WEBINAR SUMMARY

July 30, 2020

Understanding and Disrupting Offensive Innovations

Dmitri Alperovitch, Chairman, Silverado Policy Accelerator
Jason Healey, Senior Research Scholar, Columbia University's School for International and Public Affairs
Dave Amsler, Founder & CEO, Cyborg Security

KEY TAKEAWAYS

- Cybersecurity innovations come from both defensive and offensive strategies.
- The same innovations are used to defend against—and perpetrate—attacks.
- Operations and policy are the likeliest areas for disrupting offensive innovation.
- Threat hunting enables attack disruption at the organizational level.
- Cyborg Security uses these insights to disrupt attacks.

in partnership with

OVERVIEW

Despite the numerous defensive innovations developed in the last half century, attackers continue to have the advantage over defenders. Offensive innovations, which have largely come from researchers and businesses in recent years and not from criminals, have helped attackers stay ahead of their targets.

The best way to disrupt these offensive innovations is to understand what they are, where they come from, and how a mixture of technology, operational, and policy efforts can limit or stop the negative impacts to the targets. Disruption is also helped by automating a highly manual process with solutions like those offered by Cyborg Security.

CONTEXT

Jason Healey and Dmitri Alperovitch discussed how offensive innovations are aiding cyber criminals. Along with Dave Amsler, they discussed potential ways to identify and limit or stop these threats.

KEY TAKEAWAYS

Cybersecurity innovations come from both defensive and offensive strategies.

Cybersecurity often focuses on the innovations that give defenders the most advantage against attackers at the greatest scale and least cost. But, flipping the question to understand what strategies give attackers the greatest advantage also creates new security approaches.

> When you're dealing with cyberconflict you have to remember that the other side always has a move to play. This is like chess.
>
> *Dmitri Alperovitch*

In identifying the most important defensive innovations in technology, operations, and policy over the past 50 years, the New York Cyber Task Force found that most investments and metrics focus on technology *inside* the enterprise. However, this only helps a particular business and not the internet as a whole.

Process operational innovations are similarly overlooked: chief information security officer (CISO) roles, information and sharing analysis centers (ISAC), the kill chain and ATT&ACK frameworks, and security development operations (SECDEVOPS) came late, despite being difficult for attackers to bypass.

Researchers are now looking at *offensive* innovations. Some innovations came from the attacker community, but many came from researchers in the space.

Technology	– *Inexpensive rootkits*, such as Back Orifice 2000. Initially developed to embarrass Microsoft for its security holes, it provided a tool for attackers. – *Botnet and effective command and control*, which are now used to distribute large amounts of spam, malware, distributed denial of service (DDoS) attacks, and other cyberattack tools.
Operations	– *Carder markets* make use of online forums for sharing cybercriminal information. Law enforcement has infiltrated some of these forums. – *Bulletproof hosting* provides anonymous hosting infrastructure in countries that are relatively immune to law enforcement takedowns, allowing cyberattacks to be launched uninterrupted. – *Bitcoin and other anonymized payment methods* support the proliferation in ransomware attacks, as attackers have a way to collect money anonymously.
Policy	– *National sanctuaries for cybercriminals* protect attackers as long as they don't attack the host nation. – *Nation states are using proxy groups* for nefarious purposes and, in addition to payment, are ignoring criminal side jobs..

Table 1: Key offensive innovations

The same innovations are used to defend against—and perpetrate—attacks.

Numerous innovations have been created to defend against cyberattacks, while very few new innovations have come from the attackers. Instead, attackers make use of their existing innovations as well as many of the same innovations used to secure systems or by researchers to gain more insight into possible exploits.

> Attackers have not needed to innovate because they're not being forced to by strong and agile defensive moves.
>
> *Jason Healey*

Attackers also take advantage of the rush to market of new, often insecure software and Internet of Things (IoT) devices.

Technology	– *Insecure fundamental protocols*, such as border gateway protocol (BGP), transmission control protocol (TCP)/user datagram protocol (UDP), domain name systems (DNS), and internet protocols (IP) v4/v6. – *Market incentives* rewarding rushing insecure software and IoT to market.
Operations	– *Patch diffing for vulnerabilities*, allowing attackers to derive the exploit from the patch release. This is problematic as many patches are not adopted immediately, leaving systems open to attack.
Policy	– *Few and weak global cyber norms*, leading to different nations taking different paths around acceptable policies. This also creates a lack of deterrent for "grey zone" operations.

Table 2: Defender, consumer, and non-attacker innovations used to attack

Operations and policy are the likeliest areas for disrupting offensive innovation.

Despite individual organization successes in thwarting cyber criminals, the security ecosystem as a whole has not improved. While technology is the common focus of investments and metrics, true disruption of offensive innovation is mostly likely to come from operations and policy.

