GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Fidelis Cybersecurity Solutions, Inc.
1601 Trapelo Road
Suite 270
Waltham, MA 02451

Fidelis XPS™ Power Tools

Fidelis XPS Vector - Expect more from Malware Protection

June 2013

Introduction

Modern enterprises are persistently being targeted by their adversaries, whose objectives range from financial gain to achieving strategic superiority through the theft of data or key intellectual property, outright destruction and interruption of business processes, or simply establishing a beachhead to be exploited when circumstances require. The delivery of malware to end-users within the enterprise is now a key method by which this objective is achieved. Traditional computer defenses, both network and endpoint-based, are proving to be incapable of countering this threat.

Fidelis XPS™ Vector gives enterprises protection against exploits and malware, both common and targeted and does so with minimal configuration and operation required. When installed, security teams can use its reports and analysis to block certain malware and to quickly remediate compromised hosts and deny threat actors the ability to further compromise the enterprise.

Threat Overview

Enterprises are being persistently attacked by advanced threat actors who often use the network for achieving their goals. These threat actors typically use exploits and malware that evade the traditional elements of the network security stack such as firewalls and IPS by using rich encoding methods and obfuscation. These are also designed to evade detection by endpoint security tools such as Anti-Virus technologies through techniques such as polymorphism, which makes the use of static signatures ineffective.

The threat actors deliver their exploits and malware through a variety of protocols such as web (HTTP) and email (SMTP, IMAP, POP), as well as applications like instant messaging and file sharing (bittorrent). In addition, malware authors may use undefined protocols to send malware across the network ingress point. A network security solution needs to be intelligent enough to recognize this unusual protocol structure and inspect the contents of the transmission for malicious intent. As a result, controls over a single part of the network infrastructure, such as application-specific gateways for SMTP or HTTP, are no longer sufficient.

Other network-based technologies that make assumptions about the software applications and their versions running in the enterprise are susceptible to missing malware designed for other software that is operating in large enterprises, which typically have considerable diversity in the

use of such software. A combination of these factors results in most enterprises remaining vulnerable to exploits and malware being used against them. These techniques are a critical method for the compromise of enterprises, resulting in severe impact to their objectives.

The infrastructure for hosting and delivery of these exploits and malware is vast and rapidly changing, so reliance on locations of known bad sites, often termed 'threat-intelligence' is also insufficient by itself. Technologies for detecting these attacks can be expensive to acquire in the context of enterprise security budgets; as well as expensive to operate when they require multiple skilled analysts to configure systems and interpret results.

Fidelis XPS Vector

General Dynamics Fidelis Cybersecurity Solutions has developed a cost effective, easy to deploy and easy to use solution targeted at protecting enterprises against exploits and malware that doesn't require a team of skilled analysts to get actionable results and protect enterprises against malware delivered across a variety of network protocols. Fidelis XPS Vector family consists of three products: Fidelis XPS Vector 250, Fidelis XPS Vector 500, and Fidelis XPS Vector 1000; rated for networks with 250Mbps, 500Mbps, and 1000Mbps in monitored traffic respectively. This simple deployment architecture is shown in Figure 1 below.

