استفاده از رویکردهای امنیتی مبتنی بر جداسازی وب در جهت افزایش امنیت تراکنش‌های مالی تحت‌وب

Using Web Isolation Approaches To Secure Financial Online Transactions

اسماعیل ملااحمدی، مدیر واحد امنیت اطلاعات شرکت خدمات انفورماتیک نوین کیش، mollaahmadi@cert.sharif.edu
Esmaeil Mollaahmadi, Risk Management & Information Security head, Kish Informatics Services Corporation.
(الهام محمودآبادی، کارشناس توسعه شرکت بهسازان ملت، mahmoudabadi@aut.ac.ir
(Elham Mahmoudabadi, Developer, Behsazan Mellat Co.

چکیده (فارسی)

امروزه تمرکز بسیاری از حملات سایبری، بر روی کاربران نهایی است. به طوری که مهاجمان با دور زدن ابزارهای دفاعی نظیر ضدویروس‌ها و دیواره‌های آتش و هم‌چنین استفاده از آسیب‌پذیری‌های موجود در مرورگرها و افزونه‌ها، کاربران نهایی را مورد حملات خود قرار می‌دهند و از طریق آلوده کردن رایانه، تبلت و گوشی‌های هوشمند اقدام به ربودن اطلاعات بانکی و سوء استفاده‌های مالی می‌کنند. خنثی‌سازی حمله‌های مهاجمان از طریق جداسازی، یکی از رویکردهای امنیتی است که به کمک ایجاد شکاف بین کاربران و وب، احتمال دسترسی به سیستم کاربر و آلوده کردن آن را کاهش می‌دهد. جداسازی وب که گاهی از آن به عنوان جداسازی مرورگر نیز یاد می‌شود، یکی از رویکردهای تکامل‌یافته‌ی جداسازی است. بنا بر گزارش گارتنر، این رویکرد حفاظتی یکی از برترین فن‌آوری‌های امنیتی در دو سال اخیر بوده و پیش‌بینی می‌شود که در چهار سال آینده نیز، رشد استفاده از فن‌آوری‌های مبتنی بر جداسازی وب تا پنجاه درصد افزایش یابد. در این مقاله ضمن معرفی و بررسی برخی از روش‌های جداسازی وب که در چند سال اخیر در حوزه‌های مالی و بانکی مورد استفاده قرار گرفته‌اند، به بررسی مزایا و معایب این روش‌ها نیز خواهیم پرداخت.

واژگان کلیدی: جداسازی از راه‌دور، جداسازی وب، جداسازی مرورگرها، رویکردهای امنیتی، امنیت تراکنش‌های مالی تحت‌وب، امنیت کاربران نهایی.

طبقه‌بندی JEL: L86

چکیده (انگلیسی)

On today's end users are the aims of almost cyber-attacks. The attackers try to bypassing defense tools such as anti-virus and firewalls and use of browser and plug-in vulnerabilities to attack end users. This is a way for infecting the computers, tablets and smart phones to steal banking and financial user information. Eliminate of attacks through isolation is one of the security approaches that reduce the chance of infecting the device based on the concept of creating an air-gap between the web and users. Web isolation, which is also referred to as browser isolation, is one of the evolutionary approaches of isolation. According to the Gartner report, this security approach has been one of the top security technologies in the past two years, and it is expected that in the next four years, the growth of the use of web-based technologies will increase by as much as 50 percent. In this paper we will introduce some of web isolation approaches and checking the advantages and disadvantages of these methods.

Keywords: Remote isolation, Web isolation, Browser isolation, Security approaches, Web-based financial transaction security, End-user security.

JEL Category: L86.

