آزمایشگاه تخصصی آپا، قزوین

دانشگاه بین المللی امام خمینی (ره)

خبرنامه تحلیلی رویدادهای امنیتی (روزانه)

چهارشنبه پانزدهم آبان ماه ۱۳۹۸

کشف آلودگی بدافزاری[1] در دستگاه‌های ذخیره‌سازی تحت شبکه شرکت کیو.اِن.اِی.پی[2]

نسخه ۱,۰,۰

نویسنده : مونا رضا زاده **سردبیر :** محمد پیشدار

[1]-Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

[2]-QNAP Systems, Inc. is a Taiwanese corporation that specializes in Network-attached storage appliances used for file sharing, virtualization, storage management and surveillance applications.

محققان امنیت اطلاعت در مورد وجود یک بدافزار در ابزارهای ذخیره‌سازی شبکه هشدار داده‌اند

تاریخ: ۰۱/ نوامبر / ۲۰۱۹

بررسی اجمالی :

به تازگی یک بدافزار جدید و مخرب با نام کیوسانچ[1] هزاران دستگاه اِن.اِی.اِس[2] (دستگاه ذخیره‌سازی متصل به شبکه) شرکت کیو.اِن.اِپی را مورد هدف قرار داده است. این بدافزار با نفوذ به چارچوب[3] دستگاه قادر به سرقت اطلاعات احراز هویت کاربران و اجرای کدهای مخرب در سیستم آن‌ها خواهد بود. براساس گزارشات تاکنون هفت هزار دستگاه در کشور آلمان و هزاران مورد در مناطق دیگر توسط این بدافزار آلوده شده‌اند [۱].

نگاه کلی :

سیستم‌های آسیب‌پذیر	دستگاه ذخیره ساز شبکه ساخت شرکت کیو.اِن.اِپی شامل کیو.تی.اِس[4] ۴,۲,۶ ساخت ۲۱۰۸۱۲۲۷، کیو.تی.سی ۴,۳,۳ ساخت ۲۰۱۹۰۱۰۲، کیو.تی.سی ۴,۳,۴ ساخت ۲۰۱۹۰۱۰۲، کیو.تی.سی۴,۳,۶ ساخت ۲۰۱۸۱۲۲۸ و نسخه‌های قبل از آن		
شدت خطر	**در دولت**	**در تجارت**	**کاربران خانگی**
	متوسط	**متوسط**	**متوسط**
راه‌های نفوذ	ارسال یک درخواست ساده اِچ.تی.تی.پی[5] با متد گِت[6] به یک مسیر خاص		
هدف	سرقت احراز هویت کاربران و اجرای کدهای غیرمجاز		

[1]-Qsnatch
[2]-Network-attached storage (NAS) is dedicated file storage that enables multiple users and heterogeneous client devices to retrieve data from centralized disk capacity.
[3]-In computer programming, a software framework is an abstraction in which software providing generic functionality can be selectively changed by additional user-written code, thus providing application-specific software.
[4]-QTS
[5]-The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.
[6]-The GET method is used to retrieve information from the given server using a given URI. Requests using GET should only retrieve data and should have no other effect on the data.

توضیحات فنی :

در اواسط اکتبر ۲۰۱۹ مرکز امنیت سایبری فلاند[1] موفق به شناسایی یک بدافزار جدید با نام کیوسانچ در دستگاه‌های ذخیره‌سازس متصل به شبکه یا اِن.اِی.اِس شده است. این دستگاه‌ها متعلق به شرکت تایوانی کیو.اِن.اِپی بوده و تاکنون هزاران ذخیره‌ساز تحت شبکه این شرکت در سراسر دنیا توسط بدافزار مذکور آلوده شده‌اند. طبق گفته محققان، بدافزار کیوسانچ پس از آلوده‌سازی چارچوب دستگاه، نام کاربری و رمز عبور قربانی را سرقت کرده و آن را برای یک خدمت‌رسان فرمان و کنترل[2] تحت اختیار مهاجم ارسال می‌کند [۱].

بدافزار کیوسانچ پس از نفوذ به چارچوب دستگاه قربانی با استفاده از الگوریتم‌های تولید دامنه و ارسال یک درخواست ساده اِچ.تی.تی.پی (با متد گِت) به مسیر زیر کدهای مخرب خود را از سرور فرمان و کنترل دریافت می‌نماید.

https://<generated-address>/qnap_firmware.xml?=t<timestamp”<

پس از انجام این مراحل بدافزار مذکور قادر به انجام اقداماتی مانند دستکاری اسکریپت‌های زمان‌بندی شده در سیستم‌عامل، جلوگیری از بروزرسانی چارچوب، استخراج اطلاعات احراز هویت و ارسال آن‌ها به سرور کنترل و فرمان خواهد بود. تا کنون اطلاعات بیشتری در مورد گسترش این بدافزار منتشر نشده است [۱،۲].

پیشنهادات [۱،۲]

- تغییر تمام رمزهای عبور تعریف شده بر روی دستگاه
- حذف حساب‌های کاربری ناشناس از دستگاه
- نصب بروزرسانی‌های مربوطه
- بازگشت به تنظیمات کارخانه در دستگاه

منابع :

1. Threatpost Website
   https://threatpost.com/malware-targets-qnap-hardware/149796/
2. Zdnet Website
   https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/

[1]-Finland’s National Cyber Security Centre (NCSC-FI)
[2]-A command and control server (C&C server) is a computer that issues directives to digital devices that have been infected with rootkits or other types of malware, such as ransomware.
[2]-An Internet Protocol