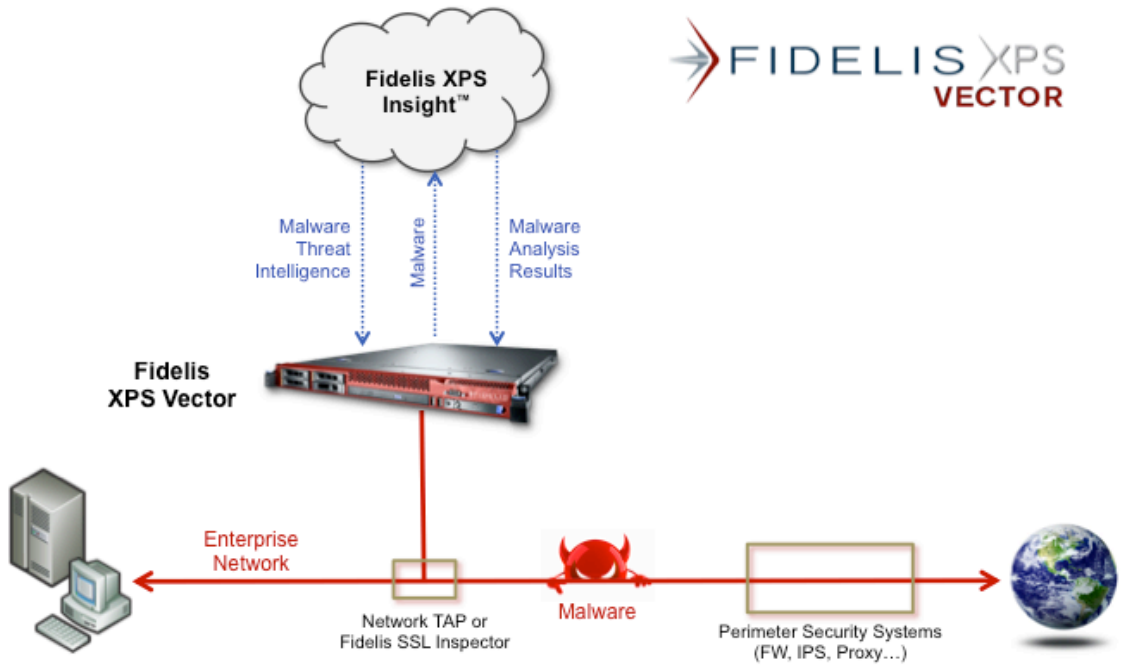

Figure 1

Each of the products is an integrated management console and network sensor and is offered in a 1U appliance. Once the product is licensed and installed on the network, it automatically starts detecting exploits and malware with no further configuration or tuning required. Thus, security analysts can simply focus on remediation activity for events detected by the Fidelis XPS Vector.

When two or more Fidelis XPS Vectors are deployed on a network, it is possible for one of them to be designated as the single management console. When this is done, it continues to operate as a network sensor but also as the management console for all the Fidelis XPS Vectors attached to it. In this way, the analyst have a 'single pane of glass' for viewing and reporting on malware detected by all the systems.

Fidelis XPS Vector uses Fidelis' patented Deep Session Inspection® technology to extract content such as executable files, MS-Office files, PDFs, Java applets, and various kinds of scripts for analysis. This content will be extracted from all Internet protocols such as HTTP, SMTP, FTP etc, regardless of whether it's on an IPv4 or IPv6 network or uses a tunneling protocol. The content can be compressed, encoded, or obfuscated in any number of ways and it will be extracted for analysis.

To conduct malware analysis, the Fidelis XPS Vector uses a number of methods, such as the application of threat intelligence, static signatures, as well as emulator-based execution for executable files and script objects. In addition, all content deemed malicious is then executed in a virtual execution environment for the inclusion of execution forensics. The determination of maliciousness occurs in the appliance. The execution forensic report creation is through a cloud-based service. This feature is part of the maintenance and requires no additional purchase. This allows Fidelis XPS Vector to provide near real-time detection of malicious objects, so analysts do not need to wait minutes or hours for an alert to populate in the system.

Detection methods are continuously being updated through the use of Fidelis Insight Threat Intelligence Feeds. This feature is part of the maintenance and requires no additional purchase.

The user-interface provides a rich set of prebuilt reports that allow the operator to quickly view alerts in a variety of ways, such as sorted by receiving host, country of origin, protocol and filetype. The user can create custom reports, representing the data present in a way that is most useful to their environment. The data, as well as the reports, can be exported in a variety of formats, such as syslog, email, or to a SEIM.

For customers who have other Fidelis XPS products deployed on their network, it's possible to manage Fidelis XPS Vector from the primary management system – Fidelis XPS CommandPost. In this way, a Fidelis XPS Vector appliance can be integrated into a larger deployment involving multiple types of Fidelis XPS products.

Key Malware Detection and Prevention Capabilities

Fidelis XPS Vector leverages Fidelis' patented Deep Session Inspection® technology to identify malware and malware-associated communication (such as command and control communication) using both session-oriented and object-oriented malware detection techniques.

The Deep Session Inspection engine enables Fidelis XPS Vector to detect malware-based threats by:

- consuming dynamic threat intelligence and threat detection rules from the Fidelis Insight threat intelligence cloud
- reassembling, decoding and analyzing network protocols, applications and content objects
- identifying certain forms of malware and malware-associated communication in real-time by doing rules-based logic on the results of the deep session analysis
- extracting content objects (including deeply embedded and/or obfuscated content objects) from the network traffic stream and passing them to a multi-stage malware detection and analysis stack that uses a combination of static analysis, emulation and virtual execution to identify and analyze malware objects

When Fidelis XPS Vector sees a network session that contains malware or malware-associated communication, it takes an action on that session. If the threat is one that can be detected by the real-time, session-oriented threat detection logic (such as previously observed malware or command-and-control communication behavior), then the action may be an alerting action or a blocking (prevention) action. If the threat is one that can only be detected by the object-oriented malware detection engine (such as an unknown malware object), then Fidelis XPS Vector can only take an alerting action on the session the first time it sees the threat. However, there is a feedback mechanism from the malware detection stack to the Deep Session Inspection engine that enables Fidelis XPS Vector to take a blocking action on the session the next time it sees the threat.

