DATA SHEET

Foundstone Targeted Malware Threat Assessment 360

Let's go hunting for unknown malware in your environment

Get visibility into unknown and hidden threats to your business. Foundstone® Services offers the Foundstone Targeted Malware Threat Assessment 360, so that your security organization can discover and respond to advanced threats in a way that goes beyond your current security monitoring tools.

Advanced persistent threats (APTs) can inflict serious harm to a customer's business. These sophisticated, covert attacks focus on stealing valuable data from targeted and unsuspecting companies. Intrusions typically target users within organizations to gain access to trade secrets, intellectual property, state and military secrets, computer source code, and any other valuable information that's available.

The Foundstone Targeted Malware Threat Assessment focuses on discovering threats and infections, aimed towards computer systems in a business environment. The assessment leverages captures of network traffic to identify relevant risks and validates them with information collected from endpoints to produce actionable and credible threat impact to your business. Our unique ability to collect from endpoints leverages a robust infrastructure of intelligence from McAfee® Labs.

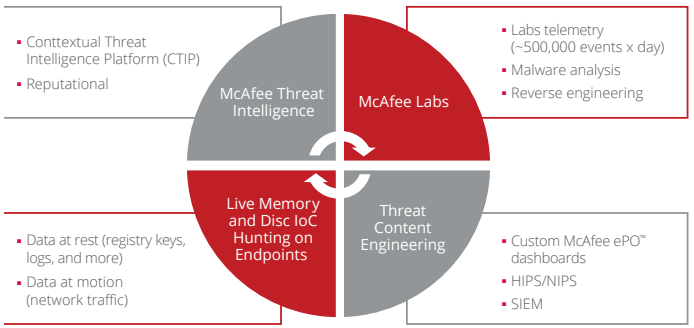

Figure 1. Foundstone Targeted Malware Threat Assessment 360.

McAfee Labs

Whether your business is global or regional, the Foundstone Services team leverages our wealth of intelligence from our commercial and consumer malware monitoring experience of more than 500,000 malware events per day. This malware zoo gives us a unique perspective of the threats and variances of malware inside organizations, verticals, and regions.

Benefits

- Early threat detection and situational awareness
- Provides a 360° view of active threats in any organization's network
- Leverages the power of the McAfee Labs cloud to provide telemetry and IoCs
- Provides meaningful, contextual intelligence from our Contextual Threat Intelligence Platform architecture
- Includes techniques used in Threat Content Engineering (McAfee ePO dashboards, and more)
- Leverages McAfee Active Response where McAfee ePO software is present and requirements are met

Threat Intelligence

Our Open Source Contextual Threat Intelligence Platform has over a decade of data to give our forensic analysts and incident responders the ability to conduct exhaustive online presence reporting. This can result in the identification of the responsible cybercriminals and provide context to the indicators of attack (IoAs) that may exist in your environment.

Indicators of Compromise Hunting

By using our unique set of indicators of compromise (IoCs), from a network perspective, to the active response and investigation of the workstations, we can take an indicator and mature its value with validation of possible malware impacting your systems. As a result, finding unknown malware may increase your observations of the good and bad of your network and give you an overall healthier outlook to your security posture.

Threat Content Engineering

The Foundstone Services team leverages several decades of data and experience using our own tools like McAfee® ePolicy Orchestrator® (McAfee ePO™) software and McAfee Enterprise Security Manager—our security information and event management (SIEM) solution—for network monitoring. This gives our advanced security analysts the ability to architect threat visibility from your systems. Our unique understanding of your security ecosystem allows us to equip your security program with predictive security management metrics that help you find anomalies and report your success in protecting your environment.

Approach

Strategically placed sensors and probes provide real-time information about the emergence and propagation of both malware and vulnerabilities. Through automated analysis of collected samples, we provide the unique ability to intelligently assess the potential impact to your organization. Additionally, the real-time tracking of domains and networks where threats are launched and hosted provides insight to predictive telemetry for emerging threat detection. Combining these items with human intellectual analysis of the real threats and risks experienced in your organization drives your efforts to streamline prioritization and effectiveness of your security program. Analysts correlate the information from the network to the endpoint and determine likely candidates of advanced threats in your network.

We start by setting up a network monitoring system with a customized set of threat feeds and alert feeds. This is matched against the behavior of your endpoints with our custom cyber intelligence content. The combination gives us the ability to pinpoint active threats within your environment to empower your incident response operations.

During initial setup, you provide the following information to our consultants:

- Relevant high-level network design to determine sensor placement, if adding sensors is not available
- Relevant endpoint distribution mechanisms and malware removal tools
- Relevant SIEM and active response tools, if available

Related Services

We offer many related services and training classes including:

- Open Source Intelligence Investigations
- DDoS Defense Assessments
- IR Program Development
- IR Policy and Procedure Definition Review
- IR GAP Analysis
- Investigative Services
- Digital Forensics
- Emergency Incident Response
- Advanced Malware Analysis
- Expert Testimony
- Malware Forensics and Incident Response (MFIRE) Class
- Contextual Threat Intelligence Services

Full access

Our solutions ship with sensors to integrate a network collection strategy focused on analyzing and contextualizing live traffic traversing the local area network (LAN) and exit routes to the internet. This is the recommended setup to optimize "live" traffic analysis, better correlation, and faster reaction to any threats detected in the customer network.

Limited access

The customer sets up the network probes and collects the network traffic using their own hardware. Traffic captures are collected during different periods of time and are shared with Foundstone consultants for offline analysis. We ship and set up a second server that will sit in the LAN and is used to hunt for IoCs, perform triage, and collect and analyze artifacts of interest. This setup is intended for environments where we cannot deploy our own network probes, yet it's possible to deploy a server in the LAN.

Restricted access

The customer doesn't allow Foundstone to deploy any system in their network. The customer sets up the network probes and captures the traffic using their own hardware. Traffic captures are collected during different periods of time and are shared with Foundstone consultants for offline analysis. We share some tools and scripts with the customer to run in their environment to do a restricted hunt for IoCs, perform triage, and collect artifacts.

Benefits

- Improved situational awareness of emerging malware threats
- Improved detection of anomalous events that involve domains, address space, or malware hashes
- Increased assurance that undesirable activity goes unnoticed
- Predictive telemetry that could indicate the intent of an attack before it happens
- Trend identification to help prepare for possible attacks

The Foundstone Difference

All Foundstone projects are managed using our proven Security Engagement Process (SEP) for project management. A pivotal aspect of this process is continual communication with your organization to ensure the success of your consulting engagements.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the McAfee global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost effectively prepare for security emergencies. Speak with your technology advisor about integrating our services or email us at **consulting@foundstone.com**. You can get more information at **www.foundstone.com**.

Foundstone Targeted Malware Threat Assessment 360	Restricted	Limited	Full Access
Live Network Analysis (based on provided information)			■
Static Network Analysis	■	■	
Network Threats Report	■	■	■
McAfee ePO Threats Dashboard (if available)		■	■
Endpoint Threat Report	■	■	■
Advanced Threat Assessment		■	■
Continuous Monitoring Dashboards for SIEM (based on provided information)	■	■	■
Remote Malware Analysis	■	■	■

McAfee
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

62203ds_tmta-360_1215
DECEMBER 2015