INFOARMOR®
DETECTION IS THE NEW PREVENTION

InfoArmor ATI Corporate Contact:
Byron Rashed
InfoArmor, Inc.
Advanced Threat Intelligence
+1 480 302 6701 Main
+1 480 302 6467 Direct
brashed@infoarmor.com

INFOARMOR RELEASES ITS VIGILANTEATI℠ ADVANCED THREAT INTELLIGENCE PORTAL

InfoArmor Rebrands and Upgrades Former IntelCrawler and PwnedList Threat Intelligence Services

SCOTTSDALE, Ariz. – October 27, 2015 – InfoArmor, Inc., an industry-leading provider of identity and cyber intelligence services, today announced the general availability of its VigilanteATI℠ cyber threat intelligence platform. VigilanteATI℠ mitigates risk by providing historical, immediate, and preemptive threat intelligence to maintain a high level of vigilance and avoid the debilitating impact of cyberattacks to business and government agencies. VigilanteATI delivers actionable threat intelligence and advanced cyber security that when compared to competitive platforms provides "the totality" of intelligence with time-tested, verified and validated data.

In 2013 and 2015, InfoArmor acquired Austin-based PwnedList and Los Angeles-based IntelCrawler respectively, to form its ATI (Advanced Threat Intelligence) business unit. PwnedList is a searchable database of email addresses and usernames that may have been compromised from data dumps. If the search results are positive, users should take the appropriate steps of changing their passwords and maintain a high level of awareness. IntelCrawler provided threat intelligence data and security research services to large corporate and government clients. Following the acquisitions, InfoArmor has been developing a comprehensive advanced threat intelligence platform and has broadened its security research services to assess a wide range of threat and attack vectors. In addition, InfoArmor leverages this valuable Advanced Threat Intelligence and contextual content within its identity and privacy products and services.

-more-

VigilanteATI delivers context-rich, actionable Advanced Threat Intelligence. Leveraging trusted operative sources, VigilanteATI provides the necessary comprehensive Advanced Threat Intelligence to effectively reveal the "who, what, why, when and how" to defend against past, present and future global cyber threats. VigilanteATI incorporates the following threat intelligence features:

- **Advanced Intelligence** – defining the gold standard of threat intelligence. InfoArmor provides elite intelligence regarding the latest trends, bad actor attribution, and other pertinent information. InfoArmor delivers valuable informational and actionable intelligence to reference or use for educational purposes and security awareness of new threat activity, specific threat actors, or other exploits that may pose a direct or peripheral risk to your organization.
- **Risk Intelligence** – distinctive industry-specific intelligence derived from our underground operative sources that includes compromised:
    - Client Accounts
    - Credit Cards (tokenized)
    - Money Laundering/Money Mules
- **Security Intelligence** – a threat intelligence feed of underground malicious and suspicious host activity to help assist in identifying cyber threat activities. Specific client network ranges can be input to provide a robust automated service that enables real-time alerts and identifies activity from the specific users and devices within your organization which are engaging with malicious threats. These malicious entities are confirmed, validated, and monitored from underground sources using InfoArmor's proprietary advanced threat intelligence practices. Information is systematically updated, and includes the compromised IPs, domains, malware signature, CnC information and other valuable data.
- **eCrime Intelligence** – a comprehensive database of underground communication and bad actor chatter from dark/closed forums that provides real-time updates and monitoring of these forums with relevant information to deliver preemptive intelligence. Client specific keyword lists associated with the

-more-

URL/brand delivers reference to client assets with additional context around specific issues or impending threats.

- **Compromised Credentials** – exposed email addresses and associated passwords linked to malicious breaches and third-party exposure. The service enables a robust search feature for specific credentials, or can include real-time monitoring and notification based on domain or account entries. Specific indicators of compromised credentials are then delivered, along with context surrounding the source of the exposure and any other reference, providing a valuable opportunity to accelerate threat containment and risk mitigation.

“Since the acquisition of IntelCrawler, our focus over the last year has been on developing the next level of threat intelligence that combines a variety of features in one comprehensive platform,” said Christian Lees, CISO of InfoArmor, Inc. “VigilanteATI not only provides actionable threat intelligence data along with context, but also delivers valuable information of past, present and potential cyberattacks to help IT security professionals mitigate risk and safeguard their business-critical data. In addition, as cyberattacks have become extremely complex, placing a huge burden on already taxed IT security resources. To meet this increasing demand and need, we have have expanded our security research and custom services offerings for those customers with specific investigative needs.”

Product Pricing and Availability

VigilanteATI is available immediately, with an API for SIEM integration in mid-2016. To request more information and pricing, please visit the InfoArmor Website at http://infoarmor.com/, or contact InfoArmor sales at +1 480 302 6701, or email sales.ati@infoarmor.com.

About InfoArmor, Inc.

InfoArmor offers industry-leading identity and cyber intelligence services that help our clients fight emerging fraud and advanced cyber threats. We combine an unparalleled global research network with big data analysis, actionable intelligence and customized service to meet clients’ dynamic security needs. From employee to

-more-

enterprise, InfoArmor is redefining how organizations fight fraud and combat an evolving threat landscape to mitigate risk on multiple levels. Today, more than 600 businesses and government agencies, including 50 of the Fortune 500, use PrivacyArmor℠, our employee identity protection solution, or our advanced threat intelligence platform to improve their data security posture. For more information visit http://infoarmor.com.

# # #