INFO BRIEF

Web Browser-Based Attacks

Browsers are integral to an effective working environment but they also serve as the perfect cyberattack vector. Web-based attacks are one of the top methods of system compromise and they are on the rise. According to a report by Sans Institute, 48% of threats entered organizations via web-based drive-by or download[1]. They can be leveraged to deliver anything from zero-day attacks, to ransomware, cryptominers and other malicious browser-executable code. Browser-borne malware costs companies an estimated average of $3.2 million per year.

What is a Web-Based Attack

Web-based threats leverage browsers and their extensions, websites, content management systems and IT components of web services and applications to harvest credentials, skim visitor payment details or infect systems with malware or ransomware (or any combination thereof). Of particular danger to organizations are fileless attacks that take advantage of browser third-party plug-ins like JavaScript, Flash, and ActiveX, as there are no links or files for security systems to detect and behavioral monitoring always leaves some window of exposure. The recent British Airways and Ticketmaster breaches were both caused by malicious JavaScript code injected into their websites.

Common Types of Web Threats

DRIVE-BY DOWNLOADS

Drive-by downloads automatically download malicious content onto an end-point without any user interaction. All it requires is visiting a malicious site or a legitimate one that has been compromised. The embedded malicious code downloads to the victim's system and scans for exploitable vulnerabilities. These can be OS, browser, application or plug-in vulnerabilities that allow the attacker to gain a foothold to eventually download the malicious payload of their choice. A variant of the drive-by-download is malvertising, where fake advertisements containing malware are displayed on legitimate websites. Ad platforms have screening mechanisms, but cybercrime groups find their way around them – it's estimated that 1in 200 online ads is malicious. Drive by downloads are second only to email as a threat delivery vector.

PLUGINS AND EXTENSIONS

Most browsers support third-party plugins or extensions to add capabilities. While many are from reputable vendors, others can include malicious capabilities. And even legitimate plug-ins can contain security flaws that attackers can target. Adobe Flash, for example, is a major source of vulnerability exploits. Successful

[1] Source: https://www.sans.org/reading-room/whitepapers/threats/2017-threat-landscape-survey-users-front-line-37910

PREVENT WEB-BASED ATTACKS WITH MOVING TARGET DEFENSE

Morphisec protects every browser instance by adding a dedicated memory defense layer that prevents attacks from ever gaining a foothold – without slowing down your business.

- Instantaneously stops browser-based threats before they can penetrate your system or gain access to your network
- Permanently sanitizes application installers of adware
- Works invisible to end user, with no alteration to application interface and no impact on operations
- Functions seamlessly across virtual, physical or hybrid IT environments

MORPHISEC
Moving Target Defense

exploitation of such vulnerabilities can let attackers install ransomware, exfiltrate data, steal intellectual property or any number of other actions that put businesses at risk.

UI-REDRESS ATTACK

Commonly called clickjacking, this type of attack tricks a user into unknowingly clicking on a button or link that enables a malicious action. The attacker uses hidden iframes, text boxes or stylesheets to disguise the real click action, while the user thinks they are clicking on something innocuous such as an antivirus alert or a "like" button.

MAN-IN-THE-BROWSER ATTACKS

A man-in-the-browser (MITB) attack uses a Trojan to infect the victim's internet browser and modify information as it is exchanged between the browser interface and the internet. Unlike some other web attacks, the user is not redirected to a malicious URL. Browsing and transactions take place as normal, but the malware interposes itself between the web application and the user's browser, capturing and relaying sensitive information back to the attacker. It can also modify how the webpage appears, injecting form fields to capture additional information. Attackers can steal personal information, such as login credentials, account details and even social security or passport numbers. While typically targeting financial sites, the stolen data is often sold on underground markets and can be used to gain entry to corporate networks, especially as 60% of internet users reuse passwords across multiple accounts[2].

