. The same is true for help desks, payment systems, and other services that can be used to support the development or launch of an attack. With all this open space and freedom, hackers can more easily create new modules. They also can steal and sell tools developed by others, such as the National Security Agency.[10]

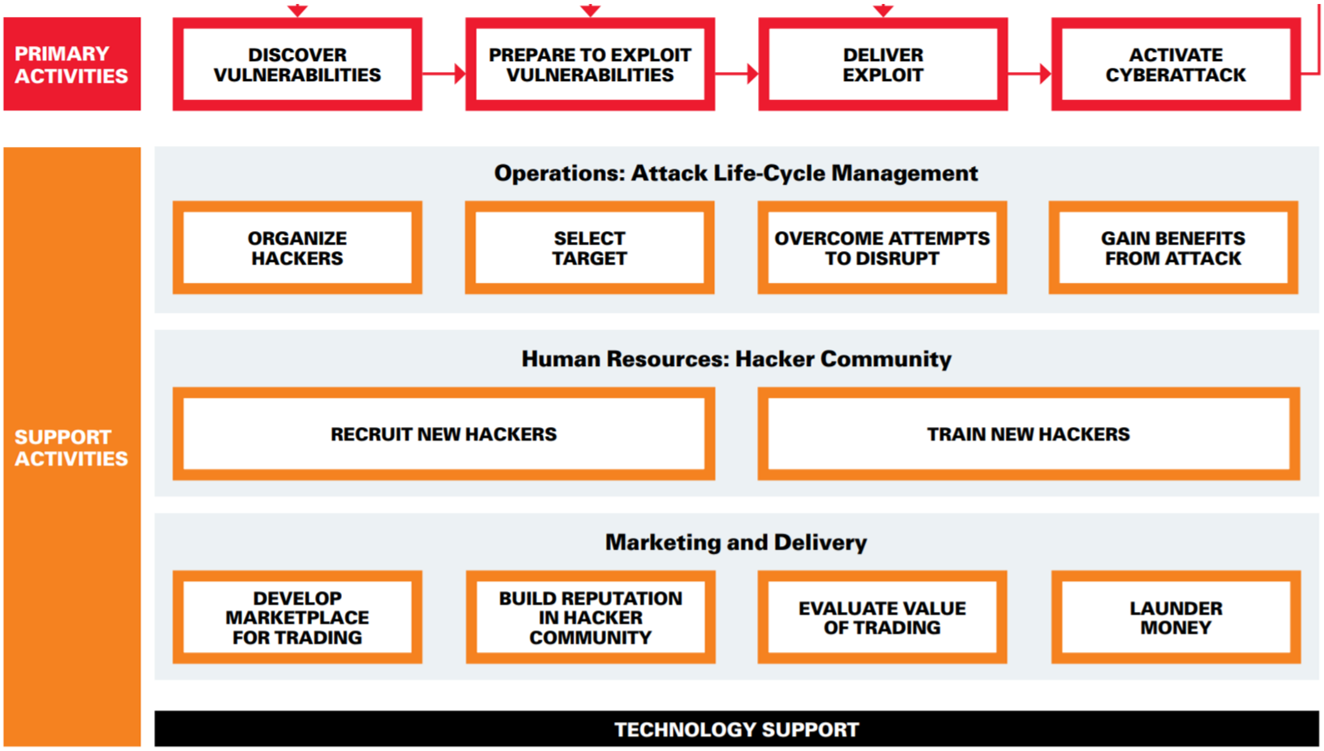
The services offered are not randomly chosen but, rather, purposefully designed, innovative responses to business opportunities — sometimes with the help of cutting-edge technologies. For example, Joker's Stash, a large dark web marketplace that offers PPaaS (personal profile as a service), uses a blockchain-based DNS to make it more difficult for law enforcement agencies to trace and take down its systems.[11] In another instance, in January 2018, a Reddit user named "deepfakes" used open-source AI to create fake porn videos featuring celebrities and politicians. Shortly after, FakeApp, a desktop application that makes it easy for anyone to generate their own fake porn videos, appeared — demonstrating just how effective AI can be at improving attack and deception services, and making this technology a major concern.[12]

Thus, we see cybercrime evolving from a nefarious hobby into a business ecosystem and value chain with a global scope. No wonder it is difficult, if not impossible, for the defense community to keep up.

