بدافزارها(قسمت دوم)

# کـــرم یاقـــوت کبـــود

علیرضا قاضی‌سعیدی
کارشناس ارشد فناوری اطلاعات و ارتباطات

**در ادامهٔ مبحث بدافزارها، در این شماره به بررسی دو دستهٔ دیگر از خانوادهٔ بدافزارها یعنی «کرم»[1]ها و «تروجان»[2]ها می‌پردازیم.**

**کلید واژه**: کرمها، تروجان ها، رابرت موریس

## کرمها

بـه عنوان پیشـینه‌ای در مورد کرمها، بد نیسـت اولین خالق کرم اینترنتی دنیا، یا به عبارت بهتر، پدر کرمهـای اینترنتی را معرفی کنیم. رابرت موریس[3] متولد سال 1965 از اعضای دانشگاه MIT ایالات متحده، در سـال 1988 اولین کـرم را بدون اطلاع دقیق از عواقب و اثرات آن روانهٔ شبکهٔ اینترنت کرد.

در واقع هـدف اصلی موریس ایجاد برنامه‌ای پویا و مقاوم به روشـن و خاموش شدن سیستم و فرمت شدن دیسک سخت بود تا بتواند از طریق آن، ابعاد اینترنت را اندازه‌گیری کند. او با این کار تعداد زیادی از رایانه‌های متصل به شبکه را که تعداد آنها در مقایسه با زمان فعلی بسیار کمتر بود، آلوده کرد و به همین دلیل، 10هزار دلار جریمه شد.

امـا چرا برای این بدافزار نام کـرم را انتخاب کرده‌اند؟ چون نمونه‌های نخسـتین آن، مانند کرم با سرعت کمی در سیستم حرکـت می‌کردنـد؛ اگـر چه امروزه سـرعت عملکـرد آنها از ویروس‌ها هم بالاتر رفته است. کرمها برای ورود به سیستم نیازمند هیچ‌گونه میزبانی نیستند و بدون این‌که کاربر کاری در جهت ورود کرم انجام دهد، تنها از طریق آسیب‌پذیریهای سیستم[4] وارد سیستم می‌شوند. از معروف‌ترین کرمهای دنیا می‌توان به کرم («Slammer Sapphire)» که با نام «یاقوت کبود» معروف شد، اشاره کرد. این کرم از سـرعتی فوق‌العاده برخوردار بود، به گونه‌ای که در هر 8/5 ثانیه دو برابر می‌شد. از جمله اهداف مورد حملهٔ این کرم مؤسسات مالی و سیستم‌های ATM بودند.

