

کرم موریس: اولین حمله سایبری بزرگ در اینترنت

محمدحسین عباسپور^۱، فرزانه رحمانی^۲ و ابوالفضل دیانت^۳

^۱ دانشجوی کارشناسی مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، آدرس پست الکترونیکی: m_abbaspoor80@comp.iust.ac.ir

^۲ دانشجوی کارشناسی مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، آدرس پست الکترونیکی: farzan_rahmani@comp.iust.ac.ir

^۳ استادیار دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران، آدرس پست الکترونیکی: adiyanat@iust.ac.ir

چکیده

کرم موریس^۱ یا کرم اینترنتی یکی از قدیمی‌ترین کرم‌های رایانه‌ای است که از طریق اینترنت توزیع شده است و اولین موردی است که توجه رسانه‌های اصلی را به خود جلب کرده است. این کرم منجر به اولین محکومیت جنایی در ایالات متحده بر اساس قانون تقلب و سوء استفاده رایانه ای^۲ در سال ۱۹۸۶ شد. این بدافزار توسط یک دانشجوی فارغ التحصیل در دانشگاه کورنل، رابرت تاپان موریس^۳، نوشته شد و در ساعت ۸:۳۰ بعد از ظهر ۲ نوامبر ۱۹۸۸، از شبکه موسسه فناوری ماساچوست^۴ راه اندازی شد.

۹

کلمات کلیدی

کرم موریس، حمله سایبری، اینترنت، بدافزار، امنیت رایانه، قانون کلاهبرداری و سوء استفاده رایانه ای.

۱ مقدمه

ماشین‌های متصل به اینترنت آن زمان را آلوده کرده است که در آن زمان تعداد بسیار زیادی بود.

کرم موریس یک برنامه خود تکرارشونده بود که از آسیب‌پذیری‌های سیستم‌های یونیکس^۵ برای انتشار در شبکه‌های رایانه‌ای استفاده می‌کرد. با این حال، به دلیل یک خطای کدنویسی، کرم به صورت نمایی تکثیر شد و باعث آسیب غیرمنتظره و گسترده شد.

کد این کرم شامل چندین مؤلفه بود. ابتدا، سعی کرد از یک آسیب‌پذیری در دیمنون انگشتی^۶ سوء استفاده کند که اجرای دستور از راه دور را امکان پذیر می‌کرد. اگر شکست می‌خورد، سعی می‌کرد از طریق ضعف در حالت دیباگ برنامه sendmail یونیکس به آن دسترسی پیدا کند. زمانی که کرم وارد یک سیستم می‌شد، یک درب پشتی نصب می‌کرد که کنترل از راه دور آینده را امکان‌پذیر می‌کرد و سپس به جستجوی میزبان‌های آسیب‌پذیرتر برای آلوده شدن می‌پرداخت.

گسترش سریع کرم موریس اختلالات قابل توجهی ایجاد کرد و بر حدود ۶۰۰۰ سیستم رایانه ای در سراسر اینترنت نوبا، از جمله ماشین‌ها در دانشگاه‌های بزرگ، تأسیسات نظامی و مراکز تحقیقاتی تأثیر گذاشت. سیستم‌ها از کار افتادند یا تا حد خزیدن کند شدند و بهره‌وری و تلاش‌های تحقیقاتی را با مشکل مواجه کردند.

تأثیر این کرم با توانایی آن در تکثیر سریع خود، مصرف منابع سیستم و مسدود کردن شبکه‌ها با ترافیک بیش از حد تقویت شد. خسارات ناشی از کرم موریس میلیون‌ها دلار تخمین زده شد که خطرات بالقوه بدافزارهای خودتکثیر شونده و

رشد سریع اینترنت در اواخر دهه ۱۹۸۰ چالش‌های جدیدی را در امنیت رایانه به وجود آورد. یکی از مهم‌ترین رویدادها در این دوره انتشار کرم موریس بود، یک برنامه خود تکرارشونده که باعث اختلال گسترده شد و آسیب‌پذیری‌های سیستم‌های کامپیوتری متصل به هم را برجسته کرد.

