In the name of GOD

Rubber Ducky

Rubber Ducky چیست و روش های ساخت آن در زمان های مختلف از گذشته تا به حال

Hossein Ahmadi

https://MrPython.blog.ir

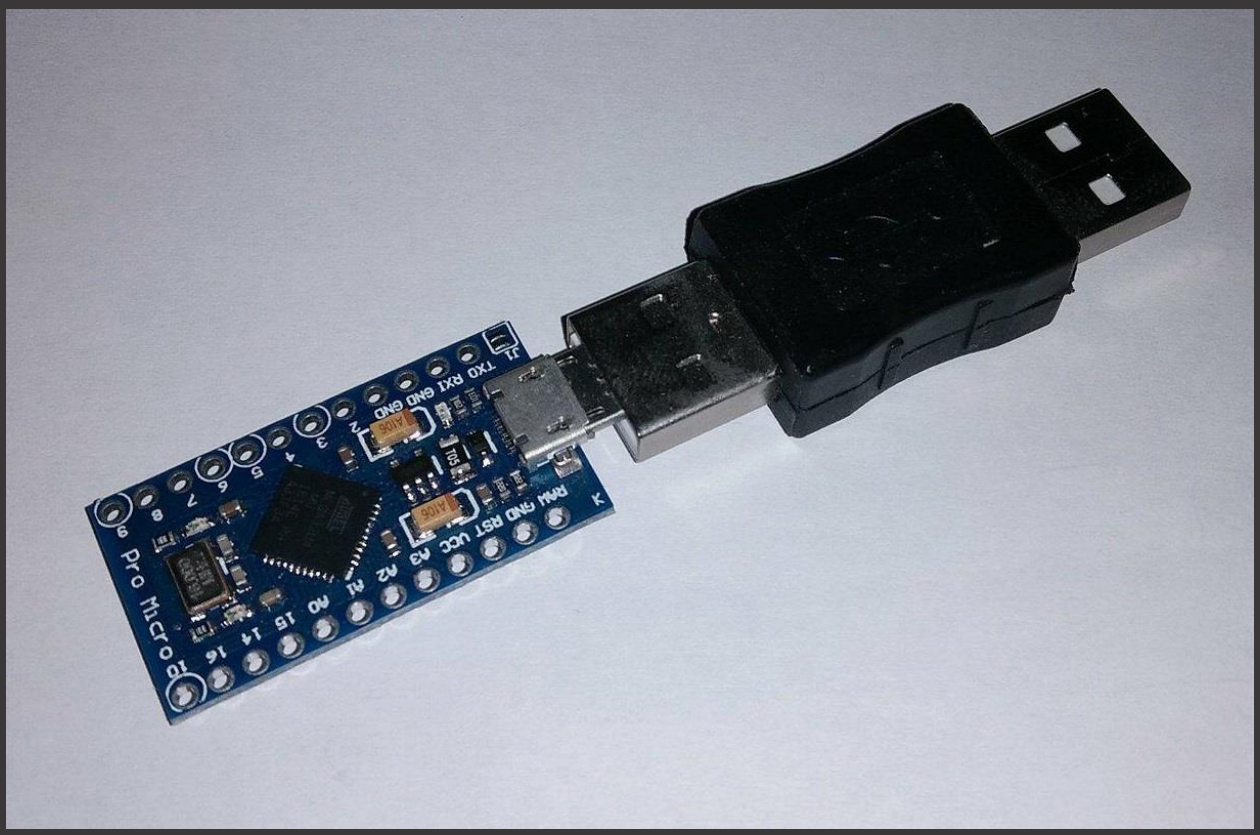
Rubber Ducky چیست ؟

Rubber Ducky یا Bad USB یک برد یا سخت افزار با قابلیت اتصال به کامپیوتر است که به محض وصل شدن به یک کامپیوتر باعث اجرای خودکار دستوراتی روی کامپیوتر هدف میشود که این دستورات از قبل برای او تعیین شده است .

معمولا در فیلم ها و سریال ها این موضوع را مشاهده کردیم که یک شخص با وصل کردن فلش مموری خود به یک کامپیوتر باعث ویروسی کردن یا اجرای یک دستور مخرب روی آن کامپیوتر میشود .

باید به این نکته اشاره کرد که Rubber Ducky فقط در قالب فلش مموری وجود ندارد و میتوان روی بسیاری از سخت افزار های دیگر نیز آن را پیاده کرد .

