Trusting Web Browsers: There is No Perimeter

February 2017

The Problem with Browsers

"Currently, virtualization techniques are the only way to safely secure all possible browsing scenarios."

Web browsers are essential for everything from research to commerce. Add cloud computing into the picture and it looks like they could be critical for the foreseeable future. Unfortunately, browsers are also the most common vector of network attack [1].

Due to the complexity and diversification of use cases, it is impossible to guarantee browser security using perimeter solutions. This is because all perimeter security products use detection and/or emulation techniques to identify attacks.

'Detection' is any method by which an activity can be identified as either good or bad, and 'emulation' is any technique that produces an artificial attack surface, allowing a vulnerability to be exploited for detection purposes.

For either of these methods to be effective, 'good' and 'bad' behavior must be predetermined. Since browser capabilities and business integration are always increasing, it is impossible to presuppose all good and bad browser behavior.

In other words, perimeter defenses are ineffective against emergent threats and will continue to diminish in efficacy against known malware as it evolves. For example, when network sandboxing technologies were first introduced they were very effective against stopping malware at the perimeter.

Since then, though, malware has been designed to 'go to sleep' to avoid detection, or to sign malicious payloads with stolen signing certificates so the sandbox allows them to pass through. The constant arms race between malware creators and security practitioners has not changed much in the last 20 years.

As bleak as this may seem, there is a solution to the problem. HP has partnered with Bromium to build on the secure solutions found in the world's most secure PC's. HP Sure Click uses virtualization-based security methods, such as hardware-enforced micro-virtualization, and does not require detection or emulation to offer protection against web-borne attacks.

Threats can be safely contained via CPU-enforced isolation, posing little or no risk to the host while analyzing malware behavior.

Risks Associated with Browsers

"In 2015, 62% of cyberattacks utilized a web browser exploit in some way.[2]"

Cyberattack motivations cover a wide spectrum, but the most prevalent is the theft or manipulation of data. The impact of these breaches ranges from brand damage and loss of revenue to complex litigation. The average cost of a breach in 2016 has increased to $4M, up from $3.2M in 2013 [3].

Large-scale incidents end up being much more expensive. A breach at health insurance company Excellus BlueCross BlueShield, for example, is expected to cost a minimum of $17.3M[4], while one at Anthem BlueCross BlueShield is estimated to exceed $100M[5].

Consider a scenario where a human resources specialist at a major corporation opens a résumé from a job applicant. The résumé contains no malicious content, but it does contain links to various references.

A website belonging to one of the references was recently hacked and is now serving up a new zero-day browser exploit. The specialist visits the afflicted site. The exploit will likely run since it originated from a previously benign domain and is leveraging a never-before-seen vulnerability.

Now the attacker has an opportunity to fully breach and scan the local machine and corporate network. Situations like this play out frequently in most organizations.

Why Browsers are Hard to Secure

"For every malicious domain detected, an additional 340 are undetected.[6]"

Various technologies and methods have been employed to increase browser security. Unfortunately, as potential attackers become more sophisticated most countermeasures have diminishing returns. Some of the most popular browser security enhancement techniques include:

- **Web Filtering**: actively filtering unwanted websites from a user's system. This usually is accomplished via a combination of static and dynamic mechanisms such as whitelists, blacklists and subscription-based website reputation services. The problem with this approach is that the enforcing technology must determine what sites are good or bad before the user accesses them.

- **Web Proxy**: attempting to pre-process web content and only passing along legitimate and benign data to the end user. The shortcoming of this approach is that it requires accurate detection and emulation to function properly.
- **Sandboxing**: running programs within a strictly moderated and segregated environment. The flaw with most sandboxing approaches is that security is enforced via software running on the user's operating system. This model can allow attacks originating within the sandbox to escape and affect the host.
- **Remote Browsing**: hosting a user's web browsing session on a non-local system such as a remote desktop. The main security issue with this approach is how to determine if a remote session has been compromised or is safe for use. Even if a remote browsing host is reset to defaults with every use, an exploit that occurs within a session has a chance to attack anything within that session, and perhaps more depending on the architecture of the remote environment.
- **Cryptographic Mechanisms**: deploying components responsible for maintaining the privacy, integrity and non-repudiation of various browser activities. Unfortunately, this does not guarantee that the activities protected by these mechanisms are benevolent.

