SOLUTION BRIEF

Why Your Organization Needs to Leverage the Cyber Kill Chain

Introduction

Back in 2011, scientists at Lockheed Martin created a computer security model now known as the Cyber Kill Chain (CKC). Based on elements of an earlier military security concept, the Lockheed model describes seven distinct phases of a cyber attack as it progresses toward its goal of stealing intellectual property and confidential data from your otherwise secure organizational network.

Today's targeted and highly-sophisticated Advanced Persistent Threats (APTs) typically move through each of these stages during their mission of destruction. It might take weeks or months (and sometimes years), but we cannot underestimate the determination, patience, and intelligence of cyber criminals determined to achieve their objectives.

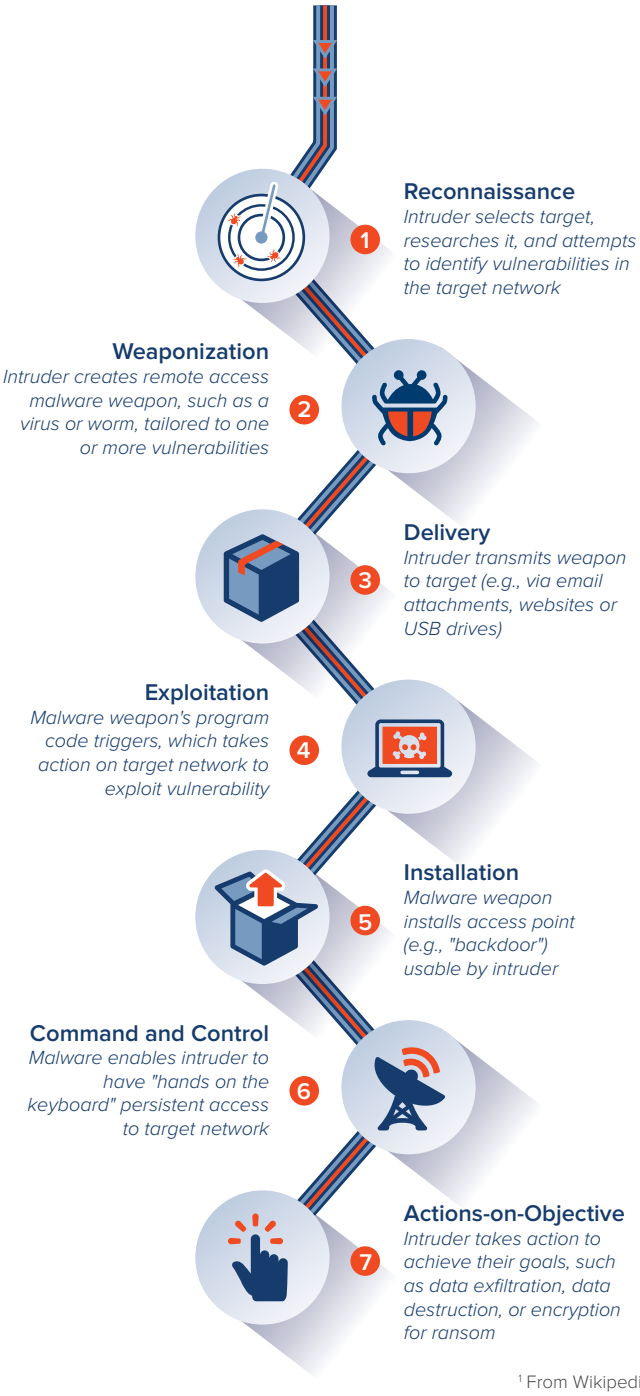
It's not surprising that the CKC model has become an increasingly useful tool for security operations teams because it can provide valuable insight into how far each threat has progressed. For example, if the threat is identified to be at the Delivery stage, it suggests that endpoint devices are possibly compromised. Obviously, that is not good, but because that action is still at a relatively early stage in the CKC, there is still time for security teams to quarantine affected devices and eliminate the threat before it can achieve its objectives. Likewise, if a threat is only identified when unusual Command & Control communications are detected between internal devices and external servers, incident response teams need to take action immediately before the threat enters the final Actions-on-Objective phase of the CKC.

Having visibility into the activity of APTs within the CKC is important for another equally important reason—it can help ensure that the security analysts and incident response team in your organization are more efficient and effective in their roles. In short, they can focus on what matters most. Too often these expensive human resources are forced to sift through a massive volume of low-level security alerts to separate true positives from false positives, decide what's most important, and determine the best course of action.

