Smart, Simple, Scalable. Everywhere.

THREATBLOCKR®

BAMBENEK CONSULTING

Every day, there is another story about another company having their banking accounts drained, someone having their identity stolen, or critical infrastructure being taken offline by hostile entities.

It isn't enough to just install a firewall and hope it protects you. Protecting your network requires the latest threat intelligence on what the attackers are actually doing. Bambenek's Well-Fed Intelligence products are used by thousands of organizations all over the world to better protect themselves from cyber threats.

Benefits

- Better protect your network from sinkhole IPs, Domain Generation Algorithm (DGA) infrastructure, and domains associated with malware.
- Well-Fed Threat Intelligence automatically updated in ThreatBlockr platform ensuring protection is always current.
- Easy and fast deployment via ThreatBlockr Cyber Intelligence Marketplace.

Well-Fed Threat Intelligence

Well-Fed Threat Intelligence is produced by Bambenek Consulting, LTD. Bambenek is a leading cybersecurity threat intelligence and data science firm led by industry veteran John Bambenek.

Well-Fed operates one of the largest repositories of curated threat intelligence that is publicly available. Using novel techniques, Well-Fed threat intelligence is generated by surveilling attackers to see where they actually live so you have the latest information to protect yourself.

Approximately one million malicious domains are monitored every hour and are curated and whitelisted to ensure that you have reliable information you need to protect yourself from cybercriminals. Well-Fed Threat Intelligence is used by thousands of organizations all over the world to protect themselves and their customers.

The Well-Fed Intelligence subscription offering available on the ThreatBlockr Cyber Intelligence Marketplace provides access to three distinct threat feeds including:

- **Sinkhole IP Feed**
  A manually curated list of over 1,500 known sinkholes.
- **DGA Feed**
  A self-curating feed that monitors malicious networks to observe current criminal activity. This is live data of between 750 and 1,500 domains, which are used by 65 malware families and nearly 1 million domains.
- **MaldomainM**
  A feed based on proprietary machine learning and analytical methods of DNS telemetry developed in Bambenek Labs. Provides protection from malware and phishing domains.

Intelligence Collection Approach

We start with known malware and passive DNS telemetry to identify DGA domains, sinkholes, and malware & phishing domains through our analytic and machine-learning layers. The data is restricted to only currently relevant threats and historical or otherwise inactive campaigns are removed. The data is then run through a unique curation layer that has multiple levels of white-listing and curation to avoid false positives. This helps ensure the data is clean, highly-actionable, and optimized for blocking at the perimeter to protect against entire malware families and campaigns.

The threat research team is constantly combing through our data and public reports to identify new malware families, campaigns, and other techniques to identify new or otherwise undetected threats to keep the data relevant and fresh. The system is frequently updated as new techniques are identified or new machine-learning models created to increase the visibility into the threat landscape.

About Bambenek Consulting

Bambenek Consulting, LTD is a boutique cybersecurity threat intelligence firm focused on surveillance of cybercrime. The product was first developed in 2013 to assist in law enforcement investigations to shorten the time between criminals setting up infrastructure and subsequently reporting that to law enforcement for action. Since then, dozens of more malware families were added to tracking and the data was used in security products and to protect organizations all over the world. It has been the basis of hundreds of academic papers in cybersecurity machine learning and to enhance the practice of cybersecurity.

The company is led by John Bambenek who has worked over 22 years in cybersecurity as an investigator that threat intelligence expert. He has spoken all over the world on criminal threats and on data science as it related to cybersecurity. He is currently finishing his PhD these in cybersecurity machine learning and has used his research to enhance the offering to deliver more proactively identifies threats so companies have even stronger protection against malware and phishing. The firm also is active in a variety of pro bono efforts to enhance cybersecurity for the general public, assist victims of cybercrime, and provide investigative support to public defenders.