Unfortunately, attackers seem to always find a new avenue of exploit. Sometimes activities that were once considered safe are exploited, or new vectors of attack are discovered, such as the steganographic concepts now being used to transport malware-afflicted image files[7].

Due to the variability of human-created software, it is reasonable to assume that a completely secure browser will not be available anytime soon.

Current Models Are Failing

"76% of IT organizations faced security challenges with zero-day threats before implementing Bromium.[8]"

Many modern attacks bypass perimeter defenses. Consider those that exploit HTML5, Adobe® Flash Player, Java, Internet Explorer, Firefox and Chrome™: as users engage in various browsing activities, data within the webpage can be used to initiate an attack on the host system.

This is exemplified by the historical popularity of Java exploits[9]. Many organizations have either commodity or proprietary software which requires Java support. This requirement may force an organization to install a vulnerable or legacy version of Java.

This vulnerable install may act as a vector of attack initiated from the browser. Software providers may release patches and updates to address this issue, but it is usually not until major vulnerabilities are exploited in the wild.

Browser exploits and web-based attacks are very effective in bypassing layered defenses because of the way web content is transmitted and rendered. It is extremely difficult to know what data may be used for an attack.

An example of this would be encrypted web traffic containing a targeted and hidden payload.

In a March 2016 global survey of 500 CIOs conducted by Vanson Bourne[10], 90% of respondents said they had seen or were expecting to see a network attack using Secure Sockets Layer or Transport Layer Security (SSL/TLS) protocols.

To have a chance at stopping such a threat, one would have to intercept it, unencrypt it, emulate the target and detect the attack in near-real time. All of this would have to occur without interfering with the end user's browser session.

This is an extremely expensive task for most organizations and often interrupts user workflow. Gartner says less than 20% of organizations decrypt all inbound SSL / TLS traffic[11]. Browser-born malware can strike without network security, endpoint security or end-users noticing until it is too late.[12]

Clearly, defense models need to evolve to keep up with today's cybersecurity challenges.

Losing the Detection Battle

Detection methodologies are quite varied. They include activities such as whitelisting, blacklisting and behavioral analysis. They range from static lists to dynamic artificial intelligence (AI) controlled rating systems.

Fundamentally they are all designed to accomplish one goal: determine if an action or artifact is good or bad prior to it affecting the system. But what exactly is good or bad is not so easy to define. In fact, the definition may vary across organizations, business units and even individuals within a business.

There are activities widely regarded as bad, but the gambit for detection revolves around the determination of what is good. It is impossible to decide if any arbitrary activity on a computer is bad with complete accuracy[13].

To avoid detection, all an attacker must do is act in a way that is not classified as bad. Consider an exploit scenario that involves a new attack method. This would not be recognized as bad until it was too late.

An example might be CVE-2016-4117, one of many recent Adobe Flash Player vulnerabilities, which was exposed in the wild for approximately seven weeks before a patch was issued[14].

Even patching might not solve the problem. More than 50% of organizations believe client-side patches are released at an unmanageable rate, which normally results in machines going unpatched for extended periods of time[15].

Losing the Emulation Battle

As stated above, 'emulation' is any technique that produces an artificial attack surface, allowing a vulnerability to be exploited for detection purposes. This would include network-based analysis engines, virtual execution engines and sandboxes.

Emulation environments attempt to simulate various versions of browsers, multiple system functionalities, or both. However, emulation does not mimic the entire operating system or all the software installed.

The flaw with emulation lies within the total number of scenarios that must be simulated to identify an attack. It is extremely difficult to accurately emulate every system that may come under attack, while keeping up to date with every version of software across the enterprise.

Due to the potentially large number of scenarios to emulate, this approach is highly prone to false negatives, meaning something malicious can easily slip by. This can lead to a false sense of security, allowing malware to execute on a target system.

End-user attack surfaces can change daily. Polymorphic malware is so prevalent it's estimated that 97 percent of malware is unique to the endpoint[16]. Since compute power is finite and results must be generated quickly, emulation can quickly become cost prohibitive.

With all these factors in mind, it becomes apparent that detection and emulation have rapidly diminishing returns against modern threats.

Virtualization for Security

In computing, 'virtualization' refers to the act of creating virtual environments such as a virtual machine (VM). Virtualization-based security models do not rely on detection or emulation to offer protection. VMs provide safe and disposable environments for users to operate in.

If something nefarious occurs, the VM can simply be reset or thrown away. The down side to virtualization is that each VM consumes the resources to run an entire operating system and the software within.