Technology	– Botnet disruption has not scaled when technology is used on its own. – US strategy of imposing friction, such as locking attacking countries out of their infrastructure or malware, may hinge on whether defensive disruptive operations cheaply scale.
Operations and Policy	– Botnet disruption has not scaled when technology is used on its own. – US indictments have mixed results; China has limited contracts with those indicted by the US, while Iran, Russia, and North Korea have not limited those contracts. – Potential exists to disrupt adversary trust networks (USCYBER vs. IRA). – There is promise for disruption of payment systems for monetization. With 95% of spam-advertised pharmaceutical, replica, and software products monetized using merchant services from a handful of banks, the US Treasury Department is able to sanction or take down those banks to stop the criminal activities.

Table 3: Potential areas for disruption

Together, technology along with operations and policy have had success. For example, when botnets are identified and disrupted using technology, law enforcement further ensures the disruption by arresting the people responsible so that the botnet cannot be relaunched.

Threat hunting enables attack disruption at the organizational level.

For individual organizations, disrupting would-be attackers relies on threat identification within their environment. While traditional security controls continue to see wide adoption and satisfaction amongst firms conducting threat hunting (See Fig. 2), detection of more advanced threats remains challenging and requires more advanced efforts, specifically threat hunting. However, for one-third of companies, their threat hunting processes remain nascent or are still maturing (See Fig. 1). These firms still rely on processes which remain unrepeatable, and which support only limited hunting or detection. Additionally, firms continue to depend very heavily on specific, highly skilled resources for threat hunting despite many firms acknowledging staffing as an ongoing issue.

> Threat hunting activities require a significant amount of analyst time and knowledge. And an analyst is only as good as what they know the attacker is doing today.
>
> *Dave Amsler*

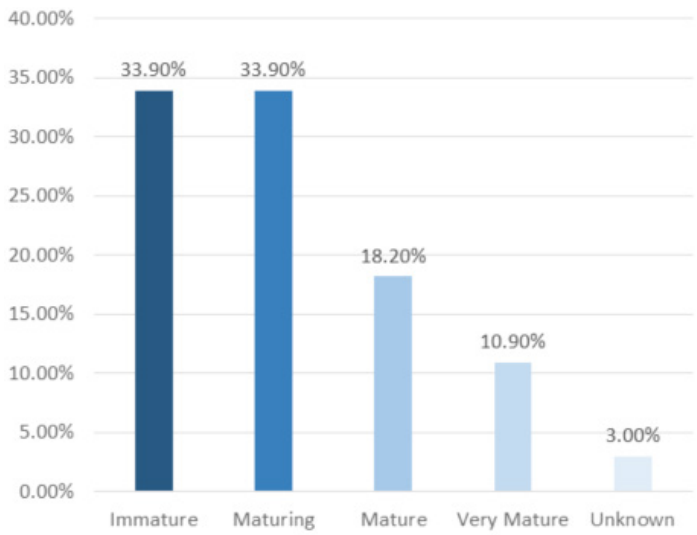

Figure 1: "What do you consider your threat-hunting maturity level?"

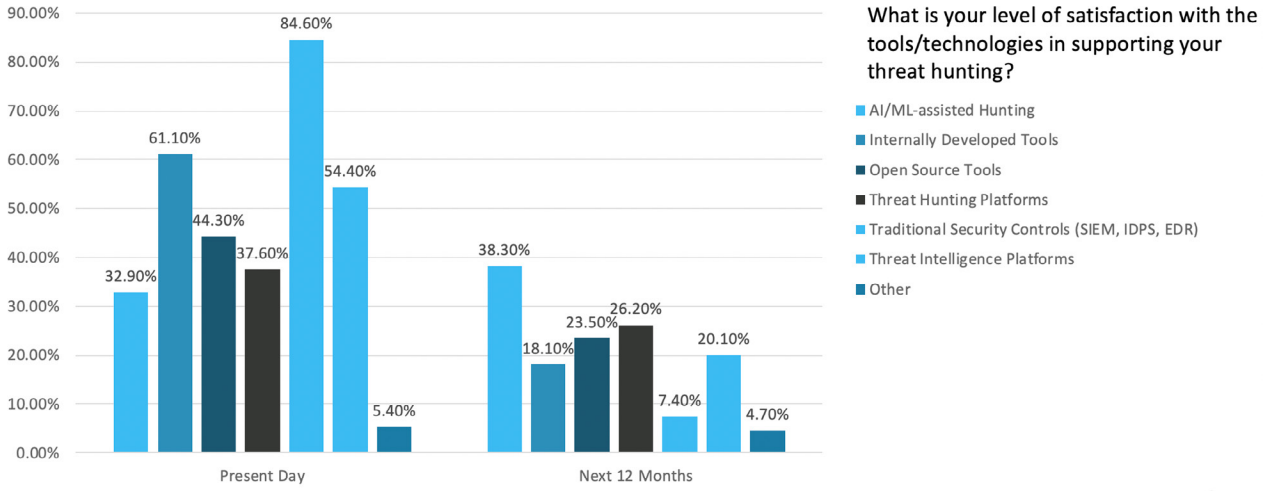

Figure 2: "What is your level of satisfaction with the tools/technologies in supporting your threat hunting?"