در دو تصویر که در ادامه آمده است دو Rubber Ducky متفاوت به تصویر کشیده شده اند که یکی از آن ها در قالب یک فلش مموری است و دیگری در قالب یک برد سخت افزاری ساده است .


Pro Micro
TXO RXI GND GND
RAW GND RST VCC A3 A2 A1 A0 15 14 16

از دست یک Rubber Ducky چه کارهایی بر میاید ؟

اگر بخواهیم روی کاربرد Rubber Ducky ها بحث کنیم میتوانیم موارد خیلی زیادی را ذکر کنیم ولی بهتر است روی مشهور ترین موارد بحث کنیم .

اول باید گفت Rubber Ducky ها قابلیت این را دارند که بسیار کاربردی باشند یا برعکس بسیار خطرناک . به عبارتی از Rubber Ducky هم میتوان استفاده ی مثبت کرد و هم استفاده ی منفی . همانطور که در تعریف این برد سخت افزاری گفتیم ، این قابلیت را دارا است که دستوراتی از پیش تعیین شده را به طور خودکار روی سیستم هدف اجرا کند بنابراین میتوان برای اتوماسیون یا خودکار کردن بعضی از کار ها از آن استفاده کرد . برای مثال شما برای پیکربندی یک برنامه خاص روی سیستمتان نیاز دارید تا یک سری دستوراتی را پشت سر هم اجرا کنید . خب شاید این کار زمان بر و حوصله سر بر باشد بنابراین میتوان یک Rubber Ducky درست کرد تا به محض وصل شدن به کامپیوتر تمام این دستورات را به طور خودکار در عرض چند ثانیه اجرا کند . این نمونه کاربرد مثبت این ابزار بود . هزاران مثال دیگر از کاربرد های مثبت این ابزار را میتوانیم ذکر کنیم . همینطور میتوان هزاران استفاده منفی از این ابزار را ذکر کرد .

برای مثال یک مهاجم میتواند با وصل کردن Rubber Ducky به یک سیستم کامپیوتری اقدام به اجرای یک ویروس خاص در سیستم هدف کند . یا مثالی فنی تر بخواهیم بزنیم شما میتوانید Rubber Ducky طراحی کنید که به محض وصل شدن به سیستم هدف شروع به نصب کردن بد افزار در سیستم کند و هزاران کارهای بدتر ...

روش های ساخت Rubber Ducky

باید بدانید که از گذشته تا حالا روش های مختلفی برای ساختن این ابزار وجود داشته است . در زیر روش های مختلف ساخت این ابزار را آورده ایم از گذشته تا به امروز .

1 – روش autorun.inf

خب یکی از قدیمی ترین روش ها برای ساخت Rubber Ducky به دوران ویندوز های XP و قبل تر بر میگردد . همانطور که احتمالا میدانید در آن روز ها قابلیتی در ویندوز های XP و قدیمی تر وجود داشت به نام autorun . این قابلیت به این صورت بود که برای مثال وقتی شما یک دیسک نصب برنامه را داخل سی دی رام میگذاشتید ، بدونه اینکه شما فایل نصب را از روی سی دی اجرا کنید ، فایل نصب به طور خودکار اجرا میشد . اگر بخواهیم فنی تر به این موضوع نگاه کنیم ، طرز کار به این صورت بود که هر دیسکی یا فلش مموری که وارد سیستم شما میشد ، ویندوز دنبال فایلی به اسم autorun.inf روی آن بود . داخل چنین فایلی اطلاعاتی مربوط به خودکار اجرا شدن یک فایل دیگر روی همان