کرم موریس که در ۲ نوامبر ۱۹۸۸ توسط رابرت تاپان موریس منتشر شد، نقطه عطفی در تاریخ امنیت سایبری بود. گسترش سریع این کرم که به عنوان یک آزمایش بی‌ضرر برای اندازه‌گیری اندازه اینترنت در نظر گرفته شده بود، آسیب‌پذیری‌های حیاتی را در زیرساخت‌های اولیه شبکه آشکار کرد که پیامدهای قابل توجهی را به دنبال داشت و باعث پیشرفت در اقدامات امنیت سایبری شد.

۲ داستان جذاب و پندآموز کرم موریس

در سال ۱۹۸۸، دنیای دیجیتال با بحرانی مواجه شد که مانند گذشته نبود. یک پروژه تحقیقاتی به ظاهر بی‌ضرر، کرمی که توسط رابرت تاپان موریس، دانشجوی فارغ التحصیل دانشگاه کورنل ایجاد شد، از کنترل خارج شد. این کرم که برای کشف قابلیت‌های اینترنت نوبا طراحی شده بود، به طور ناخواسته از آسیب‌پذیری‌ها در برنامه‌های پرکاربرد سوء استفاده کرد و به سرعت تکرار شد و باعث اختلال گسترده شد. برخلاف ویروس‌ها^۵، که برای انتشار به اقدامات انسانی نیاز دارند، این کرم از طریق اتصالات شبکه خودتکثیر می‌شود و تخمین زده می‌شود ۱۰ درصد از تمام

آسیب‌پذیری سیستم‌های کامپیوتری متصل به هم را نشان می‌دهد.

برای اشتراک‌گذاری و اتصال دانش باقی می‌ماند.

۳ نتیجه‌گیری

کرم موریس یک نقطه عطف مهم در تاریخ امنیت رایانه را رقم زد و آسیب‌پذیری های سیستم‌های متصل به هم و خطرات بالقوه بدافزارهای خود-تکثیر شونده را برجسته کرد. این حادثه راه را برای توسعه اقدامات امنیتی قوی تر و افزایش آگاهی از ملاحظات اخلاقی در برنامه نویسی رایانه ای هموار کرد. درس‌های آموخته‌شده از کرم موریس به تلاش‌های مداوم برای ایمن‌سازی اینترنت و محافظت از زیرساخت‌های حیاتی در برابر تهدیدات سایبری ادامه می‌دهد.

علاوه بر این، کرم موریس به عنوان یک رویداد مهم در تکامل امنیت سایبری است که به عنوان یک داستان هشدار دهنده و یک کاتالیزور برای نوآوری عمل می‌کند. با افشای آسیب‌پذیری‌ها در زیرساخت‌های اولیه اینترنت و ایجاد آگاهی گسترده از خطرات امنیت سایبری، راه را برای پیشرفت‌های قابل توجهی در این زمینه هموار کرد. میراث کرم موریس به عنوان یادآور ضرورت مستمر برای اولویت دادن به امنیت در یک چشم انداز دیجیتالی به طور فزاینده به هم پیوسته باقی می‌ماند.

سپاس‌گزاری

از خداوند متعال بسیار سپاسگزاریم بابت توانی که به ما جهت نوشتن این مقاله اعطاء نمود. از جناب دکتر دیانت که استاد ما در تهیه این مقاله بوده‌اند نیز بسیار تشکر میکنیم. همچنین از خانواده عزیزمان که پشتیبان و موجب دلگرمی ما هستند بینهایت سپاسگزاریم.

مراجع

- [1] Bardoc, Ylee. "Morris worm." Wikipedia, The Free Encyclopedia, en.wikipedia.org/wiki/Morris_worm, 24 Nov. 2023, 22:49 UTC.
- [2] Vacca, J. R. (2017). Computer and Information Security Handbook (3rd ed.). Morgan Kaufmann.
- [3] Kizza, M. (2015). Guide to Computer Network Security (3rd ed.). Springer.
- [4] Hafner, K., & Markoff, J. (1991). Cyberpunk: Outlaws and hackers on the computer frontier. Simon and Schuster.
- [5] Denning, P. J. (Ed.). (1990). Computers under attack: Intruders, worms, and viruses. Addison-Wesley Longman Publishing Co., Inc.
- [6] Orman, H. (2003). The Morris worm: A fifteen-year perspective. IEEE Security & Privacy, 1(5), 35-43.