مقدمه

امروزه بسیاری از جرائم رایانه‌ای از طریق اینترنت و با استفاده از آسیب‌پذیری[۱]های موجود در مرورگر[۲]ها و یا افزونه[۳]های آن‌ها انجام می‌شود [۱] و به‌کارگیری رویکردهای امنیتی مرسوم، برای مقابله با این تهدیدها، به نظر کافی نمی‌رسد. مهاجمان به‌راحتی سازوکار[۴]های دفاعی از قبیل ضدویروس[۵]ها، دیواره‌های آتش[۶] و دروازه‌های امن[۷] وب را دور زده و حمله‌های خود را انجام می‌دهند. این حمله‌ها، با آلوده کردن رایانه و یا سایر دستگاه‌ها مانند تبلت[۸]ها و گوشی‌های هوشمند[۹]، اقدام به ربودن اطلاعات محرمانه‌ی آن‌ها می‌نمایند، به‌طوری‌که آمار موجود نشان می‌دهد، بیش از ۸۰ درصد رایانه‌ها، از راه وب به بدافزار[۱۰]ها آلوده می‌شوند [۲].

حساسیت موضوع زمانی افزایش می‌یابد که دستگاه‌های آلوده‌ی کاربران، حاوی اطلاعات مالی آن‌ها باشد و حمله‌کنندگان از طریق این بدافزارها، اقدام به ربودن اطلاعات محرمانه و سوءاستفاده‌ی مالی از کاربران کنند. کارشناسان حوزه‌ی امنیت

[1] Vulnerability
[2] Browser
[3] Plugin
[4] Mechanism
[5] Anti-virus
[6] Firewall
[7] Web gateway
[8] Tablet
[9] Smart phone
[10] Malware

معتقدند که به کارگیری رویکردهای امنیتی مرسوم، برای مقابله با تهدیدات روزافزونی که از وب سرچشمه می‌گیرد، موثر نیستند. از این رو در سال‌های اخیر، رویکردهای دیگری مانند روش‌های مبتنی بر جداسازی وب[11] ارائه شده است.

برخی از روش‌های جداسازی از قبیل روش‌های مبتنی بر استفاده از زیرساخت میزکار مجازی[12] معایبی دارند. روش جداسازی وب که معمولا از آن به عنوان جداسازی مرورگر[13] نیز یاد می‌شود، تکامل‌یافته‌ی روش‌های امنیتی مبتنی بر جداسازی به شمار می‌رود. جداسازی از راه‌دور[14] مرورگر یا جداسازی وب، رویکردی است که در آن با ایجاد یک شکاف[15] بین وب و کاربر، امکان دسترسی بدافزارها به سیستم کاربر و آلوده‌سازی آن از بین می‌رود. در واقع در این رویکرد، شبکه‌ی ناامن نظیر اینترنت از سیستم کاربر نهایی[16] مجزا می‌گردد.

در سال‌های اخیر محصولات بسیاری مبتنی بر جداسازی وب ارائه شده، که در آن‌ها با مدیریت نشست[17]های وب، تهدیداتی که از طریق وب منتقل می‌شوند، خنثی شده‌اند و جریان محتوایی که کاربران نهایی بر روی دستگاه خود مشاهده می‌کند، پس از خنثی‌سازی حملات در اختیار آن‌ها گذاشته می‌شود. بسیاری از این روش‌ها مبتنی بر پروکسی[18] هستند و بنابراین نیازی به نصب نرم‌افزار بر روی دستگاه نهایی و یا مجزاسازی در سطح سیستم‌عامل ندارند و به‌دلیل سهولت استفاده و کارایی، بسیار مورد توجه قرار گرفته‌اند.

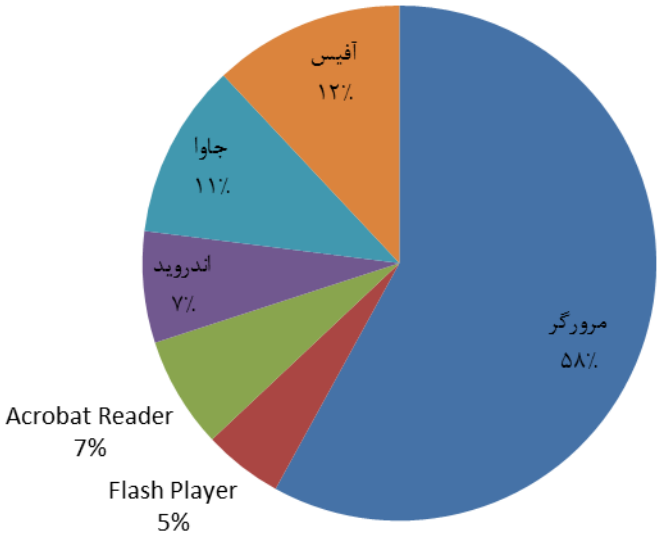
در این کار پژوهشی ابتدا مختصری به بررسی اهمیت موضوع و ضعف روش‌های امنیتی می‌پردازیم و سپس در بخش‌های بعد با مرور ویژگی‌های روش‌های مبتنی بر جداسازی وب، مزایای آن‌ها را بیان خواهیم کرد. هم‌چنین با بررسی ویژگی‌های برخی از محصولات و روش‌های جدید ارائه‌شده در این زمینه، مزایای استفاده از چنین ابزارهایی به منظور افزایش امنیت تراکنش‌های مالی تحت‌وب را برمی‌شماریم.