This can become costly for an organization running many virtual environments simultaneously. Over the last few years, malware has become virtualization aware and can detect if it is running within a VM[17]. If malware detects it is inside a VM it will attempt to avoid detection by halting further execution.

However, a new development in virtualization-based security provides the benefits of VMs while being fast and lightweight. In the 'micro-virtualization' model, individual applications are virtualized within a compact and transparent 'micro-virtual machine' (micro-VM) derived from the user's system.

This approach offers deceptive capabilities that can coax virtualization-aware malware into running. Meanwhile, forensic data will be collected about the malware executing within the micro-VM.

"When Bromium is enabled, I worry less about our staffs' browsing and clicking habits."

JUSTIN SMITH, SECURITY OFFICER,
THE VALSPAR CORPORATION

Micro-VMs are disposable environments governed by a special hypervisor called a 'microvisor', which ensures each micro-VM is separate from others and from the host system via a method called CPU-enforced isolation.

This type of isolation is provided by host CPUs directly managing resources in the micro-VMs. Micro-VMs are specifically constructed to run specific user applications such as browsers. This would allow an end user to browse website, no matter how dangerous, without risk of attack.

If an attack were to occur within a micro-virtualized browser session, it would simply be trapped within the micro-VM. Neither the user's system nor other browser sessions would be affected. The environment within the micro-VM is sanitized and the threat is nullified on closure.

Currently this safely secures all web browsing scenarios. HP Sure Click uses Bromium virtualization-based security to protect against web-borne attacks. Since the introduction to the market in 2012, Bromium has not had any customers report a breach.

Conclusion

Across almost every major enterprise, and many other entities, perimeter defenses are failing to stop threats. Modern attackers are striking deep into user assets via web browsers. Due to their relative complexity and business function, browsers are notoriously hard to secure.

Classical methods of detection and emulation are unable to defend against many current browser-based cyberattacks. HP Sure Click powered by Bromium micro-virtualization technology allows end users to safely surf the internet without risk of compromise.

If a browser-based attack penetrates all other defenses, it will be completely isolated and automatically remediated without the need for human intervention. Bromium's virtualization-based security model is ready for the cyberattack challenges of today and tomorrow.

Sophisticated technologies like micro-virtualization and CPU-enforced isolation greatly enhance the cyber resilience of a business. The Bromium platform transforms user assets from a source of attack liability into a cybersecurity resource for intelligence and defense.

[1] http://www.mcafee.com/us/resources/reports/rp-dissecting-top-5-network-methods-thiefs-perspective.pdf

[2] https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/

[3] http://www-03.ibm.com/security/infographics/data-breach/

[4] http://www.hipaajournal.com/cost-of-the-excellus-bluecross-blueshield-data-breach-3338/

[5] https://www.cnet.com/news/cost-of-anthems-data-breach-likely-to-exceed-100-million/

[6] https://www.cisco.com/c/dam/m/mk_mk/events/2016/ciscoconnect/pdf/Tracking_Down_the_Cyber_Criminals_Revealing_Malicious_Infrastructures_with_OpenDNS-Dragan_Novakovic.pdf

[7] https://www.virusbulletin.com/virusbulletin/2016/04/how-it-works-steganography-hides-malware-image-files/

[8] https://www.techvalidate.com/product-research/bromium/facts/6CE-66F-A31

[9] https://heimdalsecurity.com/blog/java-biggest-security-hole-your-computer/

[10] https://www.venafi.com/assets/pdf/wp/Venafi_2016CIO_SurveyReport.pdf

[11] http://www.gartner.com/document/2635018

[12] http://www.infosecurity-magazine.com/news/browserborne-malware-costs-top-32mn/

[13] http://groups.csail.mit.edu/cis/crypto/classes/6.857/papers/ChessWhite.pdf

[14] https://www.fireeye.com/blog/threat-research/2016/05/cve-2016-4117-flash-zero-day.html

[15] http://www.darkreading.com/endpoint/patch-management-still-plagues-enterprise/d/d-id/1324615

[16] https://www.webroot.com/us/en/about/press-room/releases/webroot-2016-threat-brief-explores-next-generation-cyber-threat-landscape-and-targeted-intrusion-trends

[17] https://blog.malwarebytes.com/threat-analysis/2014/02/a-look-at-malware-with-virtual-machine-detection/

Bromium®

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information refer to www.bromium.com or contact mkt@bromium.com