دیسک یا فلش مموری نوشته شده بود . برای مثال شما سی دی بازی مورد علاقه خود را خریده بودید . وقتی شما سی دی را داخل سی دی رام میگذاشتید ، کامپیوتر شما دنبال فایلی به نام autorun.inf روی سی دی بود . آن را پیدا میکرد و داخل این فایل نوشته شده بود که فایل نصب بازی به طور خودکار اجرا شود . نهایتا کامپیوتر شما فایل نصب بازی را به طور خودکار برای شما اجرا میکرد . این طرز کار قابلیت autorun در ویندوز بود . هکر ها از همین موضوع برای اجرای خودکار فایل های ویروسی خود روی سیستم هدف استفاده میکردند . آن ها یک برنامه ی خاصی طراحی میکردند تا فعالیتی هدفمند روی سیستم هدف داشته باشد . سپس این برنامه را روی فلش مموری خود یا دیسک خود کپی میکردند . حال نیاز بود کاری کنند تا وقتی فلش مموری یا دیسک وارد سیستم هدف میشود این برنامه ای که طراحی کرده بودند به طور خودکار اجرا شود . آن ها فایلی به نام autorun.inf روی فلش مموری یا دیسک ایجاد میکردند و داخل آن اطلاعات مربوط به خودکار اجرا شدن برنامه ی طراحی شده را مینوشتند سرانجام با وارد کردن دیسک یا فلش مموری در کامپیوتر هدف ، ویندوز با خواندن فایل autorun.inf میفهمید که باید فایل برنامه ای که هکر طراحی کرده بود را خودکار اجرا کند و این کار را میکرد .

این روشی بود که هکر ها برای اجرای خودکار فایل ها و ساخت rubber ducky در ویندوز های قدیمی تر استفاده میکردند.

در ویندوز های امروزی قابلیت autorun در ویندوز به طور پیشفرض غیرفعال شده است .

2-روش دستکاری چیپست فلش مموری

یکی دیگر از روش های ساخت Rubber Ducky دستکاری چیپست فلش مموری و تغییر رفتار آن هنگام بوت شدن بود . در بعضی از سال ها برخی شرکت هایی که فلش مموری روانه ی بازار میکردند ، فلش مموری های آسیب پذیری را وارد بازار کردند . چند نوع فلش مموری خاص بود که توسط هکر ها شناسایی شده بود که دارای نوعی آسیب پذیری بودند که به هکر اجازه برنامه ریزی مجدد (Re Program) کردن چیپست آن ها را میداد . هکر ها میتوانستند از این آسیب پذیری استفاده کنند و برنامه چیپست فلش مموری را طوری تغییر دهند تا فلش مموری کار هایی که آن ها میخواهند را روی سیستم هدف انجام دهد.

این آسیب پذیری بعد ها در فلش مموری های بعدی رفع شد و فلش مموری های آسیب پذیر دیگر روانه بازار نشدند .

2-روش ساخت دستگاه HID

HID مخفف Human Interface Device به معنای دستگاه رابط انسانی است . به دستگاه هایی که رابط انسانی برای کامپیوتر هستند مثل کیبورد ، موس و ... ، دستگاه های HID میگویند .

از دستگاه های HID میتوان برای اجرای خودکار دستورات روی کامپیوتر استفاده کرد . به عبارتی میتوان با استفاده از آن ها Rubber Ducky درست کرد . حال چرا دستگاه HID برای اینکار مناسب است ؟ همانطور که میدانید دستگاه های HID برای کامپیوتر قابل اطمینان هستند و کامپیوتر نظارتی روی آن ها ندارد . برای مثال وقتی شما کیبوردتان را به کامپیوتر وصل میکنید هیچ آنتی ویروسی آن را برسی نخواهد کرد . هکر میتواند یک برد سخت افزاری درست کند که به عنوان دستگاه HID عمل کند و بتواند کلید های کیبورد را برای کامپیوتر ارسال کند . به عبارتی دیگر نقش یک کیبورد را بازی کند . حال برای مثال اگر هدف یک سیستم ویندوزی باشد ، هکر این برد را طوری برنامه ریزی میکند تا به محض وصل شدن به کامپیوتر ، کلید های ترکیبی Windows + R را بزند تا پنجره ی RUN باز شود .
سپس کلمه ی cmd را تایپ کند و enter را بزند . حال cmd باز شده ، یک کد مخرب بنویسد و باز enter را بفرستد . تمام این اعمال در عرض چند ثانیه توسط برد انجام میشود و به این

صورت به محض وصل کردن برد به کامپیوتر ، کد هایی در cmd اجرا میشود .

این روش ساخت Rubber Ducky با دستگاه های HID بود که خوشبختانه یا متاسفانه هنوز هم روی جدیدترین سیستم عامل ها عملی است و کار میدهد .

در پست های آینده وبلاگ مسترپایتون ، ساخت Rubber Ducky به روش سوم یعنی دستگاه HID را به وسیله ی یک برد Arduino آموزش خواهیم داد . آدرس وبلاگ :

https://MrPython.blog.ir

یا حق !