ادبیات موضوع

امروزه استفاده از درگاه[19]های پرداخت اینترنتی از قبیل اینترنت بانک و موبایل بانک، رواج زیادی پیدا کرده است و بخش زیادی از کاربران بانک‌ها و مؤسسات مالی، تراکنش‌های مالی خود را از طریق اینترنت انجام می‌دهند. از طرف دیگر طبق گزارش‌های موجود بخش زیادی از حملات امنیتی بر روی اینترنت صورت می‌پذیرد و حملات باج‌افزار[20]ها و فیشینگ[21] بیش-ترین سوءاستفاده‌ی مالی را مسبب شده‌اند [۳]. طبق گزارش گارتنر[22] ۹۸ درصد از حملات امنیتی بر روی اینترنت است که ۸۰ درصد از آن‌ها با استفاده از نشانی[23]های آلوده و ترافیک‌های وب، به‌طور مستقیم کاربران نهایی را هدف قرار می‌دهند [۴].

[11] Web isolation
[12] Virtual Desktop Infrastructure (VDI)
[13] Browser isolation
[14] Remote
[15] Air-gap
[16] End user
[17] Session
[18] Proxy
[19] Portal
[20] Ransomware
[21] Phishing
[22] Gartner

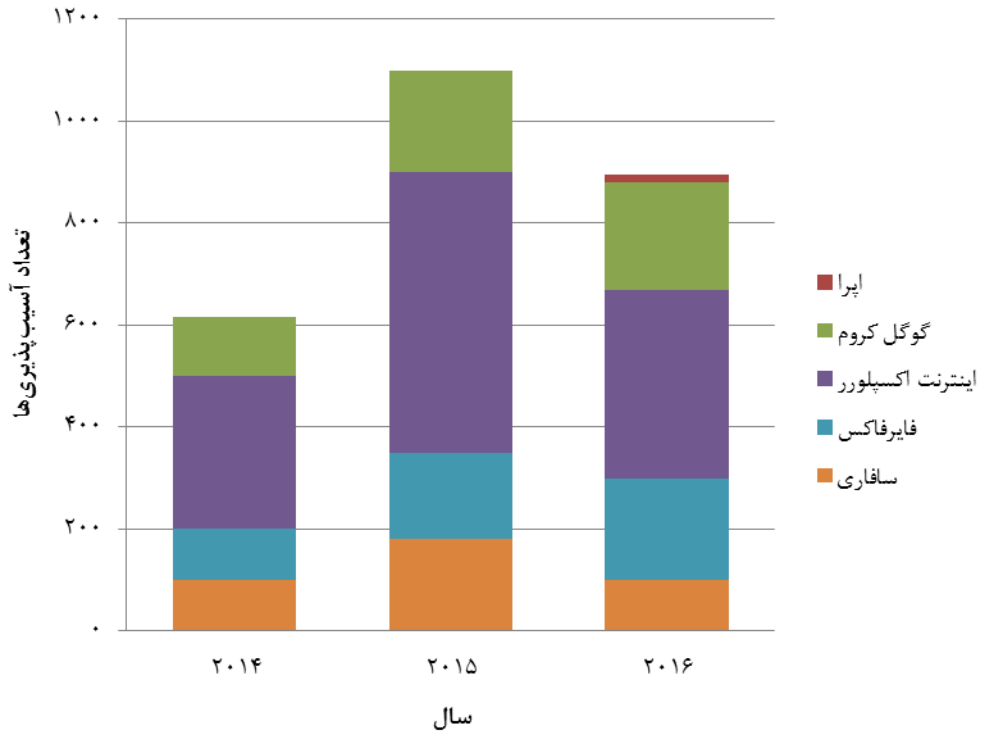
کاربران نهایی اغلب از اینترنت برای وب‌گردی و مشاهده‌ی صفحات وب استفاده می‌کنند و بدین منظور از مرورگرهای اینترنتی مانند فایرفاکس[۲۴]، کروم[۲۵] و غیره بهره می‌گیرند. همان‌طور که در تصویر ۱ مشخص شده است، آسیب‌پذیری‌های موجود در مرورگرها و افزونه‌های آن‌ها یکی از دسته‌های رایج آسیب‌پذیری‌هایی است که می‌تواند توسط حمله‌کنندگان مورد استفاده قرار گیرد [۱].