The CAaaS Value Chain

When we examined the services available on the dark web, we looked for any activity that could help an attacker, reduce the cost of an attack, or increase the benefit derived from an attack, each time asking "What is the value added?" That exercise revealed a value chain of primary activities needed to create cyberattacks and support activities that make the attacks more efficient and effective. (See "Activities in the Cybercrime Ecosystem.")

Activities in the Cybercrime Ecosystem

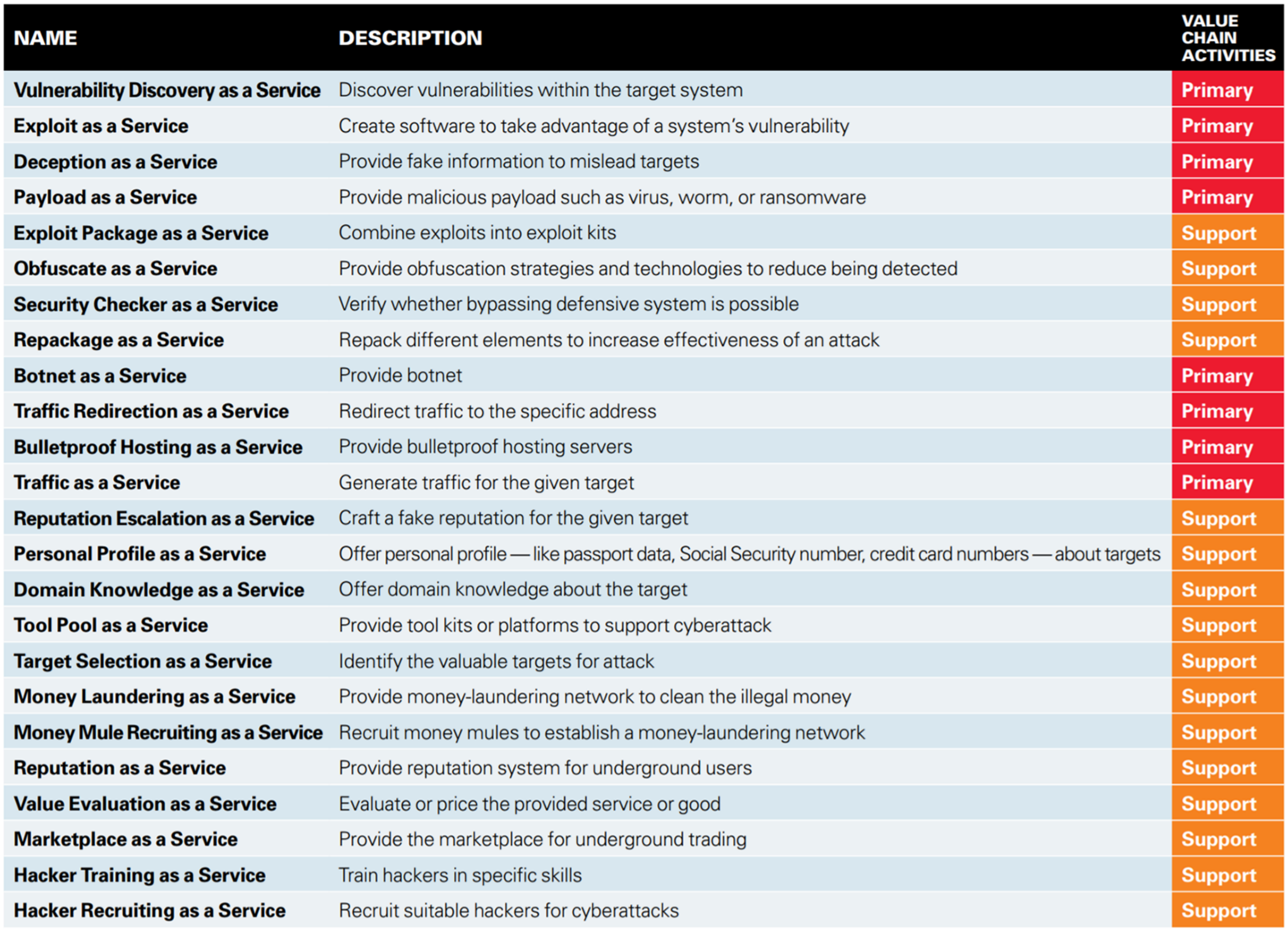

PRIMARY ACTIVITIES
DISCOVER VULNERABILITIES
PREPARE TO EXPLOIT VULNERABILITIES
DELIVER EXPLOIT
ACTIVATE CYBERATTACK
SUPPORT ACTIVITIES
Operations: Attack Life-Cycle Management
ORGANIZE HACKERS
SELECT TARGET
OVERCOME ATTEMPTS TO DISRUPT
GAIN BENEFITS FROM ATTACK
Human Resources: Hacker Community
RECRUIT NEW HACKERS
TRAIN NEW HACKERS
Marketing and Delivery
DEVELOP MARKETPLACE FOR TRADING
BUILD REPUTATION IN HACKER COMMUNITY
EVALUATE VALUE OF TRADING
LAUNDER MONEY
TECHNOLOGY SUPPORT

The primary activities of the value chain include the services needed to mount the attack: the discovery of vulnerabilities, the development and delivery of the weapons needed to exploit those vulnerabilities, and the execution of the cyberattack — whether a single action, a multistep attack, or an advanced persistent threat in which attacks remain undetected for an extended period. Support activities facilitate the cyberattack business by reducing the cost and increasing the benefit of an attack. Life-cycle management operations include activities that help select valuable attack targets, organize hackers, manage the distribution of proceeds, hide the operation from authorities, and if disrupted, recover the sidelined operation. Hacker human resources services include hiring, training, and managing trusted hackers. Marketing and delivery provides a reliable marketplace for service providers and buyers, a market-based pricing mechanism, and a system for transferring funds. Technology support offers tools and functional operations such as customer service.

The CAaaS value chain exposes the links between the attack services available on the dark web, as well as gaps that present opportunities to develop new services. (Wherever there is a demand to make cyberattacks more efficient or profitable, we can assume service providers will be motivated to fulfill that demand.) Using this value chain model, we identified 24 key primary and supporting services for sale on the dark web. For example, security checker as a service (SCaaS) provides a simulated environment to evaluate and test whether exploitations can bypass cybersecurity defenses prior to an actual attack, and deception as a service (DaaS) generates the fake websites, emails, and software used to mislead victims. Reputation as a

Services in the Cybercrime Ecosystem

The ecosystem consists of 24 key primary and supporting services. Here, these activities are listed roughly in “value chain” order, though they can be combined in myriad ways to develop and mount attacks.



