IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Isolation: Defining a Fresh Approach to Cybersecurity

Adapted from *Worldwide Web Security Forecast, 2015–2019: Steady Transition to the Cloud* by Robert Westervelt, Elizabeth Corr, Pete Lindstrom, IDC #258801

January 2017

Sponsored by Ntrepid

Current cybersecurity measures, though sophisticated, do not prevent all attacks and fall short of providing the security that we need. The solution is not more of the same; rather, different approaches are required to address the issue. Isolation is a new application of technology that fundamentally changes the approach to cybersecurity by shifting the effort from deciding whether a file or an activity is malicious to keeping all external interaction separate and distinct. This Technology Spotlight examines the isolation approach to security and looks at Ntrepid's solution, Passages, in the emerging market for isolation security.

Introduction

Let's face it. The 2017 cybersecurity reality is bleak, and the task of guarding cyberassets is increasingly difficult. We can attribute this reality to four key trends:

- **The sophistication of cybermiscreants is growing rapidly.** From massive-scale Internet of Things (IoT)–based distributed denial-of-service (DDoS) attacks to ransomware, cybermiscreants are becoming more clever. These attackers are motivated by the increasingly large "paydays" providing a return on their efforts. Cybercrime has paid handsomely as of late.
- **The perimeter has died.** It is safe to consider the impenetrable network perimeter officially dead given that data, applications, and devices cannot predictably be found in the networks that reside behind perimeters. Today, compute, application, and data resources reside on-premises or in the cloud and in both simultaneously at times. These resources are accessed from workstations, PCs, Macs, smartphones, tablets, and a potpourri of IoT devices such as printers. Cybersecurity professionals have been tasked with protecting and securing corporate resources and maintaining compliance with a host of standards such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the ISO 27000 family of standards.
- **Security tools have proliferated.** As the number of cybersecurity challenges has grown, so has the number of security point products offered by security companies to address those challenges. IBM cites an example of one client having 85 different security tools from 45 different vendors.[1] Operation, maintenance, and employee training become issues in such environments.

[1] https://www-304.ibm.com/events/tools/interconnect/2016ems/REST/presentations/PDF/InterConnect2016_7047.pdf

- **Qualified information security professionals are scarce.** (ISC)[2] predicts that by 2019, the shortfall of qualified security professionals will exceed 1.5 million. "Pushing security tasks onto traditionally non-security IT professionals and leaving some security tasks undone or sub-optimally completed are the larger, unseen outcomes."[2] In other words, the problem is getting worse.

Defining a New Approach

Although we have seen some innovative new offerings in the cybersecurity market, the approach taken by the majority of today's technologies is essentially the same: They are looking to detect the bad or malicious. This method is limited in its success, like an infinitely iterative "cat and mouse game" of detection technology implemented by security professionals and detection evasion techniques implemented by miscreants. McAfee describes the phenomenon as the Grobman Curve of Threat Defense Effectiveness.[3] The only way to escape the continual "cat and mouse game" is to deal with the problem differently.

One such new tactic is "validating the known." This approach takes a different tack to the problem, looking to validate objects as good or valid compared with a certified list of known files or objects. Objects that cannot be validated are treated as untrusted, changing the very premise of security. The binary "good versus bad" classification gives way to validated good and invalidated.

A variant of the "validating the known" approach is isolation. Isolation accepts that it may be impossible to 100% validate objects, taking an "expect the worst, protect first" perspective. As a result, objects that come from invalidated and/or untrusted channels such as the internet are sequestered, isolated in virtual machine environments with interaction limited to graphic rendering to a viewing device. Much like viewing the activity behind a glass window of a clean room, interaction with the outside world is limited to visual stimuli, regardless of whether the isolation environment is on a server, in the cloud, or on an endpoint.

Benefits of Isolation

The net effect of isolation is that any potential malicious binaries are contained within the isolation environment. Processes run in the virtualized machine have no interaction with endpoint devices such as PCs or smartphones, rendering the endpoint as a "screen" or viewing device. Any changes that happen to applications, files, or operating systems occur within the virtualized environment. The changes in the virtualized environment and any impact that the changes may have had on the virtualized host system are discarded at the end of the session as the virtualized host is discarded. Future sessions will begin with a new "golden image" based virtual machine.

Isolation is excellent for applications that need real-time response on vulnerable endpoints yet require interaction with an open cyberenvironment. Web browsing and email are excellent use cases because the latency that could be introduced by a technology such as network security sandboxing could be punishing.

[2] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

[3] http://www.mcafee.com/us/second-economy/index.html

Isolation does not necessarily mean that traditional technologies are not complementary. For example, suspicious files can still be sent to a sandbox for analysis, providing valuable intelligence. However, high-risk binaries would have no interaction with the endpoint, meaning that damage cannot be done.

Interestingly, isolation has the unintended benefit of providing an added layer of security by "embracing the cat and mouse game." Today's malware looks to evade detection. Moving from standard viruses to targeted, polymorphic malware is an example of evading detection. As sandboxes became an increasingly popular way to detect malicious binaries based on behavioral detection, cybermiscreants, realizing that most sandboxes are virtualized, implement virtual environment tests. If the malicious binary detects a virtualized environment, it is assumed that the binary is in a sandbox and the binary shuts down or fails to launch. The goal of protecting endpoints is essentially accomplished simply by allowing the binary to detect the virtualization and subsequently shut down. Executables that quickly terminate after virtual environment checks can then be submitted for forensic analysis, providing an excellent source of malware intelligence.

Considering the Ntrepid Passages Approach

Ntrepid has released an isolation platform, referred to as Passages. Passages establishes a web browser in a virtual environment on the endpoint. The browser "walks, talks, and acts" like a normal browser; however, it is hardened, completely isolating the browser from the rest of the system to manage high-risk web browsing applications on endpoints with a heightened need for security. Every new session is established based on a golden image, which is discarded at the end of a session.

The Passages platform provides additional benefits to strengthen the security efficacy of the isolation environment. All user and device identifying attributes are removed so that the originating source cannot be known. Downloaded files are placed in cloud-based file storage with integrated analysis, further protecting the host device from malicious payloads in the isolation environment. Administrative and reporting tools integrate with account management, deployment, and analytics platforms.

Challenges

As with any new technology or platform, a few challenges exist. First, attributes are present that need to be monitored, and virtualized environments require device resources. Device requirements can be minimized, but virtualization will place a processor, memory, and power "tax" on devices. Windows-based devices should be able to compensate for the tax, but issues should be monitored. Isolation can also be implemented in the network, in an on-premises server, or in the cloud. However, the network-based isolation environment has the opportunity to introduce latency into the browsing experience.

Second, we just do not know what we do not know. Cybermiscreants are clever. Ntrepid must remain vigilant in regard to vulnerabilities.

Finally, the platform does not currently have a mobile solution. Options for Apple iOS– and Android-based smartphones and tablets are important because those devices are most likely to be operated outside of the network perimeter and its corresponding security measure. Granted, mobile is a road map item for Passages.

Conclusion

The task of securing networks, applications, and data has become increasingly difficult as cybermiscreants have become more sophisticated and the resources invested for protection are increasingly limited. Thus new ways of tackling this task are necessary. Isolation is a technology that can fundamentally change the approach, isolating users and their devices from a cyberenvironment that can be perilous. Ntrepid's Passages is one such isolation platform that changes the rules of the game, protecting users from existing threats and threats yet to be discovered.
