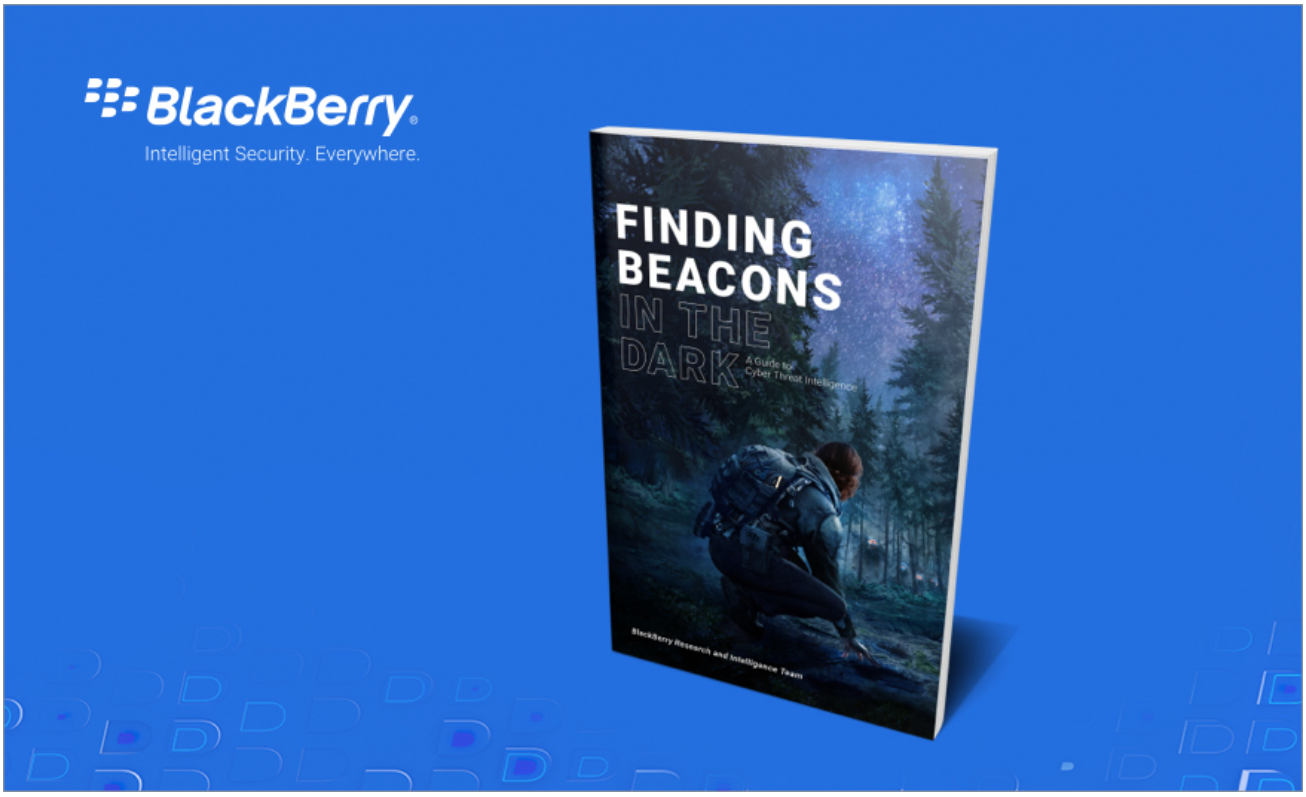
BlackBerry Shines Spotlight on Evolving Cobalt Strike Threat in New Book

blogs.blackberry.com/en/2021/10/blackberry-shines-spotlight-on-evolving-cobalt-strike-threat-in-new-book

The BlackBerry Research & Intelligence Team

RESEARCH & INTELLIGENCE / 10.13.21 / The BlackBerry Research & Intelligence Team



Nation-state backed APT groups, cyber mercenaries and cybercriminal groups use the powerful and malleable Cobalt Strike software to develop new threats. The BlackBerry Research & Intelligence Team has developed an automated system to help locate this type of threat – before it causes harm.

BlackBerry today announced a new book: *Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence*, detailing the evolution and prevalence of one of the most pervasive tools used by attackers – Cobalt Strike Beacon. This book guides the reader through a variety of techniques they can use to identify Cobalt Strike Team Servers, giving them the intelligence needed to protect themselves and their organizations against malicious Cobalt Strike payloads. It outlines how a robust Cyber Threat Intelligence (CTI) lifecycle and an extended detection and response (XDR) solution can provide defenders with the context needed to fully understand this type of threat, and be proactive in defending against it.

What is Cobalt Strike?

Initially developed as an adversary simulation tool with threat emulation capabilities, Cobalt Strike has since evolved into one of the most persistent attack methods utilized by threat actors. Threat researchers recently reported an incredible 161% year-over-year uptick in the use of Cobalt Strike by cybercriminals, making it effectively a mainstream tool in the cybercrime world. It has become a perennial problem for security practitioners, requiring robust solutions that can aid in providing defensive capabilities and enhanced threat intelligence.

Part of Cobalt Strike's attraction is its flexibility and accessibility. For these reasons, it is widely used by red teams but has become heavily abused by cybercriminals, who often use cracked or leaked copies. Threat actors can arm themselves with advanced adversarial tooling with ease, making what was once a complex affair nearly effortless. The software allows for the facilitation of many attack methods and has remained a favorite of numerous state-sponsored actors.

