بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

تبعات احتمالی نفوذ به FireEye برای سازمان‌ها و شرکت‌های کشور

هشدار

شناسه سند	MaherReport_13990922-01
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۳۹۹/۰۹/۲۲
طبقه‌بندی سند	عادی

تهران، خیابان شهید بهشتی، نرسیده به قائم مقام فراهانی، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰

(۰۲۱) ۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

۱ هک شدن شرکت FireEye و تبعات آن

شرکت FireEye یکی از بزرگ‌ترین نام‌های دنیا در عرصه امینت شبکه و فضای سایبری است که با بسیاری از شرکت‌های مهم دنیا همکاری دارد و امنیت شبکه آنها را تامین می‌کند. اما این شرکت اخیرا اعلام کرده است که توسط یک تیم بسیار قدرتمند مورد تهاجم سایبری قرار گرفته است. در نتیجه این حمله، برخی از خطرناک‌ترین ابزارهای امنیتی دنیا به سرقت رفته است.

مدیر عامل FireEye در بیانات خود اظهار داشت "با توجه به ۲۵ سال حضور در امنیت سایبری و پاسخگویی به حوادث، به این نتیجه رسیده‌ام که شاهد حمله یک کشور با بالاترین سطح تهاجمی هستیم. این حمله متفاوت از ده‌ها هزار حمله‌ای است که در طول سال‌ها به آنها پاسخ داده‌ایم. مهاجمان توانایی‌های خود را به طور مشخص برای هدف قرار دادن و حمله به FireEye تقویت کرده‌اند. آنها در زمینه امنیت بسیار آموزش دیده هستند و حمله را با نظم و تمرکز اجرا می‌کنند. مهاجمان از روش‌هایی استفاده کرده‌اند که ابزارهای امنیتی و ابزارهای forensic را مخفیانه دور می زنند. همچنین مهاجمان از روش‌های جدیدی استفاده کرده‌اند که ما یا شرکای ما در گذشته این روش‌ها را مشاهده نکرده بودیم."

هکرها موفق به سرقت ابزارهای دیجیتال Red Team شده‌اند که به منظور شناسایی آسیب‌پذیری سیستم‌ها در شبکه مشتریان استفاده می‌شد. با وجود اینکه هیچ یک از ابزارهای به سرقت رفته آسیب‌پذیری روز صفر را اکسپلویت نمی‌کنند اما احتمال اینکه هکرها بخواهند از ابزارهای سرقت شده سوء استفاده کنند وجود دارد. بنابراین شرکت FireEye مجموعه‌ای قوانین Yara، Snort، clamAV، HXIOC را منتشر کرده تا سایرین آمادگی مقابله با حملات احتمالی مبتنی بر ابزارهای سرقت شده Red Team را داشته باشند. توصیه می‌شود مدیران شبکه این قوانین را در سیستم‌های تشخیص نفوذ خود اعمال نمایند، همچنین با توجه به اینکه احتمال به‌روزرسانی این قوانین وجود دارد به صورت مداوم این لینک را بررسی نمایند و قوانین به روزشده را اعمال نمایند.

شرکت FireEye مجموعه‌ای از آسیب‌پذیری‌ها را منتشر کرده است که رفع این آسیب‌پذیری‌ها می‌تواند برای مقابله با اثرات جانبی دزدیده شدن ابزارهای این شرکت مفید باشد. لیست آسیب‌پذیری‌های مذکور در جدول ۱ بیان شده است. توصیه می‌شود، مدیران شبکه این لیست را با دقت بررسی نمایند و در صورتی که آسیب‌پذیری مذکور را رفع نکرده‌اند، اقدام به رفع آن نمایند.

شرکت FireEye مورد نفوذ قرار گرفته و ابزارهای این شرکت اکنون در دست مهاجمان است. بنابراین ضروریست تا مدیران شبکه، سیستم‌های خود را بررسی کنند و اطمینان حاصل کنند که تاکنون مورد حمله واقع نشده باشند. همچنین باید براساس قوانین ارائه شده توسط این شرکت سیستم‌های تشخیص نفوذ خود را قدرتمند

سازند و به صورت مداوم پیگیر خبرهای این شرکت باشند تا در صورت هر گونه اعلام هشدار یا راهکار جدیدی سیستم‌های خود را بهبود ببخشند.

CVE	محصول	نوع آسیب‌پذیری	امتیاز
CVE-2019-11510	Pulse Secure SSL VPNs	دسترسی به فایل دلخواه پیش از احراز هویت (Pre-auth arbitrary file reading)	۱۰
CVE-2020-1472	Microsoft Active Directory	ارتقاء مجوز دسترسی (escalation of privileges)	۱۰
CVE-2018-13379	Fortinet Fortigate SSL VPN	دسترسی به فایل دلخواه	۹,۸
CVE-2018-15961	Adobe ColdFusion	اجرای کد از راه دور	۹,۸
CVE-2019-0604	Microsoft Sharepoint	اجرای کد از راه دور	۹,۸
CVE-2019-0708	Windows Remote Desktop Services (RDS)	اجرای کد از راه دور	۹,۸
CVE-2019-11580	Atlassian Crowd	اجرای کد از راه دور	۹,۸
CVE-2019-19781	Citrix Application Delivery Controller and Citrix Gateway	اجرای کد از راه دور	۹,۸
CVE-2020-10189	for ZoHo ManageEngine Desktop Central	اجرای کد از راه دور	۹,۸
CVE-2014-1812	Windows	ارتقاء مجوز دسترسی محلی	۹
CVE-2019-3398	Confluence	اجرای کد از راه دور (احراز هویت شده)	۸,۸
CVE-2020-0688	Microsoft Exchange	اجرای کد از راه دور	۸,۸
CVE-2016-0167	Microsoftنسخه‌های قدیمی از Windows	ارتقاء مجوز دسترسی محلی	۷,۸
CVE-2017-11774	Microsoft Outlook	اجرای کد از راه دور	۷,۸
CVE-2018-8581	Microsoft Exchange Server	ارتقاء مجوز دسترسی محلی	۷,۴
CVE-2019-8394	ZoHo ManageEngine ServiceDesk Plus	آپلود فایل دلخواه پیش از احراز هویت (Arbitrary pre-auth file upload)	۶,۵