NAME	DESCRIPTION	VALUE CHAIN ACTIVITIES
Vulnerability Discovery as a Service	Discover vulnerabilities within the target system	Primary
Exploit as a Service	Create software to take advantage of a system’s vulnerability	Primary
Deception as a Service	Provide fake information to mislead targets	Primary
Payload as a Service	Provide malicious payload such as virus, worm, or ransomware	Primary
Exploit Package as a Service	Combine exploits into exploit kits	Support
Obfuscate as a Service	Provide obfuscation strategies and technologies to reduce being detected	Support
Security Checker as a Service	Verify whether bypassing defensive system is possible	Support
Repackage as a Service	Repack different elements to increase effectiveness of an attack	Support
Botnet as a Service	Provide botnet	Primary
Traffic Redirection as a Service	Redirect traffic to the specific address	Primary
Bulletproof Hosting as a Service	Provide bulletproof hosting servers	Primary
Traffic as a Service	Generate traffic for the given target	Primary
Reputation Escalation as a Service	Craft a fake reputation for the given target	Support
Personal Profile as a Service	Offer personal profile — like passport data, Social Security number, credit card numbers — about targets	Support
Domain Knowledge as a Service	Offer domain knowledge about the target	Support
Tool Pool as a Service	Provide tool kits or platforms to support cyberattack	Support
Target Selection as a Service	Identify the valuable targets for attack	Support
Money Laundering as a Service	Provide money-laundering network to clean the illegal money	Support
Money Mule Recruiting as a Service	Recruit money mules to establish a money-laundering network	Support
Reputation as a Service	Provide reputation system for underground users	Support
Value Evaluation as a Service	Evaluate or price the provided service or good	Support
Marketplace as a Service	Provide the marketplace for underground trading	Support
Hacker Training as a Service	Train hackers in specific skills	Support
Hacker Recruiting as a Service	Recruit suitable hackers for cyberattacks	Support

We identified the inputs, outputs, and supports for each service in the CAaaS ecosystem. Then we identified potential combinations of services, based on the interactions among their inputs, outputs, and supports, to demonstrate how they can be used to mount attacks. Together, these services comprise a comprehensive supply chain of attack capabilities.

Making Money in This Ecosystem

The service providers use several different pricing models. In many cases, their offerings are available for a onetime fee for unlimited use. For example, in June 2016, a Microsoft Office zero-day vulnerability (that is, a vulnerability not previously discovered and with no known fix) was priced at $30,031 in bitcoin in a dark web market. A one-day vulnerability (that is, a publicly known vulnerability for which a patch is often available but not deployed) cost about $648.10, including the exploit.

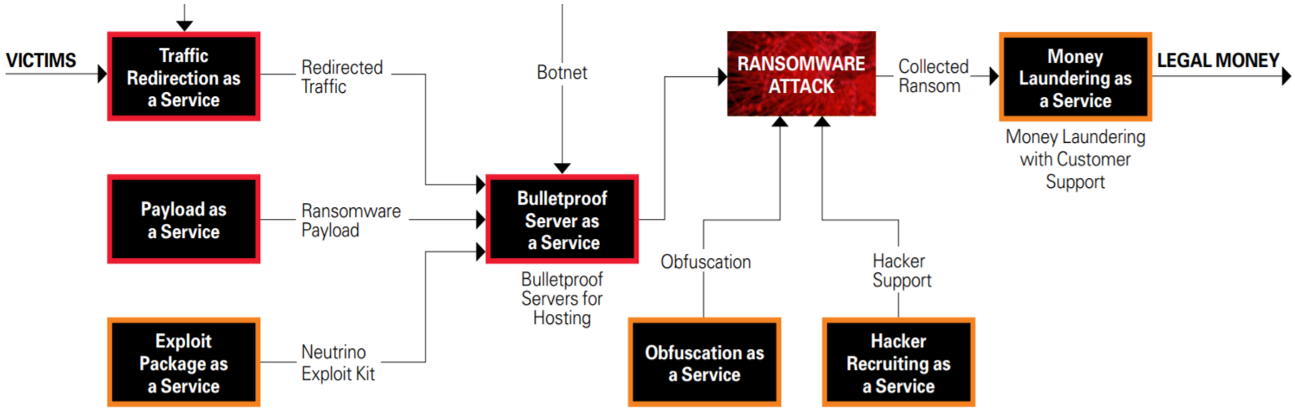
Some service providers adopt more creative, pay-for-results pricing models. For example, malware is sometimes sold on a pay-per-install basis in which buyers pay only a fee, typically in the range of 2 cents to 10 cents, if and when the malware is successfully installed on a victim's machine.[13] There are profit-sharing pricing schemes: GandCrab ransomware offers a partner program in which members share 40% of the profits with the developers.[14] There also are subscription models in which buyers receive updates and improvements in return for an ongoing fee: The Shadow Brokers' Dump Service is a "zero-day vulnerabilities and exploits" service that offers monthly subscribers access to continually updated lists of vulnerabilities, tools, and data sets.

