Advanced Programs Group

Reduce the time and costs associated with security incidents

As new threat variants, attacks and actors appear on a daily basis, even sophisticated enterprises have difficulty getting insight into these newly developed techniques and players. The best way to combat the attacks of both today and tomorrow is through actionable threat intelligence, delivered with custom, in-depth incident analysis reporting developed for your specific needs. The Advanced Programs Group (APG) from Intel Security specializes in investigating targeted intrusions performed by the most advanced threat groups. APG uses the intelligence gathered from McAfee® Global Threat Intelligence (McAfee GTI) capabilities, in conjunction with the experience of intelligence professionals, to provide actionable intelligence of developing threats, trends, and vectors.

APG provides intelligence and advanced analysis of:

- Sponsored attacks.
- Advanced persistent threat (APT) groups and actors.
- Social network analysis.
- Insider threats and attacks.

Data and Adversary Focus

APG's focus on multiple sources of data and its analysis is fundamental to its deep understanding of adversaries.

- **Reputation data:** Intel Security's data set with reputations of billions of files, Internet protocol (IP) addresses, and URLs.
- **Open source data:** Billions of data points gathered per day—indicating open ports and services—from open source collection and daily dumps of data from open source collection used in attack correlation and visualization.
- **Social network analysis:** Analysis of social structures through the use of network and graph theories to characterize networked structures in terms of nodes and the ties or edges that connect them.
- **Advanced malware feed:** Daily feeds that are the result of APG's analysis using YARA, focused on advanced persistent threats.
- **Android malware feed:** Intel Security's daily feed of new malicious Google Android malware.
- **Malicious certificate feed:** Intel Security's daily feed of malicious certificate activity, including historical data.

intel Security

APGPivot

APGPivot is a utility and service that lets APG search any IP address, domain name, or organization that has servers facing the internet. It provides banner information for all of these searches. For example, if you're interested in finding computers running particular software such as an Apache HTTP server or Pro FTP server, it will show all servers in the target space with these services running.

APGPivot is also a Big Data aggregator. If you provide data to APGPivot, it will automatically categorize and analyze the data. APGPivot researches the use of machine learning methods, so that when the user asks a question, it can drill down into the data and provide the user with the appropriate collected information to answer to the question.

Services

APG Threat Research

APG maintains awareness of the threats and attacks that have the potential to impact customers. APG leverages its data and adversary focus to delve into key malicious activity. Understanding this activity is a continuous part of the APG mindset, as well as the starting place to answer specific customer queries. Examples of threat research services include:

- Expanded and customized McAfee GTI querying and reporting.
- Focused intelligence reports.
- Attribution and actor analysis and reporting.

APG Threat Response

APG harnesses its knowledge of current and potential threats and attacks to provide threat response capabilities to its customers. Using its data, adversary focus, and continuous research as a foundation, APG helps customers respond and answer important questions about specific threats and attacks. Example of threat response services include:

- Forensics analysis and assistance.
- Response analysis and assistance.
- Mitigation strategies.

Transforming Data into Intelligence

APG uses a set of capabilities built on data and adversary focus to provide threat research and threat response capabilities to its customers.

Malware reverse engineering

Our research shows that approximately 25% of malware has some sort of protection mechanism. The malware employs these protections so that automated tools cannot be used. In these situations, the APG Malware Reversing Team is brought in to help with the answers of who, what, where, and how.

The APG Malware Reverse Engineering service gives you actionable intelligence around a malicious binary faster than other service because of our team's experience and proven history in malware analysis. APG provides a detailed report that enumerates all possible data that can be acted on, along with recommendations for a variety of countermeasures.

Visualizations and dashboards

The APG dashboard integrates multiple sources of data that is presented to the analyst in an intuitive web-based application. The dashboard allows detailed malware analysis through its real-time data feeds. Malware classifications, top hits, and detections show an overall picture of the files that Intel Security is seeing day-to-day. Visualizations display the results from APG's custom YARA scripts that are run on all of the unknown binaries of the day.

Additionally, the APG dashboard allows analysts to do multiple pivots across multiple data sets. For example, an analyst can ask for the top 10 malware hits for any region in the world. From there, they can pivot to a list of files being accessed and IP addresses being contacted by the malware. They can then ask if any other instances of malware are utilizing the same files or contacting the same IP addresses.

Adversarial monitoring and tracking
APG utilizes deep adversarial knowledge and operational experience to enhance incident response and threat analysis activities. Leveraging core competencies garnered from more than 40 years of collective experience with nation-state level groups and organizations, APG provides superior deliverables to exceed customer needs and requirements.

Custom tools development
APG develops custom tools to support all customer capabilities and to answer difficult questions. APGPivot is an example of an APG custom tool that is used in support of threat research and threat response services.

Social network analysis
APG recognizes that threats do not exist in a vacuum, nor are they solely digital in nature. There are humans behind threats, and humans have networks. APG has developed a process that centers on identifying not just the threat, but also the people, processes and technologies that support the threat. APG's tools and services visualize these network and connections, allowing our customers to take practical action through our applied intelligence.

Exercising analytical and operational techniques, APG can establish footprint and selector identifiers specific to particular adversarial groups and organizations. This seamless integration of analysis and proactive operational posturing produces actionable, effective intelligence.

About Intel Security APG

APG is a team of intelligence professionals who provide customized, applied intelligence. This gives APG the unique ability to correlate victim environment information with social and networked entities against one of the largest threat databases in the industry—from Intel Security. By working with the local threat responders, APG combines endpoint and network information with McAfee GTI to identify who the attacker is, what they have done, and what they may have accessed.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com