ADWARE

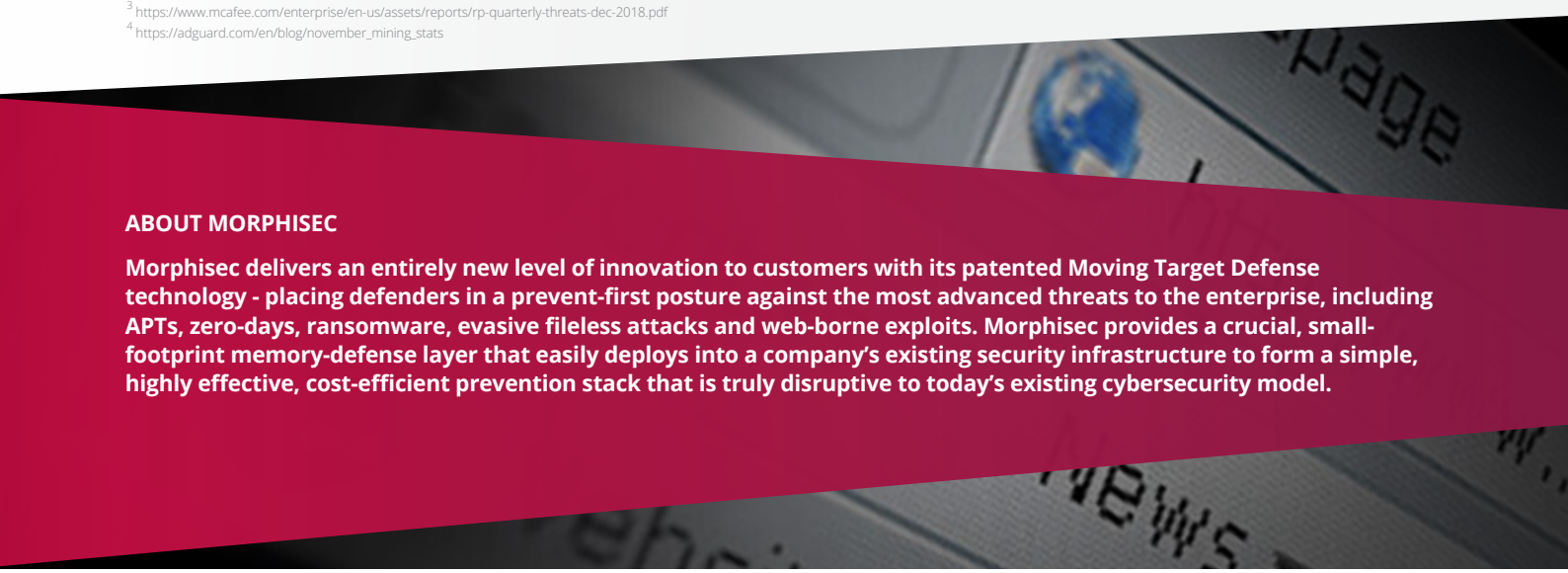
Adware is usually installed together with a free or shareware program. It is also delivered via drive-by-download. These days, adware is more than just a nuisance. Much of today's adware borders on spyware. It can collect user information, hijack the browser and search engine, redirect to unknown websites and/or display pop-up ads, which may or may not be malicious download links in disguise. In addition, many strains of adware are being incorporated as part of broader attacks with sophisticated, evasive techniques to penetrate operating systems and bypass security defenses.

BROWSER-BASED CRYPTOMINING

McAfee reported that cryptomining attacks increased by more than 4000 percent in 2018[3] and recent research by AdGuard found cryptojacking scripts on over 33,000 sites[4]. Cryptomining is the process of verifying encrypted cryptocurrency transactions, which requires considerable computational power. As payment, miners receive a small amount of cryptocurrency. In a browser-based cryptojacking attack, the attacker has injected coinmining JavaScript into a website, which then runs in the victim's browser as they visit the site, hijacking the victim's computing resources. Some variants allow compromised sites to keep mining even after the browser appears closed by using a hidden pop-under window. While browser-based cryptomining doesn't generally pose a danger to information or IP security, it can slow operations, increases enterprise CPU usage and other resources and adds to organizational costs.

Morphisec is built on Moving Target Defense to proactively prevent browser-based attacks on your physical and virtual endpoints.

[2] https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic
[3] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf
[4] https://adguard.com/en/blog/november_mining_stats



ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology - placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small-footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's existing cybersecurity model.

MORPHISEC
Moving Target Defense

www.morphisec.com
+1 617-209-2552