In contrast to service providers, attack creators are often business-savvy managers, not tech gurus. They conceive attacks and then use the services in the CAaaS value chain to execute them.

To create and execute a ransomware attack (as shown in "One of Many Possible Combinations"), an attack creator can buy the Neutrino exploit kit packaged with a ransomware payload (complete with customer support), the bulletproof servers to host the exploit kit and ransomware payload, a botnet as the infrastructure, an obfuscation service to make it more difficult for an antimalware solution to detect the attack, and a traffic redirection service to bring victims to the servers. If the creator encounters problems running the attack, he or she can hire a hacker with previous ransomware experience to solve technical issues. In addition, the creator can hire a service to collect the ransom in cryptocurrency and a money-laundering service to safely obtain it.

One of Many Possible Combinations

Here is one way that services available on the dark web can be assembled to mount a complete ransomware attack.


VICTIMS
Traffic Redirection as a Service
Redirected Traffic
Botnet
RANSOMWARE ATTACK
Collected Ransom
Money Laundering as a Service
LEGAL MONEY
Money Laundering with Customer Support
Payload as a Service
Ransomware Payload
Bulletproof Server as a Service
Bulletproof Servers for Hosting
Obfuscation
Hacker Support
Exploit Package as a Service
Neutrino Exploit Kit
Obfuscation as a Service
Hacker Recruiting as a Service

Based on prices we've observed on the dark web, the combination of services described above would likely cost the attack creator about $13,000 per month, plus a 40% commission on any gains processed through a money-laundering service. Based on revenue for the Angler exploit kit reported by Cisco in 2017 and an understanding of advanced defensive efforts, it is reasonable to assume that such an attack would redirect 900,000 users per month to the servers hosting the exploit kit and ransomware payload.[15] If only 10% of the 900,000 users were frozen out of their machines and 0.5% of the victims paid a $300 ransom, the attack would earn $81,000 per month for the attackers after money-laundering commissions. Overall, the attack would produce an ROI of more than 500%.

Success Begets Success

Within the cyberattack-as-a-service value chain, a successful attack can enhance the entire chain's ability to rapidly generate new attacks. For example, after a group named The Shadow Brokers stole EternalBlue and DoublePulsar, vulnerability exploitation tools developed by the National Security Agency, in a cyberattack in August 2016, the tools enabled new services such as TPaaS (tool pool as a service) and became part of the arsenal used in the WannaCry ransomware attacks in May 2017.[i]

In other cases, successful attacks can set the stage for follow-on attacks. For example, compromised machines can be infected with malware that creates botnets, which then reach out to other machines and infect them.

Cyberattacks can also expose new vulnerabilities to be exploited. For instance, personally identifiable information — such as Social Security numbers, digital images, and geolocation and biometric data collected from data breaches and social media and sold on the dark web — provides fodder for subsequent executives, such as CEOs and CFOs, to gain access to corporate funds and sensitive data.

There are many other examples of new services that are automatically generating attacks, and new vulnerabilities that follow from initial attacks. These enable the dark web ecosystem to grow and expand quickly, making it difficult for organizations to keep up appropriate defenses.

Changing the Defensive Playbook

Examining cyberattacks through the lens of a value chain reveals organized businesspeople using proven business models within a well-defined ecosystem governed by the dictates of supply and demand. This CAaaS ecosystem makes mounting targeted, scalable cyberattacks quicker, cheaper, and more difficult to stop. But understanding all that helps organizations reimagine how to combat cyberattacks. They can fight back in the following ways:

1. Expand the focus of cyber-threat intelligence. Many cyber-threat intelligence services collect data from enterprise IT environments to detect potential cyber threats. There is some investigation of the dark web, but it is usually limited to harvesting threat information and alerting potential targets. Investigators, for example, can find out whether a company's data is being traded in a dark web marketplace or whether its machines are part of botnets. But rarely do threat intelligence processes look at services provided in these marketplaces.