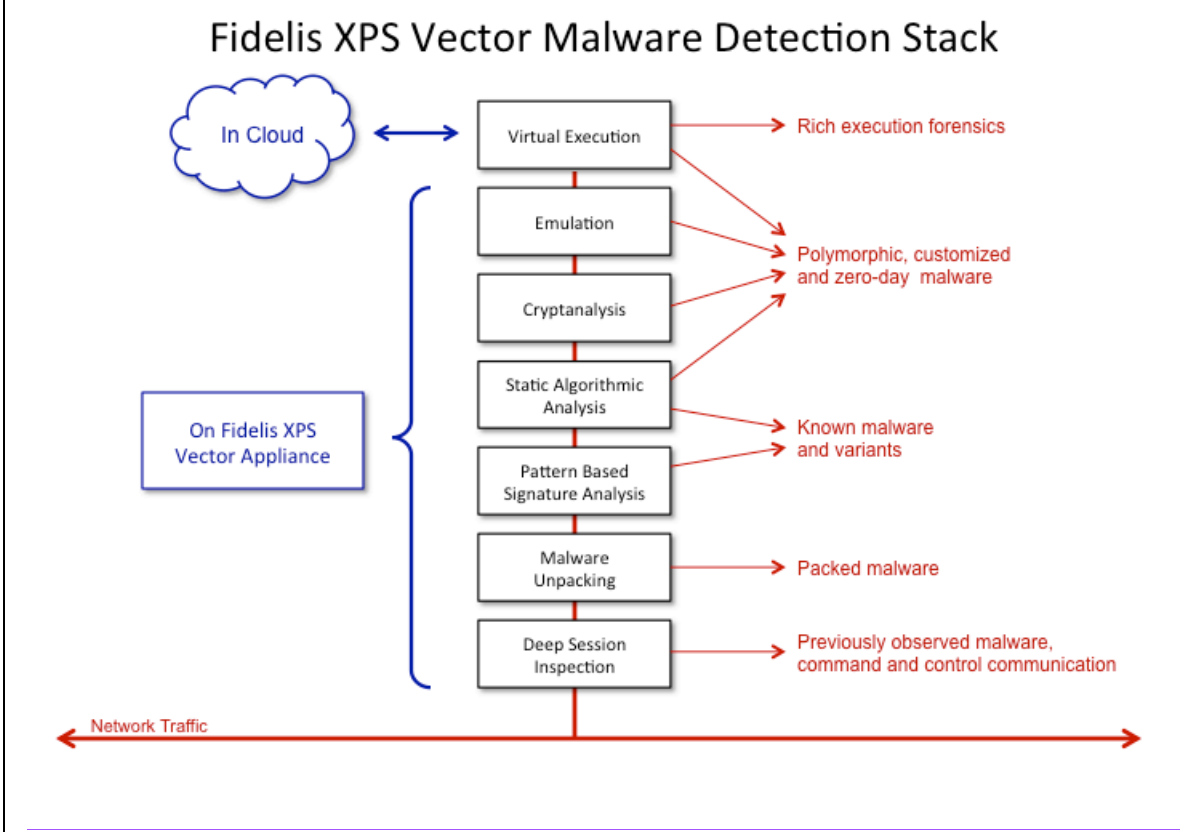

Figure 2

Once an object has been extracted from a network stream, it is subjected to a series of analysis stages that do static analysis, such as detection of packing tools used and corresponding unpacking of malware. Further, pattern based signature analysis is applied, followed by algorithmic analysis and cryptanalysis, providing information on encryption methods that may have been used.

Following this, executable and browser-based scripting objects are subjected to emulation analysis.

In cases where these stages yield a positive malware detection, the object is then submitted to a virtual execution analysis stage that is conducted in a secure, cloud-based environment. In this stage, objects are executed in a full operating environment, with typical enterprise operating systems and applications chosen. The results of this stage are rich execution forensics that are included in alert details viewable in the Fidelis XPS Vector console.

The process described in the preceding paragraphs is referred to as the Fidelis Malware Detection Stack and is shown in Figure 2 above.

