

Trend Micro

TIPPINGPOINT® THREATDV DOMAIN GENERATION ALGORITHM DEFENSE

The ThreatDV Domain Generation Algorithm (DGA) Defense family of filters is designed to detect domain name system (DNS) requests from malware infected hosts that are attempting to contact their command and control (C&C) hosts using DGAs. These filters are designed to protect against known malware families, as well as suspicious domain names generated by unknown malware families.

THE USE OF DOMAIN GENERATION ALGORITHMS IN MALWARE

Used in a number of malware families, DGAs are designed to randomly generate domain names in order to contact their C&C servers. This is done in an attempt to avoid having to hard-code IP addresses or domain names in the malware which would make them very easy to block. DGAs use a "seed" that the authors or bot herders know, so that they can register one of many thousands of domains queried by the malware when they want to initiate a campaign. For instance, seed values such as "date" and "time" are common. With knowledge of the algorithm, malware authors can predict which domain names the infected machines will attempt to access at a certain date and time, and then register one of them in advance.

DGAs were a relatively unknown technique until 2008, when the Conficker worm affected millions of networks and hosts worldwide. The writers of the malware used domain names instead of IP addresses to avoid detection and mitigation. A machine infected with Conficker could generate a large number of domain names that could be used as rendezvous points with its C&C servers. Any attempts to contain Conficker and identify its C&C hosts were soon countered with variants that increased the number of DGAs and casted a wider distribution across top level domains, which are at the highest level in the DNS. Conficker would ultimately require a worldwide effort to contain it, and it is still active in the wild today.

MALWARE PROTECTION THROUGH GROUNDBREAKING SECURITY RESEARCH

The ThreatDV DGA Defense filter family is the result of years of groundbreaking, patent-pending research conducted by the TippingPoint DV Labs threat intelligence team. Using machine learning techniques across a significant DNS dataset, the team has developed classifiers with over 95 percent accuracy that are able to detect families of DGAs using a combination of syntactical rules and logistic regression. They have also created filters that can catch many types of malware whose domain names cannot be encompassed by a regular expression that would not generate a large number of false positives. The extensive research that the DV Labs team has conducted has led to two defensive publications published at Research Disclosure and numerous speaking engagements at conferences around the world.

Key Benefits

- Detect DNS requests from specific malware families
- Detect suspicious domain names generated by unknown malware families
- Identify active, breached hosts in your network
- Disrupt the attack life cycle by identifying and blocking command and control communication

PROTECT AGAINST DYNAMIC MALWARE WITH THREATDV DGA DEFENSE

The ThreatDV DGA Defense family of filters is designed to detect DNS requests from malware infected hosts that are attempting to contact their C&C hosts using DGAs. These filters are designed to protect against known malware families as well as suspicious domain names generated by unknown malware families.

The Threat DGA Defense filters can:

- Detect DNS requests from specific malware families
- Detect suspicious domain names generated by unknown malware families
- Identify active, breached hosts in your network
- Disrupt the attack lifecycle by identifying and blocking C&C communication

DISRUPT MALWARE ACTIVITY WITH THREAT DIGITAL VACCINE (THREATDV)

ThreatDV is a premium subscription service that can be used with TippingPoint solutions, including the Threat Protection System (TPS) and Next-Generation Intrusion Prevention System (IPS), and managed through the TippingPoint Security Management System (SMS). ThreatDV includes a reputation feed that allows organizations to monitor and block inbound and outbound communications with known malicious and undesirable IP addresses and domain names. In addition to the DGA Defense filters, ThreatDV also includes malware filters that detect post-infection traffic including bot activity, phone home, C&C, data exfiltration, and mobile threats. All TippingPoint customers who subscribe to the ThreatDV service automatically have access to the DGA Defense filters.



Securing Your Journey to the Cloud

©2016 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, OfficeScan, TippingPoint and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. (DS01_ThreatDV_DGA_160606US)