The Computerworld Honors Program

Honoring those who use Information Technology to benefit society

Final Copy of Case Study

Status:
Laureate

Year:
2013

Organization Name:
Dell SecureWorks

Organization URL:
www.secureworks.com

Project Name:
Targeted Threat Intelligence Services

Please select the category in which you are submitting your entry:
Innovation

Please provide an overview of the nominated project. Describe the problem it was intended to solve, the technology or approach used, how it was innovative and any technical or other challenges that had to be overcome for successful implementation and adoption. (In 300 words or less.)

In information security, there are two generally accepted classifications for cyber threats: non-targeted or "Commodity Threats" and targeted threats or "Advanced Threats". Commodity Threats use any off-the-shelf exploit kit and send across a large array of attacks not specific to one person or organization, and are used for financial gain or simply to have fun at the expense of others. Advanced Threats focus on a specific target like a particular organization with the goal of financial gain, intelligence gathering, IP theft, etc. Traditional signature-based detection measures are not effective against advanced threat actors. In addition, signature-based detection does not correlate a series of activities to identify whether the threat is broad in application or specific to a single actor or group of actors.

Targeted threats represent a disproportionately greater risk to organizations than broad-based threats. Organizations need strong capabilities that help them address the complexities inherent in attacks by advanced threat actors in order to identify these actors and their motives, and understand their Tactics, Techniques and Procedures to effectively prevent them from achieving their objectives. The Targeted Threat Intelligence services portfolio heightens and extends security teams' visibility into threats that are specifically targeting their organizations. The Targeted Threat Intelligence services portfolio addresses the differences in actors and their behaviors to provide organizations with forward, actionable intelligence appropriate to the nature of advanced threat actors of interest. From a customer perspective, we had to be able to answer two key questions that customers might have: What are they trying to protect and who are they most concerned about? We believe we've come to market with a portfolio that addresses the realities of the marketplace. Advanced threat actors are different, they must be treated differently, and different service/execution models are necessary to effectively address the spectrum of these actors and their behaviors.

When was this project implemented or last updated? (Please specify month and year.) Has it incorporated new technologies and/or other innovations since its initial deployment? (In 300 words or less.)

The portfolio of services was first made generally available in November 2012. Yes. This project is complete and was launched to the general public on November 8, 2012. These services are now available.

Please provide at least one example of how the technology project has benefited a specific individual or organization. Feel free to include personal quotes from individuals who have directly benefited from the work. (In 300 words or less.)

Benefit 1 - Targeted Threat Surveillance service. A customer IP address was found in a DDoS booster. As a result, the customer was able to prepare for the attack and noticed that during the planned timeframe, fraudulent ACH transfers were being attempted. In this case, the DDoS activity was intended to distract IT Security and other personnel so that ACH transfers would go about undetected. Benefit 2 Enterprise Brand Surveillance. We were able to view a detailed analysis by threat actors of a targeted corporation’s new website prior to the website’s launch, and worked with our customer’s developers to address vulnerabilities known to the attackers. This ensured that the website could be launched successfully with proper security protections in place to prevent tampering or attacks by malicious actors. Benefit 3 Executive Threat Surveillance. We discovered that an executive was being targeted by a hacktivist group. This allowed the customer to issue appropriate take down notices to websites where sensitive information on the executive was found. This resulted in the sensitive information being removed and no longer accessible.

Would this project be considered an innovation, a best practice or other notable advancement that could be adopted by or tailored for other organizations and uses? If yes, please describe that here. (In 300 words or less.)

This project represents a major advancement in providing threat intelligence information that is specific to business customers and similar organizations. It addresses the various types of advanced threat actors and the Techniques, Tools and Procedures they employ. The service addresses the clear need for intelligence that is specific to the recipient and that can work to identify advanced threat actor-related activities at the earliest point possible so that these organizations can take steps to protect their networks, organizations and personnel before the threat can reach the edge of their environments.

If there are any other details that the judges should know about this project, please note them here. (In 300 words or less.)

We took great pains to understanding the problem first to deliver the right services our customers need. Dell SecureWorks Counter Threat Unit researchers and security consultants looked at the nature of the challenge posed by actors targeting a specific organization and waging a sustained campaign against that target over the last 18-24 months. We heard from numerous customers who expressed concerns, assisted multiple numerous customers during incidents involving advanced threats and have conducted extensive threat research on this challenge. As such, the development of these services was driven by the unique challenge and research into the problem, which culminated into the Targeted Threat Intelligence services portfolio discussed here. Advanced Threats represent a potent threat to organizations versus commodity threats and as a result, organizations need to consider them in a different category. Having said that, there are different types of advanced threat actors and the methods/behaviors they employ vary. This understanding fuels the nature of our service offering to address this variation and provide actionable threat intelligence tailored to the customer's organization and needs.