تصویر ۱ – دسته‌بندی حملات امنیتی بر روی اینترنت

طبق گزارش سیمنتک[۲۶] که در سال ۲۰۱۶ منتشر شده است ۷۸ درصد وب‌سایت‌ها، آسیب‌پذیری‌های بسیار حیاتی دارند و با استفاده از این آسیب‌پذیری‌ها، کدهای مخرب بدون تعامل کاربر اجرا شده و می‌تواند منجر به آسیب‌پذیری‌های جبران‌ناپذیری شوند [۵]. در تصویر ۲ تعدادی آسیب‌پذیری‌های موجود در مرورگرهای مختلف در سه سال اخیر نشان داده شده است.

[23] URL
[24] Firefox
[25] Chrome
[26] Symantec



تصویر ۲ ° آسیب‌پذیری‌های موجود در مرورگرهای مختلف

رشد آسیب‌پذیری‌های موجود در مرورگرها و افزایش روند گسترش استفاده از اینترنت در سال‌های اخیر و وجود نقطه‌ضعف در سازوکارهای امنیتی مانند ضدویروس‌ها، دیواره‌های آتش و غیره، سبب شده است که حمله‌کنندگان بتوانند با استفاده از نقطه‌ضعف‌ها و هم‌چنین آسیب‌پذیری‌های موجود در مرورگرها، کدهای خود را بر روی رایانه و یا ابزار کاربر نهایی اجرا کنند. سازمان‌ها و شرکت‌های بزرگ دنیا نیز از این چالش مستثنی نبوده‌اند. در سال ۲۰۱۰، گوگل[۲۷]، یکی از بزرگ‌ترین شرکت‌های کامپیوتری، اعلام کرد که قربانی حمله‌ی سازمان‌دهی شده‌ی گروهی از نفوذگر[۲۸]های چینی قرار گرفته است. حملات موفق دیگری توسط همان گروه به سازمان‌های دیگر مانند یاهو[۲۹]، ادوبی[۳۰] و غیره نیز انجام شد. این حمله که یکی از بزرگ‌ترین حملات رایانه‌ای ثبت‌شده در تاریخ است با استفاده از ضعف امنیتی در مرورگرهای کارمندان آن سازمان‌ها انجام شد [۲].

حمله‌کنندگان با استفاده از آسیب‌پذیری مرورگرها، اقدام به اجرای کد دلخواه خود و بدافزارها بر روی یارانه‌های کاربران نهایی می‌کنند. این بدافزارها با ربودن اطلاعات حساس و محرمانه‌ی کاربران مانند اطلاعات مرتبط با تصدیق هویت و اطلاعات مالی این کاربران، اقدام به سوءاستفاده‌های مالی می‌کنند.

[27] Google
[28] Hacker
[29] Yahoo
[30] Adobe

برخی از راه‌کارهای به‌کار گرفته شده

در سال‌های اخیر، کارشناسان برای کاهش اثرات ناشی از چنین حملاتی روش‌هایی را پیشنهاد کرده‌اند. استفاده از سیستم‌عامل و مرورگرهای کاملا به‌روزرسانی‌شده، هر چند خطرات را کاهش می‌دهد ولی در مورد حملات روز صفر[31]، اثر چندانی ندارد.

