Barracuda Advanced Threat Detection

Bringing a New Layer of Security for Email

White Paper

Evolving Needs for Protection Against Advanced Threats

IT security threats are constantly evolving and improving, especially as attackers compete to create new ways to exploit and discover new vulnerabilities. For this reason, it simply isn't enough to depend on a single strategy or technology layer to protect your networks, data, and users. Instead, a security solution that will remain relevant and effective over time must be built on an agile, versatile platform that evolves and incorporates new scanning technology, modules, and strategies designed to detect the rapidly evolving threats.

Barracuda has built simple and easy-to-use email security solutions that protect our customers from new and emerging threats, without having to manage the complexities of multiple products and solutions.

Barracuda Advanced Threat Detection

Continuing to execute on this strategy, Barracuda provides an Advanced Threat Detection (ATD) layer to its security platforms. This service combines a variety of microservices to create a multilayered scanning strategy that efficiently filters both known and unknown threats. Barracuda ATD complements the native security infrastructure of network, email, and web environments with additional layers of sophisticated detection. It scans for malware, zero-hour exploits, and targeted attacks by screening and analyzing files in a secure cloud-based sandbox environment, to deliver security that is second to none.

The Barracuda ATD service uses three distinct layers to scan, identify, and take action on threats:

Layer 1 - Multi-opinioned anti-virus engine

- Powerful open source virus definitions. Barracuda Networks leverages the open source community to help monitor and block the latest virus threats.
- Real-Time Protection to immediately block the latest virus, spyware and other malware attacks as they emerge with virus and spam propagation activity reports at an early stage.
- Proprietary virus definitions. Barracuda Networks proprietary virus definitions are gathered and maintained by Barracuda Central, an advanced 24/7 security operations center that works to continuously monitor and block the latest Internet threats.

Layer 2 - Static Analysis

- Powerful machine learning farm, via high volume and highly diverse global threat data.
- Leverages Vector Machine algorithm to deliver fast and accurate verdicts.
- Taught with 50 million+ endpoints in the field ingesting good and bad files plus millions of files everyday via email security workloads.

Layer 3 - Dynamic Analysis

- Analyzes inbound email attachments in a separate, secured cloud environment, detecting new threats and determining whether to block such messages.
- Full-system emulated sandbox for remote analysis and detonation of advanced threats designed to evade detection.
- Analyzes attachments and files for advanced malware, zero-hour exploits, and targeted attacks not detected by Layers 1 or 2.

Threat Intelligence with 100% Coverage

Barracuda Advanced Threat Detection combines behavioral, heuristic, and sandboxing technologies to protect against zero-hour and targeted attacks. ATD automatically scans email attachments in real time, and suspicious attachments are executed in a secure sandbox environment to observe behavior. In addition to blocking malicious attachments, ATD integrates new findings into Barracuda's real-time threat intelligence system, extending protection to all customers.

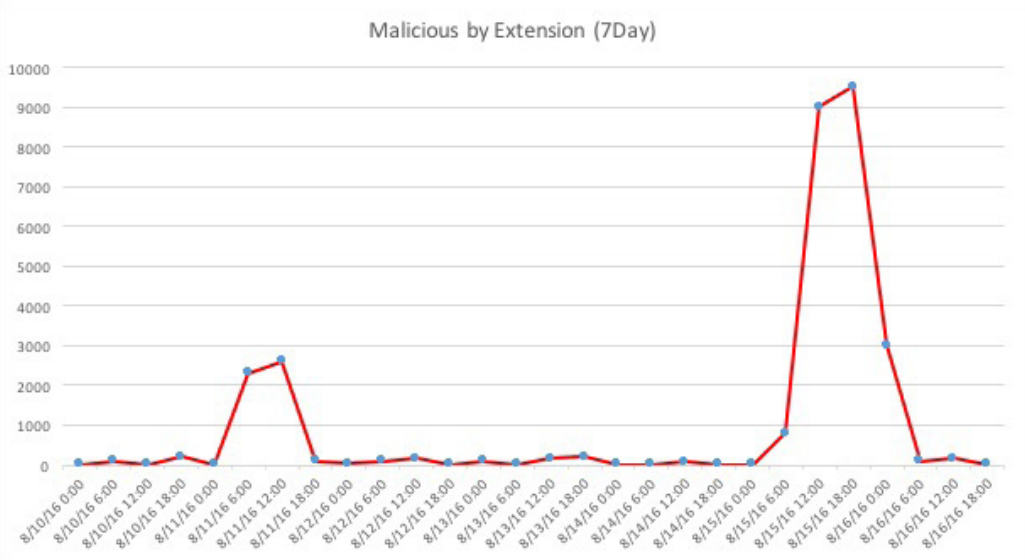
Barracuda ATD leverages a powerful global threat intelligence system, which ingests vast amounts of diverse threat information from over 50 million deployed collection points around the world. Whenever new attacks occur against networks, web gateways, web applications, or email systems, that information is absorbed in real time and shared across Barracuda's products and user base.

