ویکی‌پدیا
دانشنامهٔ آزاد

تهدیدهای پیشرفته و مستمر

از ویکی‌پدیا، دانشنامهٔ آزاد

پیشرفته مستمر (Advanced persistent threat) منظور روش‌های پیشرفته و معمولاً مخفی برای بدست آوردن مستمر اطلاعات در مورد فرد یا گروهی از افراد از جمله دولت‌های خارجی است.

در حوزه امنیت اطلاعات، منظور زیرمجموعه‌ای از هاست که در یک الگوی دراز مدت حملات نفوذی پیچیده علیه دولت‌ها، شرکت‌ها و فعالان سیاسی استفاده می‌شود. این اصطلاح به گروهی که پشت این حملات است نیز اشاره می‌کند. تصور غلط رایج دربارهٔ APT این است که این نوع‌ها به‌طور ویژه دولت‌ها را هدف قرار داده‌است. فناوری ('اینترنتی') APT توسط حمله کنندگان در بسیاری از کشورها استفاده می‌شود به عنوان وسیله‌ای برای جمع‌آوری اطلاعات از فرد، گروه و افراد مشخص.[۱][۲][۳] گفته می‌شود که برخی از گروه‌های درگیر در APT توسط منابع متعدد دولتی به‌طور مستقیم یا غیرمستقیم حمایت می‌شوند.[۴][۵][۶]

تعاریف

تعریف متفاوتی از APT ارائه شده‌است. اما می‌توان بر اساس اجزای نام آن را توضیح داد:[۷]

-- بدین معنی است که سطحی از همکاری انسان‌ها در انجام این حملات وجود دارد به جای اینکه برنامه کامپیوتری به‌طور خودکار انجام دهند. عاملین یک هدف خاص دارند و ماهر، با انگیزه، سازمان یافته و خوب تأمین شده هستند.

پیشرفته -- حمله کنندگان در پشت از طیف کاملی از تکنیک‌های جمع‌آوری اطلاعات استفاده می‌کنند. این ممکن است شامل تکنیک‌های پیشرفته نفوذ باشد، اما همچنین ممکن است شامل تکنیک‌های جمع‌آوری اطلاعات متداول از قبیل فناوری‌های استراق سمع تلفن و تصویربرداری ماهواره‌ای باشد. در حالی که بعضی از ابزار حمله ممکن است «پیشرفته» دسته‌بندی نشوند (مثلاً نرم‌افزارهای مخرب معمول که در دسترس عموم است) ولی عاملین حمله معمولاً امکان دسترسی و توسعه بیشتر ابزارهای پیشرفته مورد نیاز را دارند. آن‌ها از روش‌ها و ابزار مختلف حمله جهت رسیدن به هدف خود استفاده می‌کنند.

مستمر -- عاملین حمله هدف خاصی را در اولویت قرار می‌دهند و به دنبال بدست آوردن نفع مالی فوری نیستند. این نوع‌ها نشان بر این است که حمله کنندگان توسط موجودیتهای پشت پرده هدایت می‌شوند. حمله از طریق نظارت مستمر و تعامل به منظور دستیابی به اهداف تعریف شده‌است. منظور حملات مداوم و به روز رسانی نرم‌افزارهای مخرب نیست. در واقع روش «آهسته و پیوسته» روش معمولاً موفق تری است.

منابع

۱. An Evolving Crisis" (http://www.busine" ssweek.com/magazine/content/08_16/b4080032220668.htm). BusinessWeek. April 10, 2008. Retrieved ۲۰۱۰-۰۱-۲۰.

۲. The New E-spionage Threat" (http://w" ww.businessweek.com/magazine/content/08_16/b4080032218430.htm). BusinessWeek. April 10, 2008. Retrieved ۲۰۱۱-۰۳-۱۹.

۳. Google Under Attack: The High Cost" of Doing Business in China" (http://www.spiegel.de/international/world/0,1518,672742,00.html). Der Spiegel

۴. Under Cyberthreat: Defense" Contractors" (http://www.businessweek.com/technology/content/jul2009/tc20090076_873512.htm). BusinessWeek. July 6, 2009. Retrieved ۲۰۱۰-۰۱-۲۰.

۵. Understanding the Advanced" Persistent Threat" (http://tominfosec.blogspot.com/2010/02/understanding-apt.html). Tom Parker. February 4, 2010. Retrieved ۲۰۱۰-۰۲-۰۴.

۶. Advanced Persistent Threat (or" Informationized Force Operations)" (http://www.usenix.org/event/lisa09/tech/

8,0172742,00.html). Der Spiegel. 01/19/2010. Retrieved ۲۰۱۰-۰۱-۲۰. Check (date values in: |date= (help
K. Daly. November 4, 2009. Retrieved ۲۰۰۹-۱۱-۰۴.
۷. What's an APT? A Brief Definition" (ht" tps://web.archive.org/web/20100324133007/http://www.damballa.com/solutions/advanced-persistent-threats.php).
slides/daly.pdf) (PDF). Usenix, Michael
Damballa. January 20, 2010. Archived from the original (http://www.damballa.com/solutions/advanced-persistent-threats.php) on 24 March 2010. Retrieved 2010-01-20.