A New Approach to Assessing Advanced Threat Solutions

December 4, 2014

DELTATESTING

A New Approach to Assessing Advanced Threat Solutions

How Well Does Your Advanced Threat Solution Work?

The cyber threats facing enterprises today are sophisticated, wide ranging, and highly targeted. They combine never-before-seen exploits, stealth, and perseverance. The security industry has attempted to respond to these threats with better, non-signature-based anti-malware technologies. But how do you know if you're really protected from today's threats? Only a methodology based on using realistic and authentic threats can answer this question. With this in mind, Delta Testing recently put a number of vendor products to the test.

EVOLUTION OF TODAY'S THREATS

Advanced malware is a huge problem for signature-based anti-malware systems as, of course, unknown malware brings with it no signature. Yet increasingly, criminal attackers are capitalizing on vulnerabilities and illegally acquired enterprise data to inject sophisticated malware in targeted attacks. The latest research shows that these types of attacks are multiplying. According to IBM figures published in April 2014, there were 1.5 million cyber attacks in the United States in 2013, with manufacturing and finance the top two targeted industries.[1]

This year has seen some of the biggest and costliest cyber attacks in history. Executives at JPMorgan Chase had to face up to the breach of 76 million account details.[2] And in the UK, the *Financial Times* reported that, if cyber offences and credit card fraud were included in official data, the total number of crimes in England and Wales would be more than 40 percent higher.[3]

Cybercrime has reached historic levels of penetration across the globe and the primary challenge to the vendor community is to respond with new solutions, as traditional tools such as antivirus and firewalls are losing effectiveness against advanced threats.

The challenge, then, for the security buyer - these days part of a team facing pressure on all sides to keep the business safe, reduce costs, and meet compliance demands - is to be in possession of data-led evidence of the technical efficacy of their security products.

[1] http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html

[2] http://dealbook.nytimes.com//2014/10/02/jpmorgan-discovers-further-cyber-security-issues/

[3] http://www.ft.com/cms/s/0/3d9d6f24-5524-11e4-89e8-00144feab7de.html?siteedition=uk#axzz3GPoKKW9m

DELTA TESTING METHODOLOGY

Here at Delta Testing, we believe that as attacks have evolved, so must the method for evaluating the effectiveness of products claiming to protect from these attacks. Delta Testing tries to replicate the attacks organizations actually see to the best of its ability. To this extent, we use real malware samples seen in production environments obtained by our incident response partners as well as from researchers in government agencies and universities.

Since our focus is on testing for advanced threats, Delta Testing does not rely on legacy malware, such as common viruses or worms, or known malware repositories for its malware samples. Repositories like VirusTotal are useful for security analysts doing malware analysis and research.[4] However, they do not represent a realistic test of security technologies, especially those focused on advanced malware. Repositories such as these essentially represent collections of "known" malware and as such, every major security vendor monitors them and updates their signature database for new submissions.

Our approach is designed not to trigger an alert based exclusively on a signature or hash match but to allow appliances to detect attacks through advanced emulation or virtualization features (sandboxes). After all, in a real targeted attack, attackers often use never-before-seen malware, which has a very good chance of slipping past signature-based technologies.

Attackers could also obfuscate malware or encode it using techniques like XOR. Detection of these kinds of threats therefore may require understanding the entire sequence of events, since the decoding might happen separately and with knowledge not available during the initial malware download. In fact, in our experience, detecting the malware is often contingent on the detection technologies' ability to first process and detect for the malicious HTML or JavaScript that kick-starts the process. And as you would expect, that is an entirely different challenge due to the volume and complexity involved – JavaScript and HTML are far more prevalent on the Internet than discrete file-based objects. So this can really put a security technology to the test.

All in all, the goal of our methodology is to use techniques that advanced malware authors use to evade detection and hide their tracks. It is our belief this is the difference between advanced malware and more common nuisance threats like adware and spyware. This is what makes advanced malware more dangerous and potent. Therefore, technologies that claim to be designed to combat today's advanced threats should be tested against these techniques and complexities.

As an important note, Delta Testing will also not reuse samples from preceding tests in any of our future tests. While this is more effort on our part as a testing organization, we believe this is the only way to test true unknown malware protection capabilities as well as keep a level playing field (as vendors in this test would now have seen the samples and can create a signature for the malware by the next testing round).

As a final comment on our methodology, a "one-off" test is often not enough to tell the entire story. Real attackers are persistent, work in phases, and change their tactics when one approach fails. In fact, Lockheed Martin has likened the cybercrime process to a military kill chain with several discrete phases.[5] At Delta Testing, we have developed a series of tests designed to focus on different aspects of protection from advanced attacks based on this kill chain process. In this report, we focus on the overall ability of a security appliance to detect the signs of an advanced attack.