Recent research from the Ponemon Institute based on a survey of 600+ organizations revealed some disturbing trends in this regard. Consider these data points from the report:

- Security teams receive nearly 17,000 new alerts each week, generated by the tools deployed within their security infrastructure
- Nearly 96% of these alerts are ignored because they are deemed unimportant, and/or there are not enough time/resources to investigate each one

Summary of the Seven CKC Phases[1]



[1] From Wikipedia

- Organizations waste about $1.3 million annually processing alerts that turn out to be false positives
- Inevitably, a breach occurs, but it is not discovered, contained, and fully resolved for 252 days on average, costing organizations $4 million annually to clean up

If security teams were able to visualize the progress of each newly identified APT moving through each step of the CKC, it could have a significant, positive impact on the data points above. But how can we achieve that?

Intelligence In Your Security Architecture

Every organization serious about cyber security has already made significant investments in building a strong first-line of defense. That includes next-generation firewalls, secure web gateways, intrusion prevention systems, and robust endpoint security tools. These tools have proven their value in the market, and they all do a good enough job of stopping APTs before they start.

However, all of these tools—including endpoint products—must balance protection with performance. In other words, if any of these tools spends too much time inspecting traffic to make a block-or-allow decision, they could introduce network latency that slows performance, impacts user productivity, and generates a flood of complaints to the IT help desk. To minimize their impact on the network, most of these tools must apply a rules-based approach to their decision making. They quickly look at the traffic, then try to match it to an expansive list of objects identified as threats. If any object in the new traffic matches the list, it's blocked. If it looks OK (i.e., no equivalent on the list), it continues through the network. Think of it as a passport control agent quickly checking you against a "no-fly" list, while a hundred people cram in line behind you, anxious to get through. With this rules-based model, sometimes the bad stuff does get through.

When an APT can slip by your first-line of defense, that's when you urgently need clear visibility into what's happening, and where it is in the CKC. The "prevention" tools in your first-line of defense generate a lot of data that can be passed to your SIEM for more in-depth forensic analysis. But it can take a lot of time and resources to find the proverbial malicious needle in the haystack. A better option, now widely adopted by forward-leaning organizations, is to deploy a detection layer that works in conjunction with your first-line of defense and employs an advanced analytics engine that correlates all relevant threat, log, and event data so IR teams can focus their efforts on APTs that bypass this "prevention" layer.

Cyphort and the Cyber Kill Chain

Cyphort's innovative Anti-SIEM is a distributed, open software platform that seamlessly integrates with your existing security tools to deliver advanced threat detection, advanced threat analytics, and one-touch threat mitigation. The SmartCore analytics engine ingests web, email, and lateral spread traffic from Cyphort collectors, as well as relevant data from the other security tools in your network. By analyzing and correlating this data, it can then deliver to the Anti-SIEM dashboard a detailed view of how the threat has progressed through the CKC. This provides incident response teams with prioritized, actionable threat information. Just as important, security analysts can also see a consolidated, user identity-based, timeline view of the entire security incident, which includes details on all related events generated by other devices.

This innovative process within the Anti-SIEM delivers two essential values to your organization:

- **Security.** Unlike traditional SIEMs, which are weak in proactive threat detection, the Anti-SIEM focuses there first, using machine learning and behavioral analysis technologies to quickly find advanced threats. It then builds a complete actionable view around that threat. The result is reduced dwell time, faster threat resolution, and a more secure network.
- **Productivity.** The SmartCore analytics engine within the Anti-SIEM automates many of the time-consuming manual steps that security teams would normally have to deal with in order to identify the threat and determine its scope and severity. This can significantly improve staff productivity and accelerate incident response time.

To learn more about the CKC, Anti-SIEM, SmartCore technology, and their value to your organization, call us at 1.855.862.5927 or email Cyphort at info@cyphort.com.

About Cyphort

Cyphort is a privately held cybersecurity company founded in 2011 and based in Santa Clara, CA. The company provides SMB and enterprise customers with the Anti-SIEM, an open, scalable software platform that combines advanced threat detection, analytics, and mitigation capabilities. The solution minimizes the cost and complexity of traditional SIEMs, while delivering immediate, actionable insight into security incidents for fast threat resolution. www.cyphort.com

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com
Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com