استفاده از سازوکارهای امنیتی مانند ضدویروس، دیواره‌ی آتش و غیره نیز یکی از روش‌هایی است که برای کاهش خطرات ناشی از این حملات پیشنهاد می‌شود، ولی همان‌طور که گفته شد، این سازوکارهای امنیتی نیز نقطه‌ضعف‌هایی دارند که قادر نخواهند بود اطمینان‌خاطر کاملی را برای کاربران نهایی فراهم آورند.

در سال‌های اخیر فن‌آوری‌هایی مبتنی بر جداسازی، برای افزایش امنیت کاربران ارائه شده است. برای نمونه در این روش‌ها و بسته به نوع حساسیت آن‌ها ممکن است تراکنش‌های مالی کاربران از طریق سامانه‌هایی انجام شود که با آن سامانه‌ها، کارهای روزمره‌ی دیگر مانند وب‌گردی و غیره انجام نمی‌شود. این روش‌ها نیز اثرات ناشی از این خطرات را کاهش می‌دهند.

با رشد مفاهیم مرتبط با مجازی‌سازی، استفاده از این روش‌ها نیز برای امن‌سازی موردتوجه قرار گرفته است. جداسازی میزکار، یکی از روش‌های جداسازی است که استفاده می‌شود. یک ماشین مجازی بر روی یک کارگزار[32] مجازی اجرا می‌شود و در واقع این ماشین مجازی از سیستم کاربر نهایی دور می‌ماند. این روش هر چند می‌تواند از دسترسی بدافزار به داده‌های موجود بر روی دستگاه کاربر جلوگیری به عمل آورد، ولی معایبی نیز دارد. از جمله این‌که اگر محیط میزکار مجازی مزبور در اثر وب‌گردی کاربر آلوده شود، این آلودگی بر روی این محیط باقی می‌ماند و می‌تواند با استفاده از ربودن اطلاعاتی که در مراجعه‌های بعدی وارد می‌شود، اقدام به سوءاستفاده نماید. به‌علاوه در این روش بدافزارها به اطلاعات موجود بر روی ماشین مجازی دسترسی دارند.

روش تحقیق

در این قسمت از مقاله ابتدا عملکرد سیستم‌هایی که بر مبنای جداسازی وب کار می‌کنند، مورد بررسی قرارگرفته و معماری آن‌ها ترسیم می‌شود و سپس تعدادی از محصولاتی که از این رویکرد استفاده کرده‌اند مانند فایرگلس[33] و BankVault معرفی شده‌اند.

جداسازی وب

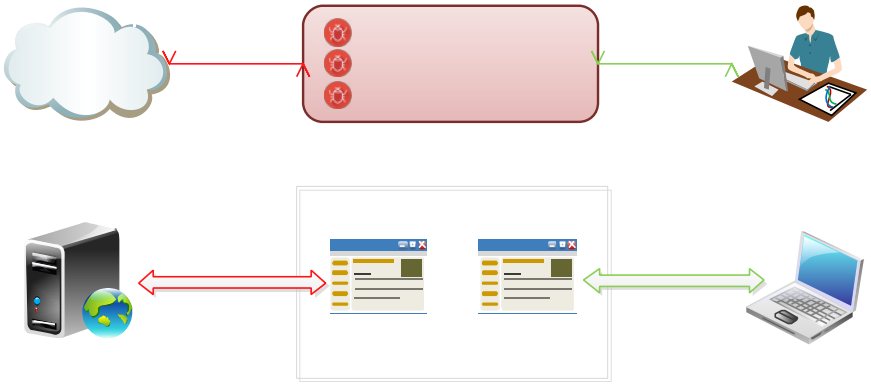
جداسازی وب که گاهی از آن به‌عنوان جداسازی از راه‌دور مرورگر نیز یاد می‌شود، یکی از رویکردهای تکامل‌یافته‌ی جداسازی است. بنابر گزارش گارتنر، این رویکرد حفاظتی یکی از برترین فن‌آوری‌های امنیتی در دو سال اخیر بوده است [۴] و پیش‌بینی می‌شود که در چهار سال آینده رشد استفاده از فن‌آوری‌های مبتنی بر جداسازی وب تا ۵۰ درصد افزایش یابد.