Example #1: Ransomware Outbreak

- In March 2016 , eight variants of Locky appear across the internet.
- 7 of 8 variants were blocked by our Static Analysis Layer in less than one second.
- The remaining variant was blocked by our Dynamic Analysis Layer within minutes.

Example #2: Methodical Attack via MS Word

- Public domain AV signature provider mistakenly categorized all .doc files as viruses.
- Large numbers of legitimate .doc files were blocked from transmission when they encountered an AV layer.
- Security vendors reacted by disabling AV technology from blocking .doc files affected by the false positive.
- The next day, Barracuda ATD Service detected a larger than usual amount of .doc files being sent over email.



- Barracuda ATD found 80% of these .doc files to contain polymorphic malware, able to change its signature to evade standard AV.

Lessons Learned

The first lesson is that criminals are constantly watching the security industry, and are alert to opportunities that arise. In this case, they quickly realized that .doc attachments would likely receive reduced scrutiny, and launched large numbers of attacks within a matter of days.

Another lesson is that multiple layers of protection are essential to keep you secure even when something goes wrong, as it did in this case. While traditional antivirus stopped being effective, the attacks were successfully stopped by a more dynamic layer of protection.

Finally, it's a reminder that all users must remain vigilant at all times. Your first and best line of defense against many types of attack is a user base that is well trained to spot and respond to suspicious emails and attachments.

Using ATD as an Effective Layer of Protection

While many security vendors use machine learning in their threat detection systems, what they lack is volume and diversity. Machine learning requires high volumes and diversity of data to be most effective. When presented with high volume and a diverse set of data, machine learning farms are able to learn, evolve, and adapt when fed from a variety of data sources like web, email, and network data traffic.

Barracuda's ATD infrastructure utilizes a hardware-accelerated machine learning farm that ingests data from more than 50 million endpoints in the field. Looking at over 900 attributes per artifact, Barracuda ATD is able to calculate and identify new and emerging threats in minutes. To put this into perspective, companies such as FireEye and Wild Fire scan at most 200 – 300 attributes.

In a 2016 independent test of advanced threat detection technology, only Barracuda achieved 100% effectiveness with zero false positives and zero false negatives. Other solutions scored as low as 86.5%, with 93.3% marking the midpoint score. The report also indicated that many attacks were detected immediately, some attacks took close to 24 hours to be detected, and other attacks were never detected by some products.

Conclusion

Public cloud service providers like Google (Google Apps for Work/Education) and Microsoft (Exchange and Office 365) provide native security to keep users safe from a wide array of threats. But these "native" features often do not include multiple layers of protection or the flexibility to adapt to a changing threat landscape. With the addition of Barracuda Advanced Threat Detection, users of email systems like Microsoft Exchange and Office 365 can easily add an effective, nimble, and adaptable solution to detect and prevent today's sophisticated, targeted, and zero-day attacks.

Barracuda Advanced Threat Detection is available with and can be added to Barracuda Essentials, NextGen Firewalls, and Web Security Gateway.

For more information please visit our technical library.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data, regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

US 1.0 • Copyright 2016 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008
408-342-5400/888-268-4772 (US & Canada) • barracuda.com
Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States.
All other names are the property of their respective owners.

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com