Because many of today's cyberattacks are created by linking services, the emergence of new services can alert defenders and potential targets to the kinds of attacks that may be brewing. For example, the spike in data breach incidents over the past few years suggests that we will likely see an increase in services offering personal profiles and, thus, in the number and kinds of attacks that use personal profiles. Monitoring and investigating these services can yield insights into new and more effective defense mechanisms.

Furthermore, since we know that the demand exists for services that will enhance the business case for attackers and that providers will work to fill that demand, we should be able to identify and potentially block emerging attack vectors. For example, when cryptojacking services like Coinhive, CryptoLoot, and JSEcoin emerged in dark web markets and the price of cryptocurrency skyrocketed in late 2017, we could have expected the increase of cryptojacking attacks that occurred in early 2018.

2. Pursue a good offense as the best defense. Cyber strategy in most organizations is mainly reactive. Companies defend themselves after successful attacks have been launched. A value-chain-based view of attacks enables a more proactive strategy: We can switch to playing offense by disrupting the CAaaS ecosystem.

infiltrated Hansa, one of the largest dark web markets at the time, and collected information for a month before acting against the service providers and attack creators using it. The operation not only shut down Hansa but also had the knock-on effect of eroding trust in other dark web markets.[17]

Another offensive strategy is to disrupt select services that are frequently used to create attack vectors, thereby making it difficult and risky to orchestrate an attack. For example, by monitoring and infiltrating botnet services, law enforcement agencies can anticipate and prevent attacks that use them. Likewise, infiltrating cryptocurrency-based money-laundering services could deter attackers by making it difficult for them to access their illegal gains.

3. Create a cyber-defense service value chain. If cybercriminals can create a value chain that makes it easier and more profitable to launch attacks, why can't we build a defensive value chain? Cyberattack defense cannot be relegated to law enforcement agencies alone. Instead, it requires an ecosystem aimed at combating cybercrime that includes many actors — individuals, corporations, software and hardware providers, cybersecurity solution providers, infrastructure operators, financial systems, and governments — working together.

Ideally, for instance, we would see governments supporting the creation of a defensive value chain with policies and regulations. Infrastructure operators, such as the internet service providers, would use their advantaged monitoring position to disrupt the delivery of cyberattacks. Financial institutions would act to block the monetary activities of cybercriminals, including their money-laundering networks and cryptocurrency monetization activities.

Granted, bringing together such disparate parties with so many interests is a Herculean task, and it's not entirely clear how it should be approached. One possibility is to better align the capabilities needed to combat cybercrime with financial incentives to act. If organizations demonstrate sufficient demand and willingness to pay for cyber defense as a service — so that it can essentially compete with cyberattacks as a service for providers and resources — a robust defense ecosystem is more likely to materialize.

No matter how it is accomplished, however, collecting defense services into a value chain would likely motivate more service providers to create and sell as-a-service cyber-defense offerings, expanding the menu of activities that could be assembled by defenders to thwart attacks. Fighting fire with fire would be far more effective than today's splintered efforts.

4. Approach defense as a business problem first, not a technology problem. When business leaders ask, "How can we prepare for unknown cyberattacks?" they often assume that attackers are using new and perhaps unknown technologies. Although this is sometimes true, frequently the attackers and defenders use the same technologies: DDoS attacks, for example, use technology originally developed for software stress testing. Ironically, many technologies used in attacks were initially developed by the defense vulnerabilities that attackers may prey upon, and enable potential targets to anticipate next moves. Organizations can also use their managerial expertise in business processes, operations, and strategies to help create a more complete perspective on cyberattacks. Protecting the business and detecting, responding to, and recovering from attacks is not solely the responsibility of technology experts.