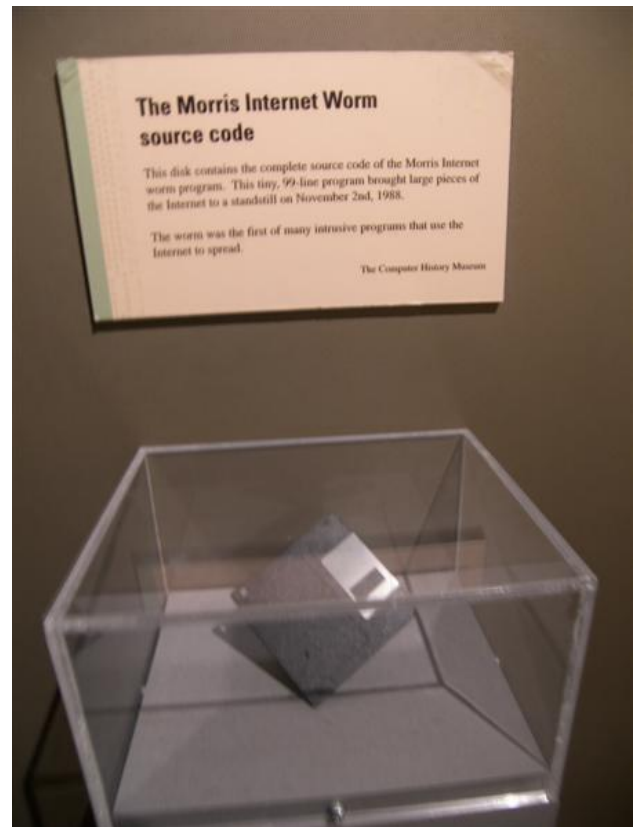
پانویس‌ها

^۱ Morris worm

^۲ Computer Fraud and Abuse Act

^۳ Robert Tappan Morris

^۴ Massachusetts Institute of Technology network



شکل ۱: فلاپی دیسک حاوی کد منبع کرم موریس، در موزه تاریخ کامپیوتر [1]

داستان کرم موریس فقط در مورد هرج و مرج ناشی از آن نیست، بلکه در مورد واکنش زیبای آن نیز است. این حادثه شکنندگی اینترنت و نیاز به اقدامات امنیتی قوی را آشکار کرد. این امر باعث ایجاد دو موسسه مهم شد: مرکز هماهنگی CERT^۱ (CERT/CC) در دانشگاه کارنگی ملون^۲ و گروه منطقه امنیتی نیروی ضربت مهندسی اینترنت (IETF)^۳. سازمان CERT/CC به عنوان یک منبع مرکزی برای هماهنگی تلاش‌های امنیت سایبری ظاهر شد، در حالی که IETF یک گروه اختصاصی برای رسیدگی به آسیب‌پذیری‌های امنیتی در پروتکل‌های اینترنتی ایجاد کرد.

شکار موریس کرم خود گواهی بر روحیه همکاری جامعه اولیه اینترنتی بود. با اطلاعات محدود و ابزارهای ابتدایی، محققان در سراسر جهان به طور خستگی ناپذیری برای درک رفتار کرم و شناسایی منبع آن تلاش کردند. چند روز پس از حمله، تیمی در دانشگاه برکلی کالیفرنیا^۴، کرم را به کامپیوتر موریس در کرنل ردیابی کردند که منجر به محاکمه و محکومیت نهایی او شد.

حادثه کرم موریس به عنوان یادآوری تلخ از تعادل ظریف بین نوآوری و امنیت است. این حادثه پیامدهای ناخواسته ای را که می‌تواند از اقدامات حتی با نیت خوب ناشی شود برجسته می‌کند و بر اهمیت همکاری در حفاظت از دنیای دیجیتال تأکید می‌کند. امروزه، امنیت سایبری به عنوان یک حوزه همیشه در حال توسعه باقی مانده است که دائماً با تهدیدات جدید و پیچیده دست و پنجه نرم می‌کند. با این حال، درس‌های آموخته‌شده از کرم موریس همچنان به توسعه اقدامات امنیتی قوی ادامه می‌دهد و تضمین می‌کند که اینترنت یک پلتفرم^۵ انعطاف‌پذیر و در دسترس

^ΔViruses

[£]Unix

[¥]fingerd daemon

[^]CERT Coordination Center

^ªCarnegie Mellon University

[`]Internet Engineering Task Force (IETF) Security Area Group

^{^^}University of California, Berkeley

^{^^}platform