SANS 2025 CTI SUMMIT
Abstract submitted by Erica Peterson and Michael J. Graven

Introduction

We'll start with a brief overview of modern sales and marketing operations - not bogging down in detail, just enough to help intelligence professionals understand the main parts of a modern marketing and sales process. What's the difference between marketing and sales? (There is a difference.) What are the critical success factors? We'll run through a quick glossary of terms, relating the words marketers use with the words network defenders use.

Then, we'll present a quick study of a good marketing campaign and sales process. Our goal in this section is to quickly construct a frame of reference for people unfamiliar with sales and marketing so they can begin to relate it to their own experience with concepts and processes they already understand.

Section 1: Marketing and Sales Are Threat Actors

With that frame of reference set, we'll make our first assertion: marketers and salespeople use TTPs that can be organized and understood the same way attackers do.

We will use the MITRE ATT&CK Enterprise Tactics as the organizing framework. Reconnaissance through Persistence roughly corresponds to marketing, and execution through Impact corresponds to sales, with overlap in the middle. We will assume the audience is familiar with the Tactics and won't belabor those definitions, focusing instead on relating them briefly back to the "what good marketing looks like" from the previous section.

(However, to avoid unnecessary conflict, we will anonymize examples unless it was work that one of us did ourselves, and we don't intend to stir the pot on really poor sales practices. Everyone can do that at the bar afterward.)

Then, we will present some of the tools that marketers and salespeople use to support the execution of the Techniques we identified.

We'll show how marketing and sales tools can be used in CTI investigations to support all-source analysis. Because we're not intelligence analysts, and we don't want to tell experts how they should do their jobs, this section will be more of "the beginning of the story," inviting the audience to think about how they might use marketing resources in their own investigative processes. We'll illustrate a few use cases from our consultation with working analysts and open the discussion for a few minutes to include the attendees in the thinking.

Section 2: Threat Actors Use Sales and Marketing

In the second section, we will flip the script and look at threat actors' use of sales and marketing activities. We will use excerpts from public reporting from several cyber threat intelligence vendors to illustrate the similarities between familiar threat actor TTPs and marketing ones. We will select a few threat actors that the audience will likely be familiar with, including at least one of the ransomware/extortion actors and at least one nation-state/APT actor.

We will return to the ATT&CK for Enterprise Tactics matrix. Again, we will downselect a few tactics of interest that illustrate the threat actors' known capabilities, and we'll relate those tactics and a few associated techniques to marketing and sales tools and techniques. There are many parallels here, so we'll pick a few examples from both the crime and the espionage side.

Then, we will turn again to public reporting to illustrate how the criminal groups are, quite literally, conducting marketing and sales. We'll share a few examples of public reporting that show how criminal threat actors market themselves to crime-as-a-service providers, such as initial access brokers, content shops, financial services, and the like. And we'll invite the audience to contribute their own examples if they've seen espionage actors doing the same.

Section 3: Taking Advantage of Other People

In the last section, we will return to CTI's business and introduce a potentially unexpected twist: marketing and salespeople could be a recruiting source for intelligence analysis teams.

Several well-known voices in threat intelligence came from journalism backgrounds. That makes sense. Effective use of threat assessments leads to decisions and actions. Succinct, clear writing to inform the reader is an exact parallel between both responsibilities.

But threat intelligence sometimes has an advocacy component to it. Effective use of threat assessments leads to decisions and actions. And that pipeline of knowledge to decision to action is paralleled in marketing and sales operations.

We will identify marketers' skill sets that map to key capabilities of intelligence analysis and reporting. We'll show several examples of good analytic output and advocacy and relate them to good marketing and sales material.

If time permits, we will also briefly survey a few topics that call back to section one: how CTI and security practitioners can work more effectively with sales and marketing inside and outside their organization. We'll show a few practical ways to reduce the annoyances of the modern vendor-customer relationship. We'll discuss the vendor's motivations and how to turn the tables on a salesperson who isn't being your "partner," no matter how much steak they buy. We will

also tell you how to keep getting the steak.

Conclusion

To conclude, we'll return to the key takeaways. We'll encourage the attendees to engage with their own sales and marketing teams to learn more about how they might use the tools available to their organization in CTI production. And we'll identify a few ways and topics that CTI recruiting can look for hidden talent in their own organizations.

Finally, no matter how much time we have, we will save two minutes to share the "five ways to get fewer cold calls" (you won't believe number three) and the "one weird trick" that will revolutionize how you work with salespeople. It will be a little silly but actionable.