Cobalt Strike's primary payload, Beacon, provides a wealth of features for attackers, including keylogging, remote screenshots, data exfiltration, credential harvesting, privilege escalation, and many more. The software has played a significant role in the escalation of ransomware-based attacks over the past 18 months. The new BlackBerry® book highlights the current threats facing organizations, provides a comprehensive defense framework, and uncovers links between cyberattacks previously thought to be unrelated.

Though Cobalt Strike is sold legitimately to red-teamers, for cybercriminals, obtaining existing malware and related tools via underground forums can be significantly cheaper than developing in-house technology, making their use of Cobalt Strike ideal as it presents significant attribution challenges to law enforcement. This challenge can be further complicated when cyber-mercenary groups are working at the behest of larger actors, even up to the scale of nation-states.

"Cobalt Strike presents an almost perfect software for cybercriminals, while highlighting a central conundrum of the security sector – that well-built tools can both aid and increase cybercrime," says Eric Milam, Vice President of Research and Intelligence, BlackBerry. "Cobalt Strike is feature-rich, well supported and actively maintained by its developers. Its payload provides a wealth of features for attackers. This makes it an attractive option for APT groups and cybercrime novices alike."

What is Cyber Threat Intelligence?

In the new book, the BlackBerry Research & Intelligence Team presents a robust system for hunting the Internet for instances of Cobalt Strike Team Server, which is the command-and-control (C2) server for Cobalt Strike Beacon. In addition, they present their CTI lifecycle, which outlines a multi-phase approach to building intelligence-led protection for products and services underpinning most XDR products and services.

By following the CTI lifecycle to hunt for Team Servers, and extracting configurations from the Beacon payloads they serve, the book demonstrates how to leverage the resulting dataset to provide powerful intelligence insights. These insights can help to reveal clusters of servers associated with known threat groups and campaigns, as well as links between them that were previously unseen, empowering defenders to expose correlations between seemingly disparate network infrastructure.

BlackBerry's Goal: Turning the Hunted into the Hunter

While the increasing proliferation of Cobalt Strike use within the criminal underground presents a significant concern, so does its continued (ab)use by sophisticated APT groups. As recently as October 2021, APT41 was witnessed using the software in phishing emails targeting Indian citizens, while Dridex operators have used Cobalt Strike heavily to underpin their recent phishing and malspam campaigns.

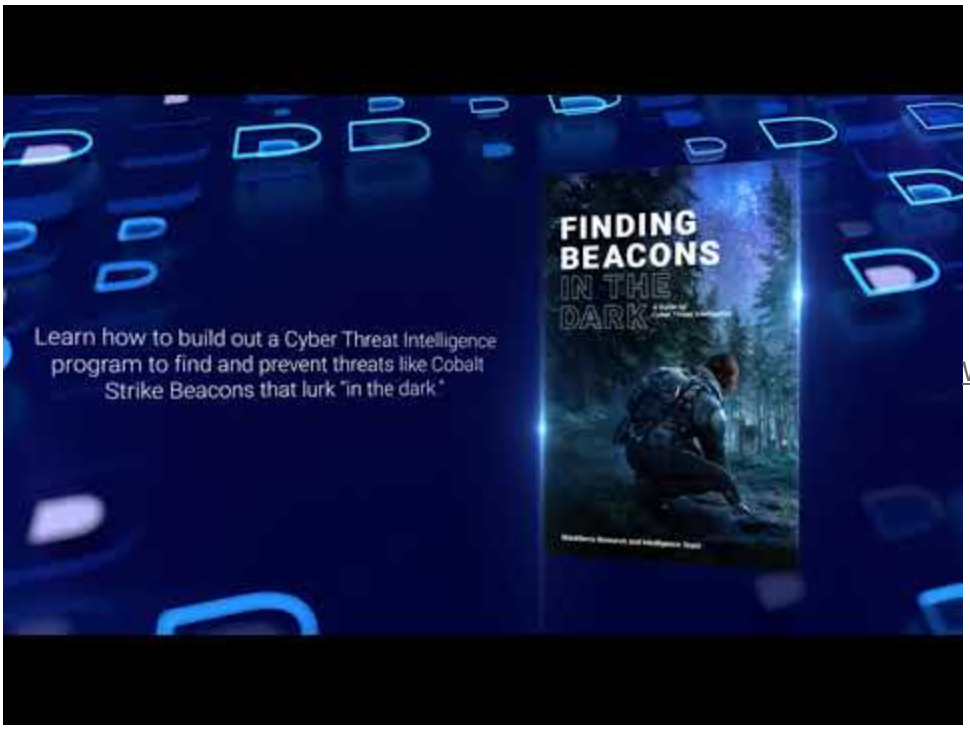
"The aim of this book is to aid the security community by sharing our knowledge, presenting the steps we've taken to create an automated system to hunt for Cobalt Strike, and most importantly, demonstrating how to derive meaningful threat intelligence from the resulting dataset," says Billy Ho, Executive Vice President of Product Engineering, BlackBerry. "This information can then be used to provide insights, trends and intelligence on threat groups and campaigns."

The resulting intelligence can also be leveraged to provide actionable Indicators of Compromise (IOCs) to all XDR stakeholders, including defenders, hunters, analysts, and investigators alike. These will help readers to:

- Defend their organizations
- Produce in-depth CTI reports
- Better understand the threat landscape
- Stay ahead of the curve and give better advice to C-level executives and security teams seeking to make well informed security decisions

The new BlackBerry book *Finding Beacons in the Dark: A Guide to Cyber Threat Intelligence* will be available in November 2021.
You can pre-order the book **here**.

Watch the video trailer below:



Watch Video At:

https://youtu.be/fAYNuBGaJng

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back