Barracuda

Advanced Threat Detection

Next-level protection against advanced malware, targeted attacks, and zero-hour exploits

When existing antivirus protection and/or intrusion prevention systems being used are no longer capable of solely dealing with modern, persistent threats, it is essential to add Advanced Threat Detection to a company's security environment.

The Barracuda Difference

Barracuda Networks' Advanced Threat Detection (ATD) implements full-system emulation which provides the deepest visibility into malware behavior while simultaneously being the toughest one to evade. Files are checked against a cryptographic hash database that is constantly updated, and in case the file is unknown, it is emulated in a virtual sandbox where malicious behavior can be discovered. While traditional solutions mostly detect network threats after they have breached the network and after sending log notifications to the administrator, the Barracuda NG Firewall supports two types of emulation policies that can be assigned to specific file types.

The first policy is the traditional "let the user download a file and forward it to the emulation service." As soon as the file is scanned and malicious file activity has been identified, a log event will be created and the administrator can contact the user to remediate the threat. Since the malware has been downloaded to the corporate network, preventing the malware from spreading and damaging valuable corporate assets is now key. In order to minimize this breakout, Barracuda NG Firewall provides an automatic User/IP/machine blacklisting feature that will automatically quarantine victims of advanced malware by blocking further network activities. The second policy that can be assigned on a per-file basis forces the user to wait until the file is emulated and not malicious or suspicious. Only safe files will be forwarded to the respective user.

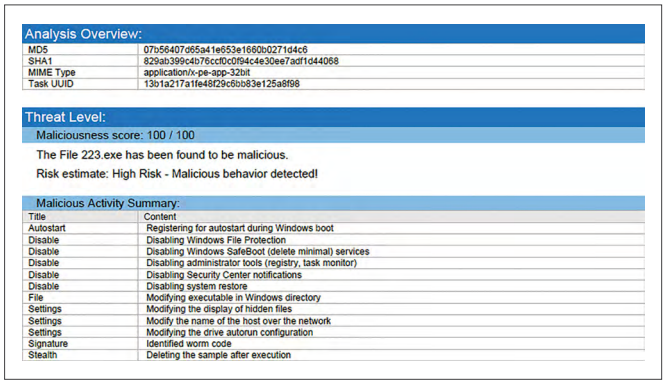
Barracuda **NG Firewall**
The next-generation firewall for enterprise-scale distributed networks

The Barracuda Advantage

- **Flexible, Simple Deployment:** Easy to deploy, easy to use, and affordable Advanced Threat Detection. No new equipment is needed.
- **Full-System Emulation:** Not only detects targeted and persistent attacks, but also malware that was designed to evade detection by traditional sandboxes used by first-generation advanced persistent threat security vendors.
- **Automatic User and IP Blacklisting:** Based on identified malware activities infected users can be automatically blocked from the corporate network.
- **Customizable, On-demand Analysis Reports:** Available for any emulated file providing full information on malicious activities such as registry entries, network activity (e.g., botnet command and control center traffic), or obfuscation tactics.
- **Unrivaled Detection Speed:** Provides instant threat visibility and protection.
- **Information on Identified Malware:** It's centrally stored and shared in order to optimize emulation.

Key Features

- Prevent malicious files—even unknown ones—from entering the organization and avoid network breaches.
- Identify zero-day malware exploits, targeted attacks, advanced persistent threats and other advanced malware which routinely bypass traditional signature based IPS and antivirus engines.
- Granular Control over PDFs, EXEs/MSIs/DLLs, Android APKs, Microsoft Office files, and compressed files and archives
- Full interoperability with the integrated SSL Inspection files can be extracted and checked in order to detect advanced malware in the encrypted stream.
- Cloud based emulation – resource intensive file emulation is offloaded to the Barracuda Cloud.
- Learning local cryptographic hash database for emulation optimization
- Multiple and simultaneous OS environments for emulated files
- Automatic email notifications in case malware activity has been identified can help minimizing the time for reaction of the administrator in order to mitigate the network breach.
- Available for hardware and virtual appliances as well as for Microsoft Azure and the Amazon AWS Cloud



Analysis Overview:

MD5	07b56407d65a41e653e1660b0271d4c6
SHA1	829ab399c4b76ccf0c0f94c4e30ee7adf1d44068
MIME Type	application/x-pe-app-32bit
Task UUID	13b1a217a1fe48f29c6bb83e125a8f98

Threat Level:

Maliciousness score: 100 / 100

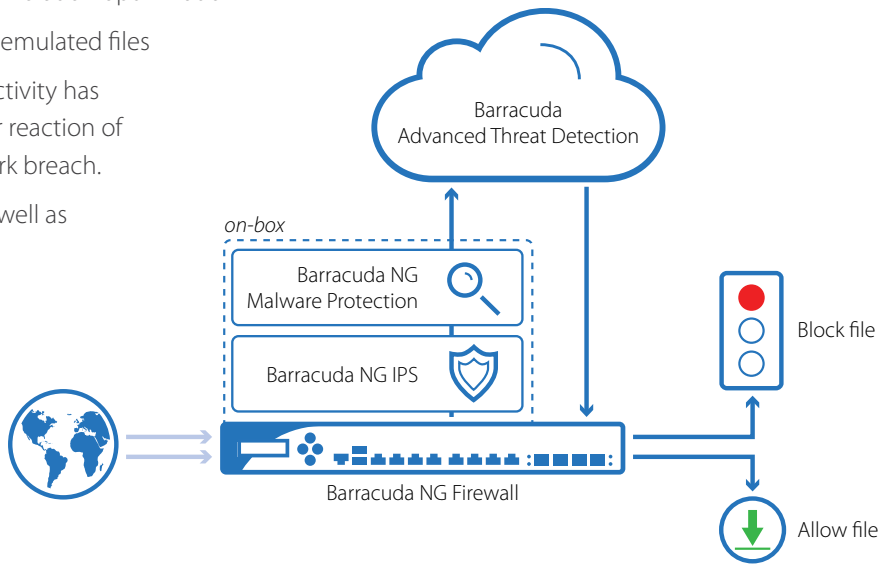
The File 223.exe has been found to be malicious.

Risk estimate: High Risk - Malicious behavior detected!

Malicious Activity Summary:

Title	Content
Autostart	Registering for autostart during Windows boot
Disable	Disabling Windows File Protection
Disable	Disabling Windows SafeBoot (delete minimal) services
Disable	Disabling administrator tools (registry, task monitor)
Disable	Disabling Security Center notifications
Disable	Disabling system restore
File	Modifying executable in Windows directory
Settings	Modifying the display of hidden files
Settings	Modify the name of the host over the network
Settings	Modifying the drive autorun configuration
Signature	Identified worm code
Stealth	Deleting the sample after execution

Example for a Barracuda ATD Report that shows why a specific file was identified as advanced malware



ANALYSIS AND PREVENTION OF THREATS (MALWARE, INFECTED OBJECTS)	
Dynamic, on-demand analysis of malware programs (sandboxing)	●
Dynamic analysis of documents with embedded exploits (PDF, Office, etc.)	●
Detailed forensics for both, malware binaries and web threats (exploits)	●
High-resolution malware analysis (monitoring execution from the inside)	●
Support for multiple operating systems (Windows, Android, etc.)	●
Flexible malware analysis in the cloud	●

Availability

- The Barracuda Advanced Threat Detection is available as a separate subscription.
  An active Barracuda Malware Protection or Barracuda Web Security subscription is needed.
- Barracuda NG Firewall model F200 and higher
- All Virtual Appliances
- Microsoft Azure and Amazon AWS public cloud offerings