در این روش با ایجاد شکاف، بین وب و کاربر، از کاربر در مقابل مخاطراتی که ممکن است اثرات نامطلوبی بر روی دستگاه

[31] Zero-day
[32] Server
[33] Fireglass

کاربر ایجاد کند، محافظت به عمل می‌آید. درخواست کاربر به یک محیط جداسازی‌شده ارسال می‌گردد. به این محیط گاهی کانتینر[۳۴] (ظرف) مجازی گفته می‌شود.

کدهای دریافت‌شده از وب، در این محیط اجرا می‌شود و سپس به‌صورت جریانی امن و قابل نمایش از داده‌ها، به دستگاه کاربر نهایی ارسال شده و در آن‌جا نشان داده می‌شود. در تصویر ۳، نمایشی از این مفهوم قابل رویت است.



تصویر ۳ ° ارتباط با اینترنت از طریق مرورگر جداسازی‌شده

کدهای مربوط به یک وب‌سایت و یا پست‌الکترونیک[۳۵] و فایل‌های دریافت‌شده به‌جای آن‌که روی دستگاه کاربر اجرا شود در این محیط اجرا می‌شود. اطلاعات دیداری به سمت نقطه‌ی نهایی (دستگاه کاربر) ارسال می‌گردد و عملیات موش‌واره[۳۶] و صفحه‌کلید[۳۷] به سمت این ناحیه‌ی محافظت‌شده ارسال می‌شود. در پایان، این محیط به همراه تمامی بدافزارهای احتمالی آن متلاشی می‌گردد و در این بین، اگر وب‌سایت مزبور آلوده باشد، حمله‌کننده هیچ دسترسی به سیستم کاربر و داده‌های حساس روی آن نخواهد داشت.

تنظیمات مرورگر کاربر به‌گونه‌ای است که برای استفاده از سامانه‌های قابل‌اعتماد در لیست سفید[۳۸]، مثل CRM، درخواست از طریق مرورگر به وب ارسال می‌شود، ولی اگر نشانی درخواستی کاربر، در لیست سفید وجود نداشته باشد، درخواست به سمت محیط حفاظت‌شده ارسال شده و سپس بیرون از شبکه‌ای که کاربر در آن قرار دارد، درخواست به سمت کارگزار ارسال می‌شود و فقط تصویر نتیجه برای کاربر برگشت داده می‌شود. وقتی که می‌گوییم تصویر نتیجه ارسال می‌گردد، ممکن است این برداشت به وجود آید که کاربر بین حالتی که از پروکسی استفاده می‌کند و حالتی که استفاده نمی‌کند، تفاوتی احساس

[34] Container
[35] Email
[36] Mouse
[37] Keyboard
[38] White list

خواهد کرد. در حالی‌که این‌گونه نیست. محیط حفاظت‌شده، نتیجه را به‌گونه‌ای برای کاربر نهایی ارسال می‌کند که کاربر هم‌چنان می‌تواند بر روی بخش‌های مختلف صفحه‌کلید کلیک و درخواست جدیدی را ایجاد کند. در واقع کاربر متوجه‌ی استفاده از مرورگر راه‌دور نخواهد شد.

