AppGuard: Validation Testing with Weaponized Documents
AppGuard: Helping Secure the Endpoint

Red Phoenix Consulting partnered with Blue Ridge Networks to offer students of ECPI University an opportunity to perform penetration testing on an endpoint security software, AppGuard. AppGuard prevents viruses, fileless malware, botnets, polymorphic malware, weaponized documents, targeted attacks, in-memory attacks, ransomware, phishing, watering-holes, drive-by-downloads, and other undetectable advanced threats.

We tested AppGuard for a period of 50 hours over the course of a five-week period. AppGuard was loaded onto a Windows machine running Windows 8. While the testing occurred on a machine running Windows 8, AppGuard can also be installed on Windows XP through Windows 10, Windows Servers and Linux Servers. The processor was an Intel Core i3 with 4GB of memory. The system was also running Malwarebytes, but for testing Malwarebytes was disabled. The testing was completed with AppGuard default policy out of the box with no adjustments.

We used multiple tools to perform our analysis. These tools included Kali Linux, Burpe Suite, Metasploit, and Security Onion. This testing was conducted in a lab environment at the Raleigh, NC campus of ECPI University. The class was titled “Ethical Hacking”. This class is an upper level class designed for seniors. The class provided a close look at hacking techniques and how to utilize those to ethically hack systems for the good of the system owner.

Methodology

We used multiple forms of social engineering during the testing. Phishing attacks, business email compromise, and clickjacking were used. We also directly downloaded the weaponized documents onto the laptop and attempted to simply open the document.

A weaponized document is a Word, Excel, or PDF document that has been poisoned by adding malicious code as a macro to the document. This is one of the most prevalent vectors for delivering ransomware, cryptojacking malware, and most other forms of malicious software.

We selected several weaponized documents that are logged and tracked by the IBM X-Force Exchange and have a Common Vulnerabilities and Exposures (CVE) number.

Malware Variants Used During Testing

- **FlawedAmmyy RAT**
  - SHA: 0e916e17f8cbe2f1ae29e13f116c8611cb7679607695ee d355025295fb1999a
  - CVE: CVE-2017-11882

- **Haka.exe**
  - SHA: 4246e2e2bf91f36bd7142587ea2593304b656f6db25fbdc 568f4d3cb584e98b5c
  - CVE: CVE-2017-11882

- **Emotet**
  - SHA: 5de907e366f6770a23f589f4578e0d6417641a
  - CVE: CVE-2018-15982

- **Oakbot**
  - SHA: 0bbba90c611483084cb9bc695635332a32fa3cabe4782 b7f1251544a5a607c
  - CVE: CVE-2007-4673

All of these malware variants were tested against AppGuard using one or more of the following attack vectors:

**Phishing Attack**

The malware was attempted to be delivered to the system using an email with the weaponized document attached. The email recommended that the receiver open the attachment for some type of reward or to receive important work-related information. If the document were opened, the system would then be infected.

**Business Email Compromise**

A false business email account was established, and several students were given business related roles such as CEO, CFO, CISO and email accounts were established for each role. An email was constructed to mimic the email of the CEO demanding that the CFO send funds immediately to a certain account. The account information was included in a PDF with the company letterhead and all necessary information. The PDF was weaponized and if opened, the system would become infected.

**Clickjacking**

An email was sent to the victim. This email recommended that the receiver click a hyperlink in the email to receive a reward or to retrieve needed business information. If the victim clicked the link, the system would become infected.
Results
Over the 50-hour period, we were able to successfully launch over 30 different attacks. The students received valuable information on how an attack of this type is constructed and how social engineering is used. The students also received valuable instruction on how to review event logs and to decipher what had happened to cause the logged event. As stated earlier, we used multiple different attack vectors in the process.

“None of the attacks were successful as AppGuard did not allow the malware to perform the functions they were constructed for.”
- James W. Martin, President, Red Phoenix Consulting

AppGuard performed as advertised and prevented the malware from harming the system.

The most impressive functionality of AppGuard other than the protection engine itself, was the extensive logging that occurs with each potential attack. These log records could prove to be invaluable to a forensics investigation or a postmortem examination of the attack. In essence, the logs would be a very useful Threat Intelligence feed to combine with other network feeds and intelligence that can be utilized as attack information without a compromise ever occurring at the protected endpoints, laptops, desktops, tablets, servers and other windows driven devices such as POS and ATMs.

One of the examples included blocked script and executable files that might be unknown to detection-oriented tools for months. The forensic benefit of these logs with an early attack suppression can result in capture of adversary artifacts (files) that would be otherwise destroyed by command later in the attack.

Conclusion
The testing conducted was not intended to be an all-encompassing test of AppGuard but rather a test using a small sample of malware variants currently in the wild. The sample malware were chosen because they are extremely harmful if they were successfully deployed to a victim. The attack vectors are those that are seen while attempting to deliver these malware variants.

AppGuard performed well during testing, and there were no successful attacks using any of the malware or any attack vector.

The most impressive functionality from the security perspective is not only repelling every attack, but also the log information that AppGuard captures, which is easily available to the user and the security experts.

AppGuard is an essential tool to use in protecting the endpoint. AppGuard could be used as part of the layered approach to secure the endpoint. The modern endpoint is constantly moving and having a trusted ally to help secure it would be extremely helpful. AppGuard should be considered as that ally.

About Red Phoenix Consulting
Red Phoenix Consulting is a premier cyber security consulting firm. With over 30 years of service in the security arena, Red Phoenix is perfectly positioned to provide unparalleled services to our clients. Red Phoenix and its partners strive to provide our clients counsel and guidance to navigate the threat landscape that threatens your organizations security.

About Blue Ridge Networks
Blue Ridge Networks is a proven cybersecurity isolation and containment technology innovator delivering network segmentation, remote access, and endpoint cybersecurity solutions that eliminate vulnerabilities to critical network infrastructure and prevent exfiltration of mission critical data. The company has successfully provided resilient, scalable, and affordable cybersecurity systems, software, and managed services for over 20 years, protecting critical operations of its government and enterprise customers with no reported breaches of its technologies - ever. For more information, visit: www.blueridgenetworks.com or contact sales@blueridgenetworks.com.