[4] www.virustotal.com

[5] http://www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

PRODUCTS AND VENDORS

Delta Testing recently tested some of the leading vendors in the advanced threat protection market using our methodology. All vendors tested are key players in the security industry with a focus on advanced malware detection and protection. Appliances tested were from AhnLab, Check Point, Fidelis Cybersecurity Solutions, FireEye, McAfee, Trend Micro, and Vendor A. (Vendor A has requested that pursuant to their license agreements, Delta Testing exclude their name and product details from this report so that they remain anonymous.)

All appliances were updated with the latest published software version before testing commenced. Appliance details are as follows.

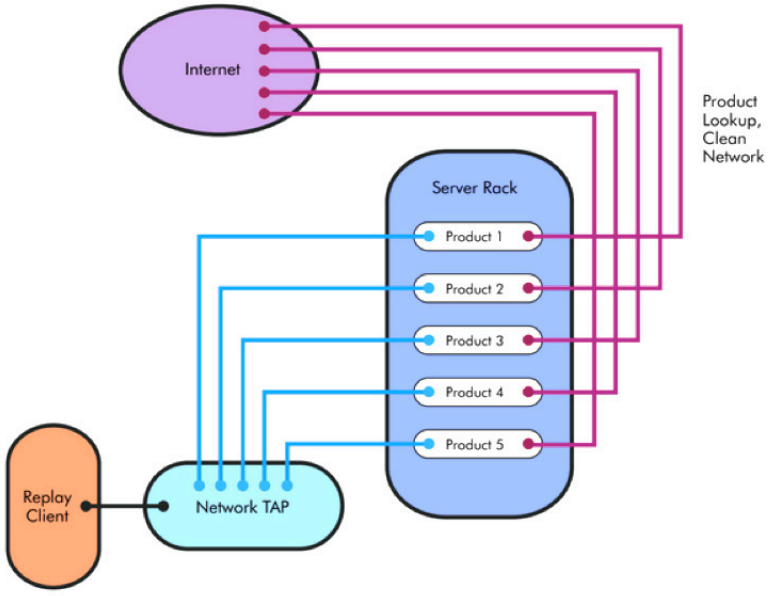
Vendor	Appliance(s)	Version(s)
AhnLab	MDS 2000	Version 2.1.2.27(Build 75r)
Check Point	2200 Appliance 4600 Appliance	Version R77 Version R77
Fidelis Cybersecurity Solutions	XPS Edge 200 XPS Sensor XPS CommandPost	Version: 7.6.5 Version: 7.6.5 Version: 7.6.5
FireEye	NX 7500	Version 7.4.0
McAfee	Advanced Threat Defense Network Security Platform	Version 3.0.2.36.34869 Version 8.0.5.9
Trend Micro	Deep Discovery Advisor Deep Discovery Inspector	Version 2.95.0.1104 Version 3.5
Vendor A	Vendor A Appliance with Cloud-based Sandbox	Version 6.0.0

All products were connected using a VSS vBroker 220 Network Tap.

In this particular test, the sole objective was to determine the detection rate of security products against advanced threats.

TEST CONDITIONS AND SET-UP

In this first round of testing, packet captures, stripped of customer data and obtained from Delta Testing's incident response partners, were replayed through advanced malware protection products from various vendors. The network diagram below shows the lab setup for this test.



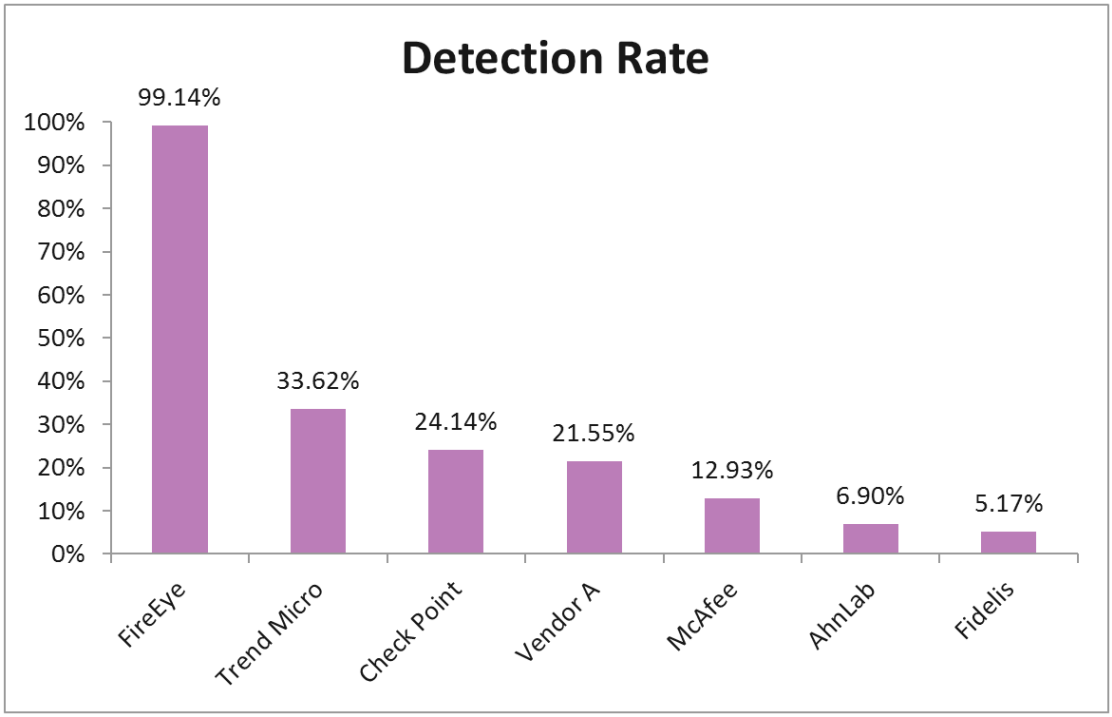
Once the replay was complete, all security products were allowed time for analysis of packets in their on-appliance or cloud-based virtual environments (sandboxes).