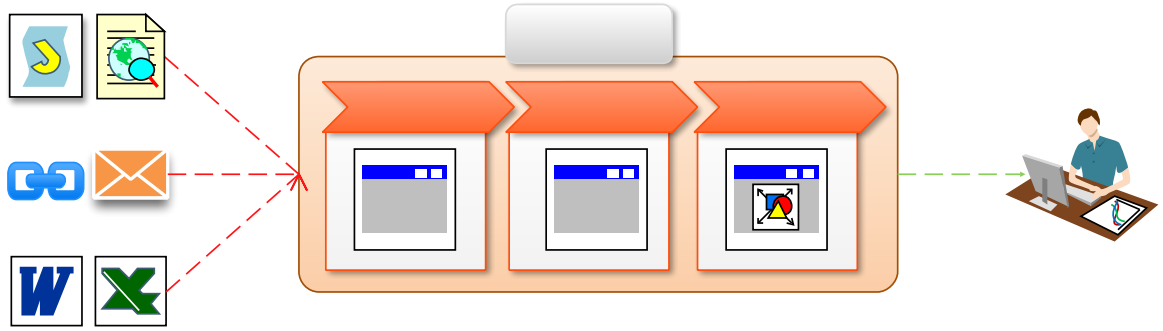
تفاوت عمده‌ای که روش جداسازی مرورگر با مجازی‌سازی میزکار دارد، آن است که در روش‌های مجازی‌سازی مانند میزکار، شما کل رایانه را از کاربر دور کرده‌اید اما در روش‌های جداسازی مرورگر، شما مرورگر را به یک محیط دیگر منتقل کرده‌اید. در این روش می‌توان مستندات را از اینترنت بارگیری[39] کرده و به‌صورت از راه‌دور دید. هم‌چنین این مستندات می‌توانند در فضای ابری[40] جدا از سیستم و داده‌های حساس کاربر ذخیره شوند و در مواقع لزوم مورد استفاده قرار گیرند. حتی در صورتی که کاربر نیاز به دسترسی مستقیم به مستندات داشته باشد، می‌تواند با به‌کارگیری روش‌های امن آن را به سیستم خود منتقل کند.

برخی از محصولات مبتنی بر جداسازی وب

همان‌طور که گفته شد، طبق گزارش گارتنر، روش‌های مبتنی بر جداسازی وب جزء ده فن‌آوری برتر امنیتی استفاده شده هستند. در این سال‌ها، بسیاری از استارتاپ[41]های جدید، محصولات و روش‌هایی مبتنی بر این فن‌آوری ارائه نموده‌اند. آشنایی با این محصولات و ویژگی‌های آن‌ها، به شناخت بهتر این روش و جداسازی وب کمک می‌کند.

- فایرگلس، در جولای ۲۰۱۷، شرکت سیمنتک اعلام کرد که استارتاپ فایرگلس را با قیمت ۲۵۰ میلیون دلار خریداری کرده است. این خبر خود به تنهایی، تاییدکننده‌ی اهمیت موضوع پیش‌بینی گارتنر برای استفاده‌ی هر چه بیش‌تر روش‌های مبتنی بر جداسازی وب در چهار سال آینده است. فایرگلس ارائه‌دهنده‌ی روش مبتنی بر پروکسی برای جداسازی وب می‌باشد. همان‌طور که در تصویر ۴ نشان داده شده است، در این محصول شرکت سیمنتک، با استفاده از روش جداسازی وب، محتوای دریافت‌شده از اینترنت پس از دریافت و اجرا، دوباره برای نمایش آماده شده و به‌صورت امن تحویل کاربر می‌شود.

[39] Download
[40] Cloud
[41] Startup



تصویر ۴ ° راه‌کار جداسازی وب در محصول فایرگلاس شرکت سیمنتک

- یکی دیگر از استارتاپ‌هایی که در سال گذشته خبرساز شد، استارتاپی با عنوان BankVault بود که در ژوئن ۲۰۱۶ به‌عنوان برترین استارتاپ در زمینه‌ی فین‌تک در دره‌ی سیلیکن[۴۲] شناخته شد. این شرکت استرالیایی اکنون دارای دو محصول BankVault و SafeWindow می‌باشد که هر دو محصول نیز به کمک روش‌های مبتنی بر جداسازی وب، به افزایش امنیت تراکنش‌های مالی برخط[۴۳] کاربران کمک می‌کنند.

یافته‌ها و نتایج

همان‌طور که در بخش‌های قبل تشریح شد، در روش جداسازی مرورگر، با ایجاد فضایی بین سیستم کاربر و امکان دسترسی بدافزارها به داده‌های محرمانه‌ی کاربران از بین می‌رود. در این بخش به برخی از مزایای این روش در مقایسه با روش‌های دیگر می‌پردازیم.

- این روش محدودیت‌های خاصی را برای کاربر نهایی ایجاد نمی‌کند. در واقع کاربر تفاوتی را احساس نمی‌کند و همان‌طور که قبلا از مرورگر دستگاه خود برای انجام تراکنش‌های مالی استفاده می‌کرد. باز هم از مرورگر خود استفاده می‌کند و در واقع نیازی به نصب برنامه و یا استفاده از روش‌های مجازی‌سازی بر روی سیستم خود ندارد. سادگی استفاده از این روش برای کاربران نهایی مزیت عمده‌ای به حساب می‌آید.