Another challenge that firms face is the often manually intensive nature of hypothesis-based threat hunting. The traditional hunting processes require significant effort from specific, highly skilled, analysts—from establishing a hypothesis and identifying relevant threat data and research, to establishing a hunt plan and documenting their results—and often without that effort, the hunting effort is neither rigorous nor repeatable. Not only can this process be complicated, but it often takes analysts and hunters away from their primary function: threat identification and analysis.

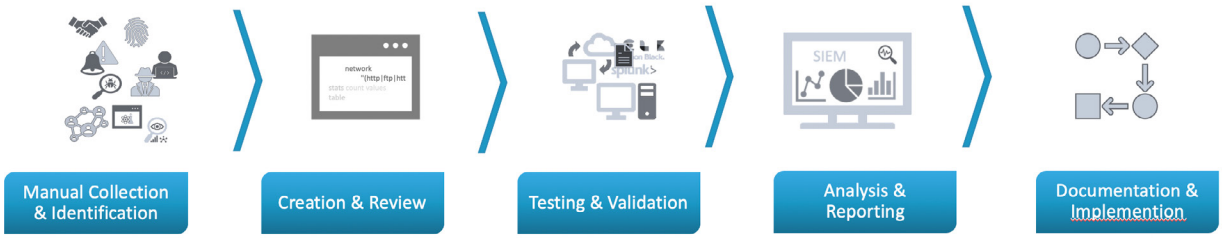

Figure 3: Threat hunting is a highly manual process

Cyborg Security uses these insights to disrupt attacks.

Cyborg Security's C.O.R.E. Platform helps organizations more effectively disrupt attacks. Using the platform, analysts can easily and effectively identify and respond to threats in a customized, automated, and repeatable way. The solution:

- Allows analysts to effectively and rapidly identify and respond to threats within their environment.
- Augments security analysts into threat hunters and evolves traditional security operations into skilled hunt teams.
- Provides access to the Cybernetic Threat Intelligence Feed.

ABOUT CYBORG SECURITY

Threat hunting is in Cyborg's DNA. Founded by a team responsible for delivering tailored threat hunting services to hundreds of clients globally, Cyborg Security is composed of some of the best cyber leadership and threat hunters in the industry. Cyborg was founded to address the problems and shortcomings observed across the industry, and to leverage that combined expertise and previous experience. Cyborg Security's core belief is that effective threat hunting cannot be achieved through artificial intelligence, machine learning, or third-party services; threat hunting relies on the foundational backbone of any security operations team: its analysts and expertise.

Cyborg is changing the threat hunting space. Through Cyborg Security's C.O.R.E. platform, organizations are able to access comprehensive hunt packages containing cross-platform threat hunting content, playbooks, threat intelligence, and comprehensive best-in-class tagging, all of which is customized for their needs and environments. By making threat hunting more accessible and reducing barriers to entry and success, Cyborg is bringing a capability that was once reserved exclusively for governmental agencies and the largest multinational corporations to all organizations.

Learn more about Cyborg Security at www.cyborgsecurity.com

BIOGRAPHIES

Dmitri Alperovitch

Chairman, Silverado Policy Accelerator

Dmitri Alperovitch is the Co-Founder and Chairman of Silverado Policy Accelerator, a non-profit focused on advancing American prosperity and global leadership in the 21st century and beyond.

He is a Co-Founder and former CTO of CrowdStrike Inc., a leading cybersecurity company. A renowned cybersecurity visionary and business executive, Alperovitch is a thought leader on cybersecurity strategy and state tradecraft and has served as special advisor to the Department of Defense.

Jason Healey

Senior Research Scholar, Columbia University's School for International and Public Affairs

Jason Healey is Senior Research Scholar at Columbia University's School for International and Public Affairs, specializing in cyber conflict and risk. He started his career as a US Air Force intelligence officer, before moving to cyber response and policy jobs at the White House and Goldman Sachs.

He was founding director for cyber issues at the Atlantic Council where he founded the Cyber 9/12 Strategy Challenge for cyber policy students and is the editor of the first history of conflict in cyberspace, *A Fierce Domain: Cyber Conflict, 1986 to 2012*. He is on the DEF CON review board and served on the Defense Science Board task force on cyber deterrence.

Dave Amsler

Founder & CEO, Cyborg Security

A recognized cybersecurity expert and experienced entrepreneur, Dave founded and self-funded Foreground Security, a leading MSP and first of its kind VSOC, building the company into the seventh largest cybersecurity services firm in North America before being acquired by Raytheon.

Dave is heavily involved in the industry and is an original investor in Swimlane, a leading vendor in the SOAR industry, as well as other startups. He has held senior leadership positions at CyberSpann and GE. He is credited with creating the threat hunting category, leading new innovations in the space, and is a well-known thought leader in the cybersecurity ecosystem.