As cyberattacks are becoming more frequent, dynamic, and damaging, it is clear that the current defensive mindset is not adequate to stem the tide. We need to shift our view of cybercrime from that of a chaotic, random set of events to that of a structured, often predictable set of business engagements and processes. Understanding cybercrime as an orchestration of services available on the dark web offers new insights into potential threats and effective ways of fighting them. It’s long past time to start beating the bad guys at their own game.

ABOUT THE AUTHORS

Keman Huang is a research scientist at Cybersecurity at MIT Sloan (CAMS). Michael Siegel is a principal research scientist at the MIT Sloan School of Management and codirector of CAMS. Keri Pearlson (@kpearlson) is the executive director of CAMS. Stuart Madnick is the John Norris Maguire Professor of Information Technology in the MIT Sloan School of Management, professor of engineering systems in the MIT School of Engineering, and codirector of CAMS.

2. P. Roberts, “Exclusive: Mirai Attack Was Costly for Dyn, Data Suggests,” The Security Ledger, Feb. 3, 2017, https://securityledger.com.

3. D. Palmer, “This Is How Much the WannaCry Ransomware Attack Cost the NHS,” ZDNet, Oct. 12, 2018, www.zdnet.com.

4. Symantec, 2018 Internet Security Threat Report, March 2018.

5. Symantec, 2019 Internet Security Threat Report.

6. M.E. Porter, Competitive Advantage: Creating and Sustaining Superior Performance (New York: The Free Press, 1985).

7. K. Huang, M. Siegel, and S. Madnick, “Systematically Understanding the Cyberattack Business: A Survey,” ACM Computing Surveys 51, no. 4 (July 2018).

8. J. Seymour and P. Tully, “Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter,” Black Hat USA, 2016, www.blackhat.com.

9. “The Next Paradigm Shift: AI-Driven Cyberattacks,” white paper, Darktrace, Cambridge, England, 2018.

10. R. Hackett, “Hackers Have Allegedly Stolen NSA-Linked ‘Cyber Weapons’ and Are Auctioning Them Off,” Fortune, Aug. 16, 2016, www.fortune.com.

11. B. Krebs, “Will the Real Joker’s Stash Come Forward?” Krebs on Security (blog), May 2018, https://krebsonsecurity.com.

12. J. Brandon, “Terrifying High-Tech Porn: Creepy ‘Deepfake’ Videos Are on the Rise,” Fox News, Feb. 20, 2018, www.foxnews.com; and “Deepfake,” Wikipedia, https://en.wikipedia.org; Reddit banned the /r/fakeapp channel in February 2018.

13. J. Caballero, C. Grier, C. Kreibich, et al., “Measuring Pay-per-Install: The Commoditization of Malware Distribution,” USENIX Security Symposium, 2011: 13

14. “Behind the Veil — GandCrab Ransomware Partner Program,” LMNTRIX Labs, Feb. 3, 2018, www.lmntrix.com.

15. Cisco, 2016 Annual Security Report, January 2016.

16. T. Moore, “Introducing the Economics of Cybersecurity: Principles and Policy Options,” Proceedings of a Workshop on Deterring Cyberattacks (Washington, D.C.: The National Academies Press, 2010); and M. Yip, N. Shadbolt, and C. Webber, “Why Forums?: An Empirical Analysis Into the Facilitating Factors of Carding Forums,” proceedings of the 5th Annual ACM Web Science Conference, 2013: 453-462.

17. S. Khandelwal, “Dark Web Users Suspect ‘Dream Market’ Has Also Been Backdoored by Feds,” The Hacker News, July 21, 2017, https://thehackernews.com.

i. S. Khandelwal, “Shadow Brokers, Who Leaked WannaCry SMB Exploit, Are Back With More 0-Days,” The Hacker News, May 16, 2017, https://thehackernews.com.

ACKNOWLEDGMENTS

This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

REPRINT #: 61101