- با استفاده از روش‌های مبتنی بر جداسازی وب، امکان پنهان کردن هویت کاربر در وب فراهم می‌شود. این مورد یکی از ویژگی‌های برخی از محصولات ارائه‌شده در این زمینه است. در این روش کاربر از طریق یک پروکسی میانی به کارگزار برای انجام تراکنش‌های خود متصل می‌شود. بنابراین اطلاعات نقطه‌ی پایانی[۴۴] پنهان می‌ماند. پنهان ماندن اطلاعات نقطه‌ی پایانی می‌تواند به بالا بردن امنیت تراکنش‌های مالی کمک کند.

[42] Silicon valley
[43] Online
[44] End point

- از آن‌جایی که روش‌های مبتنی بر جداسازی وب از روش‌های مجازی‌سازی مبتنی بر کانتینر لینوکس[45] و داکر[46] استفاده می‌شود. در مقایسه با روش‌هایی که از مجازی‌سازی سیستم‌عامل‌ها استفاده می‌کنند تاثیر بسیار ناچیزی بر روی بازدهی می‌گذارد. این مطلب به حدی ناچیز است که اثر آن بر روی کاربر ملموس نخواهد بود.

- روش‌های مبتنی بر جداسازی، برخلاف سازوکارهای مبتنی بر ضدویروس و دیواره‌های آتش که بیش‌تر در مقابل حملات شناخته‌شده عمل می‌کنند، در مقابل حملات روز صفر نیز کار می‌کنند. از آن‌جایی که محیط حفاظت‌شده‌ی واسط که کدهای دریافت‌شده بر روی آن اجرا می‌شود پس از اتمام نشست به کلی از بین می‌رود حتی در صورتی که در اثر آلودگی ناشی از بدافزارها، آلوده شده باشد، در نشست‌های بعدی اثری از آلودگی باقی نخواهد ماند.

جمع‌بندی

استفاده از روش‌های مبتنی بر جداسازی مرورگر، که در این کار پژوهشی به بررسی آن پرداخته شده است، یکی از فن‌آوری‌های امنیتی است که دو سال گذشته محبوبیت زیادی پیدا کرده است و طبق نظر مراجع معتبر، پیش‌بینی می‌شود که استفاده از این گونه روش‌ها، در سال‌های آتی رشد چشم‌گیری هم داشته باشد. با استفاده از این روش‌ها، به کمک جداسازی سیستم کاربر و محیط اجرای مرورگر، از خطرات ناشی از بدافزارها جلوگیری به عمل می‌آید. مراقبت از داده‌های کاربران تاثیر به‌سزایی در کاهش جرایم مالی مرتبط با تراکنش‌های برخط خواهد داشت.

با وجود به وجود آمدن استارتاپ‌های مرتبط با این موضوع در چند سال اخیر در کشورهای مختلف دنیا، استفاده از این رویکردها در استفاده از محصولات و روش‌های مشابه در کشورمان می‌تواند اثرات چشم‌گیری در افزایش امنیت کاربران و کاهش سوءاستفاده‌های مالی مرتبط با آن داشته باشد.

منابع

[1] It's Time to Isolate Your Users From the Internet Cesspool With Remote Browsing. (September 2016). *Gartner, Inc*. Analyst: Neil MacDonald.
[2] Top Benefits of Isolated Remote Browsing. (2016). *Citrix Systems, Inc*. White Paper.
[3] SANS 2016 Survey on Security and Risk in the Financial Sector. (October 2016). *SANS Institute InfoSec Reading Room.* Written by G. Mark Hardy.
[4] A new paradigm to Threat Prevention: Fireglass Web Isolation technologies. Digital & Business Disruption. (September 2017). *Symantec Corporation World Headquarters.* Indonesia.
[5] Internet Security Threat Report ISTR Government. (June 2017). *Symantec Corporation World Headquarters* (Volume 22). United Stated of America.

[45] Linux
[46] Docker