Operation SMN

Cybersecurity Coalition Interdicted the Axiom Threat Actor Group

By Peter B. LaMontagne, Novetta CEO

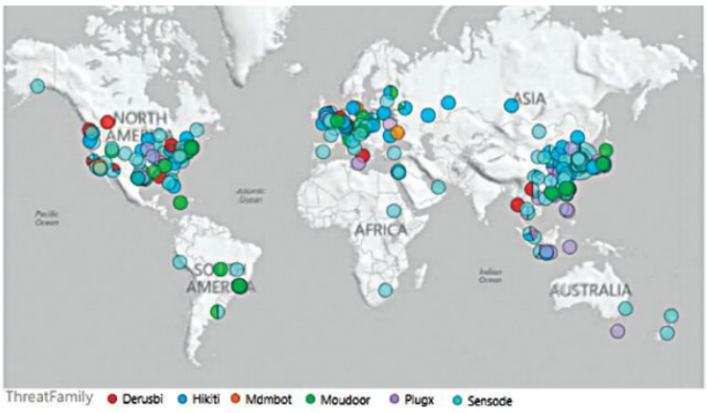
Information sharing has proven essential to the interdiction and mitigation of cyber espionage efforts by advanced threat actor groups. The cybersecurity analytics community needs to improve the processes for collaboration in order to provide better security across the entire ecosystem. Novetta recognized this necessity after the joint discovery of a Chinese-based threat-actor group deemed Axiom and decided to take action.

On October 14, 2014, Novetta announced it was leading a cybersecurity coalition. This coalition included a group of influential security and technology firms including Bit9, Cisco, FireEye, F-Secure, iSIGHT Partners, Microsoft, Tenable, ThreatConnect Intelligence Research Team (TCIRT), ThreatTrack Security, Volexity, and more who agreed to partner to protect their combined customer base.

After months of cooperation, Novetta released a report titled "Operation SMN: Axiom Threat Actor Group Report"[1] on behalf of the group's collective findings. The report details the characteristics of Axiom, operating out of mainland China on behalf of what is believed to be a Chinese government intelligence branch. "Operation SMN: Disruption of 'Axiom,' a Prolific Chinese Cyber Espionage Group,"[2] is available as a webinar.

The main objective of Operation SMN was to proactively mitigate against the Axiom threat actor undetected in order to report and remediate all associated malware exploits associated with their efforts and practice. There is evidence the Axiom group has been operating unfettered as far back as 2009. Unfortunately these acts have been organized under multiple descriptions and names by various security analysts and organizations, all outwardly unconnected. But, through ground-breaking data disclosure, these superficially separate campaigns were confirmed as the actions of a single actor group: Axiom.

Supported by Microsoft's Coordinated Malware Eradication program, the coalition shared and received technical data detailing the removal of malware families used by Axiom. More than 43,000 separate installations of those related tools have been removed from machines protected by Operation SMN partners. So far, 180 of those infections were examples of Hikit, the late-stage persistence and data-exfiltration tool that represents the height of an Axiom victim's operational life cycle.



Hikit and related family detections and infections

Through the tools and technical assistance Novetta provided, the coalition forced Axiom to use different exploits and expend more resources. And by leveraging multiple industry perspectives and technical capabilities, the coalition established a foundation to deliver successful mitigation on future malware threats and actors.

The unified approach of Operation SMN should stand as the industry standard for malware reverse engineering and threat-actor interdiction. Novetta hopes that through the proven success of the coalition's efforts, others within the industry will embrace and adopt a similar approach in the future, leading to less devastating malware intrusions.

Peter B. LaMontagne, Novetta CEO

NOVETTA SOLUTIONS

Novetta Solutions is ISSA's Premiere Patron Sponsor 2014

The Open Forum

The Open Forum is an opportunity for security practitioners to express their opinions, thoughts, and wisdom on security-related topics of their choice. Articles should be 700-800 words and include a short bio and photo. Please submit to editor@issa.org.

1 http://novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf.

2 http://w3.novetta.com/Lead-Lifecycle_Webinar2.html?leadsource=ISSA-Webinar2.