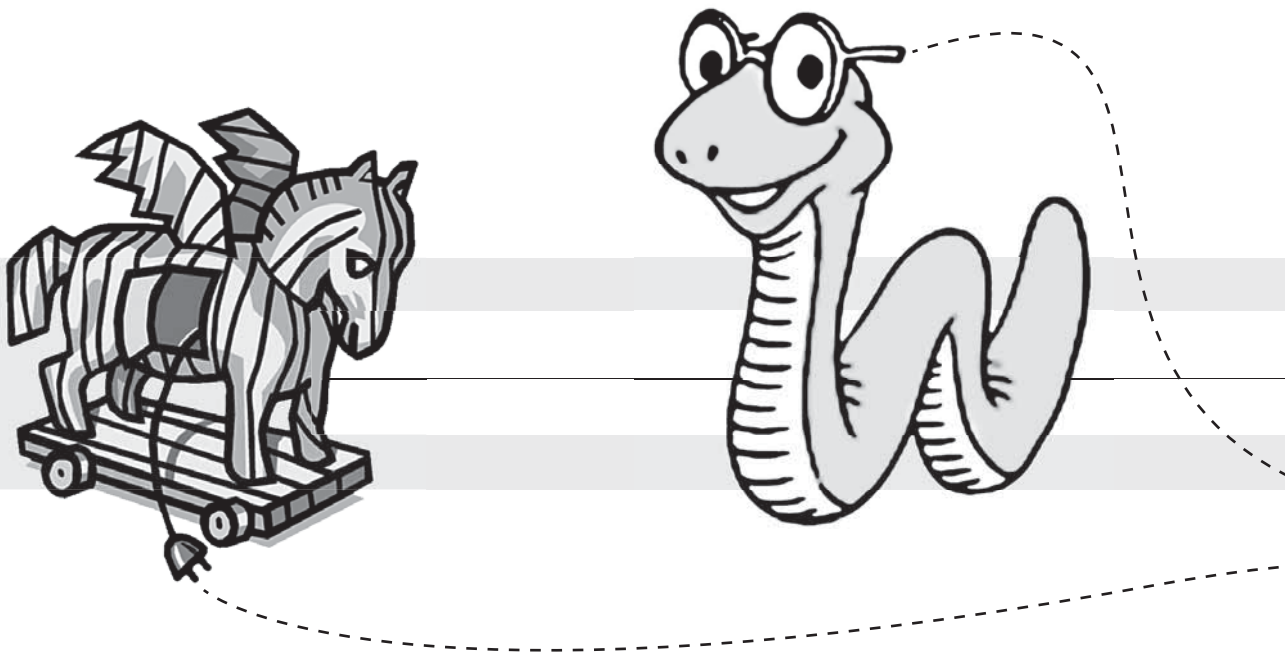
## تروجان‌ها

تروجان‌ها یا اسبهای تروا، برنامه‌های مخرب کوچکی هستند. که به صورت «پنهانی»[5] در سیسـتم قربانی اجرا می‌شـوند و سیستم قربانی را تحت تأثیر قرار می‌دهند. نام‌گذاری این دسته از بدافزارها به داسـتانی از یونان باسـتان اشاره دارد که در آن، شـهری از طریق اسبی چوبی که سربازان دشمن در آن پنهان شده بودند، اشغال شد. در حالی‌که ساکنین شهر ابتدا بر این باور بودند که اسب‌چوبی هدیه‌ای به نشانهٔ پایان جنگ است.

نکتـهٔ مهمی کـه در مورد تروجان‌ها اهمیت دارد این‌اسـت کـه «هکر» می‌تواند به مدد تروجان موجـود در رایانهٔ قربانی، به دزدی «پسـورد»های ذخیره شـده روی سیستم او، خواندن اطلاعـات و مسـتندات فایل‌ها، پاک کـردن اطلاعات و حتی نمایش تصویر و پنجره‌های دلخواه خود بپردازد.

برای توضیح عملکرد تروجان‌ها لازم اسـت دو مفهوم زیر را توضیح دهیم.

1. **کانال آشـکار**[6]: که یک مسـیر ارتباطی قانونی در یک سیستم رایانه‌ای یا شبکه برای انتقال داده به حساب می‌آید.
2. **کانال پنهان**[7]: مسیری برای انتقال داده در سیستم رایانه‌ای و یا شبکه به گونه‌ای که سیاستهای امنیتی زیر پا گذاشته می‌شوند.



در واقع تروجان ساده‌ترین نوع کانال پنهان است.

تروجان‌ها را می‌توان به طور کلی به اقسام زیر تقسیم‌بندی کرد:

- تروجان‌های دست‌رسی از راه دور[8]؛
- تروجان‌های ارسال کنندهٔ اطلاعات[9]؛
- تروجان‌های مخرب[10]؛
- تروجان‌های پروکسی[11]؛
- تروجان‌های پروتکل انتقال فایل[12]؛
- تروجان‌های از کار اندازندهٔ نرم‌افزارهای امنیتی[13]؛

تروجان‌های از راههای زیر وارد سیستم شما می‌شوند:

1. نرم‌افزارهای پیام‌رسان فوری[14]؛
2. ضمائم[15]؛
3. دست‌رسی فیزیکی مهاجم به سیستم[16]؛
4. مشکلات موجود در نرم‌افزارهای ایمیل یا مرورگر[17]؛
5. «اشتراک‌گذاری فایل»[18] که برای مثال می‌توان به «torrent» اشاره کرد که منبع ورود تروجان‌های بسیاری بوده است؛
6. «برنامه‌های جعلی و ساختگی»[19] که از آن جمله می‌توان به بسته‌های نرم‌افزاری امنیتی جعلی و آنتی‌ویروس‌های جعلی اشاره کرد که گاه برای از کار انداختن آنها و یا اثراتشان به مشکل برمی‌خوریم؛
7. سایت‌های غیرقابل اعتماد و برخی نرم‌افزارهای رایگان[20]؛
8. دانلود کردن فایل‌ها، بازیها و محافظ صفحهٔ نمایش از سایت‌های اینترنتی.

در برخی از نرم‌افزارهای امنیتی با واژه‌ای به نام «Rootkit» مواجه می‌شویم که در واقع نوعی تروجان با قابلیت قرارگیری در هستهٔ سیستم عامل است و اثرات مخربی به همراه دارد. چرا که می‌تواند تغییراتی را حتی در سیستم عامل شما ایجاد کند. تروجان‌ها هم‌چنین می‌توانند در نقش «جاسوس‌افزار»[21] یا ردیاب «صفحهٔ کلید»[22] عمل کنند. واژهٔ دیگری که در مورد تروجان‌ها ممکن است با آن مواجه شوید، «Wrapper» است که در واقع نوعی نرم‌افزار برای اتصال تروجان به یک فایل دیگر، مثلاً فایلی از نوع «مالتی مدیا»[23] است. در شماره‌های بعدی روشهای مقابله با بدافزارها و پیشگیری از ورود آنها به سیستم شما به تفصیل بررسی خواهند شد.

## پی‌نوشت

1.worm
2.Trojan
3.Robert Morris
4.Vulnerability
5.hidden
6.Overt channel
7.Covert channel
8.Remote Access Trojan
9.Data-Sending Trojan
10.Destructive Trojan
11.Proxy Trojan
12.FTP Trojan
13.Security Software Disabler
14.Instant Messenger Applications
15.Attachments
16.Physical Access
17.Browser and email software
18.File Sharing
19.Fake Programs
20.Untrusted sites and some Freeware softwares
21.Spyware
22.Key Logger
23.Multi Media