After analysis was complete, each product's interface was checked to see if an alert had been triggered to determine detection. Detection rates were calculated as a percentage by dividing the number of detections against the total number of malicious samples sent.

In some case, there was a chance for the products to produce multiple alerts per sample (for instance, if the appliance showed a separate alert for each malicious item within a single attack). However, for this test, detection was defined as any single alert associated with one replay. For example, if an appliance showed three alerts for one replay, this was marked as "detected" for that capture.

During this test, there were no attempts to test the products with additional network loads or with traffic that might cause the product to produce a false positive; all packet captures were malicious samples. Analysis time was also not limited in this round of testing for any of the security products.

RESULTS



ANALYSIS AND RECOMMENDATIONS

Detection rates varied widely based on our results from a high of 99.14% for FireEye to a low of 5.17% for Fidelis. The products included in this test were all globally known vendors. If we had conducted a more conventional test with known malware samples, we believe that all of them would likely score better and probably more equally.

Our current working theory is that most mainstream vendors are on par when it comes to detection of previously known attacks. However, as soon as you move more towards a methodology which uses previously unknown malware, detection rates start to show significant variations based on the technology and detection methodology used by the vendor. This has, needless to say, significant implications for the security industry. In this test, we were able to replicate as much as possible an advanced attack on an organization in a lab environment with real samples. We were then able to analyse which of the vendors under test could continue to detect as much as possible.

While we are only reporting on the raw figures here, in this particular test, the results imply shortcomings in the technology solutions especially when subjected to as realistic a test as we described above. Perhaps it also indicates gaps in existing testing methodologies that leverage the same principles used for traditional solutions (e.g. IPS, anti-virus, etc.) and applying those same methods to advanced threat detection systems.

The results also lead us to draw another conclusion. In our testing, there was only one sample that was missed by all vendors – which is good. However, no product caught all samples either. This implies that an organization cannot rely simply on detection technology alone. Malware has evolved too far for that. In order for an organization to provide "360 degree security," remediation and incident response processes must be best in class as some attacks will get through no matter what. Organizations that are not prepared for that eventuality will pay a heavy price.

With the growing number of threats and mainstream media interest in high-profile breaches, enterprises need to make security an integral part of the business with greater emphasis on threat prevention through awareness for example. Many APT threat actors gain access to enterprises through phishing or other surreptitious means, so education for employees is also important.

Enterprises should make informed decisions on their security purchases and know where the technology they invest in stands in terms of stopping actual advanced attacks. We believe that our methodologies will help them do just that. As stated earlier, a single test is not enough to convey a holistic picture of what is happening; look for additional tests and reports from Delta Testing coming soon.

The aim of Delta Testing is simple:

To create the best possible evaluation process of security products against advanced targeted attacks.

DELTA TESTING DISCLAIMERS

FireEye sponsored the execution of this test and chose the vendors selected. Other than this, FireEye was not involved in the test sample creation, configuration, testing, or analysis. Delta Testing carried out all tests in its facilities; all tests were conducted and analysed by Delta Testing employees.

Test results published in any of Delta Testing's reports represent only a snapshot of an appliance's ability within one particular test case. Delta Testing makes no claims or guarantees for effectiveness of any product for any specific purpose, and this report is not meant to be an endorsement for any product tested. Prospective purchasers should use their own judgment to determine whether said products will meet their individual requirements.

Delta Testing made every effort to contact each of the vendors in the test to inform them of aspects of the testing.

Delta Testing specializes in security testing methodologies and research and is committed to creating the industry's finest test systems to combat advanced attacks. Private and custom tests are available upon request. Please contact us at info@deltatestingltd.com or visit us online at http://www.deltatestingltd.com.