In certain cases, objects that are determined to be highly suspicious but not positively identified as malware are submitted to the cloud-based execution analysis stage.

All submissions to the cloud-based service are private and not shared with other organizations. Enterprises can choose the types of objects that are automatically submitted for cloud-based analysis. Where appropriate, the enterprise administrator can disable all automatic submissions and make manual determinations of which objects need be submitted for such analysis.

Fidelis XPS Vector uses proprietary methods to achieve blocking of sessions containing malware and associated command-and-control. When enabled, prevention of such malicious sessions can be achieved through packet-drops or through the generation of TCP Resets to the endpoints of the session, forcing the connection to close.

Benefits

Fidelis XPS Vector is designed to provide maximum malware protection with the least possible configuration and operational inputs required. Coupled with the rich details available in alert reports, this results in considerable benefits to the enterprise customer. The key benefits of the product are highlighted below.

Features	Benefits
Multi-stage detection engine with strong static *and* dynamic malware detection and analysis components	High Detection Rate, Lower Risk
High speed on-box detection engine can analyze hundreds of extracted objects per second	High Detection Rate, Lower Risk
Strong network *and* execution based forensics	Fast Incident Response, Low TCO
Integrated management system and sensor on single appliance	Low TCO

Customer Use-Case

A large manufacturer of marine vehicles based in the Unite States was among the first to use Fidelis XPS Vector. Their business depends heavily on the security of their operation, in terms of safeguarding key intellectual property such as designs, as well as manufacturing processes. Their operations are tightly integrated with a large base of suppliers and the personnel base includes a large number of contractors. They are aware of the need to protect their enterprise against targeted attacks and also of the fact that they've been subject to reconnaissance by various threat actors over the years.

The company's enterprise security staff is highly mature but operate with the usual set of budgetary constraints that affect modern enterprises. Their network security stacks do include next-generation firewalls and filtering web proxies but compromised systems are discovered

from time to time, indicating that certain threats are slipping through their defenses. They evaluated the anti-malware options provided with their next-generation firewalls, but realized that it provided little by way of forensics, operated on a very limited set of malicious objects and consequently were not satisfied with the continuing gaps in their security posture.

They deployed Fidelis XPS Vector 250 in monitoring mode on their network and fed it traffic from both their Internet access points, thus achieving enterprise-wide coverage with a single product. Within 30 minutes of racking and powering on the system, they had it configured to achieve maximum protection, exporting event information to their SIEM for correlation with other event information as well as emailing the security team for all detected events that were deemed critical.

After a few days of operation, they detected a set of exploits that were delivered to users through a waterholing attack on a trade association website. Through an examination of the detailed execution forensics provided in the alert and use of their endpoint forensics tools, they determined quickly that their user systems hadn't been compromised. However, they notified the trade association of the exploits on their website so that they could take appropriate remediation actions.

In the subsequent month, a recently compiled Trojan malware was detected as having been delivered to one of their users by email. The obfuscation used in packaging the executable resulted on their email protection stack missing the malware but Fidelis XPS Vector detected it immediately and corrective action was taken before any real damage was inflicted.

After 6 weeks in operation, the Fidelis XPS Vector appliance became an integral part of the security stack in their enterprise. In the future, they intend to consider an upgrade to the Fidelis XPS Direct solution to achieve broader visibility and control in their environment.

Conclusion

The modern enterprise needs to remain vigilant against threat actors who utilize malware to infiltrate and compromise networks. Fidelis XPS Vector gives enterprises protection against exploits and malware, both common and targeted and does so with minimal configuration and operation required. When installed, security analysts can use its findings and analysis to quickly remediate compromised hosts and deny threat actors the ability to further compromise the enterprise. It is simple to use and easy to deploy and comes with a rich set of enterprise features. It also offers an upgrade path to the broader visibility provided by the complete Fidelis XPS solution, which customers can leverage after they have achieved control over malware targeting their enterprise. Fidelis XPS Vector is an essential component of the enterprise network security stack.

About General Dynamics Fidelis Cybersecurity Solutions

General Dynamics Fidelis Cybersecurity Solutions provides organizations with a robust, comprehensive portfolio of products, services, and expertise to combat today's sophisticated advanced threats and prevent data breaches. Our commercial enterprise and government customers around the globe can face advanced threats with confidence through use of our Network Defense and Forensics Services, delivered by an elite team of security professionals with decades of hands-on experience, and our award-winning Fidelis XPS™ Advanced Threat Defense Products, which provide visibility and control over the entire threat life cycle. To learn more, visit www.fidelissecurity.com.