The QNapping of QNAP Devices

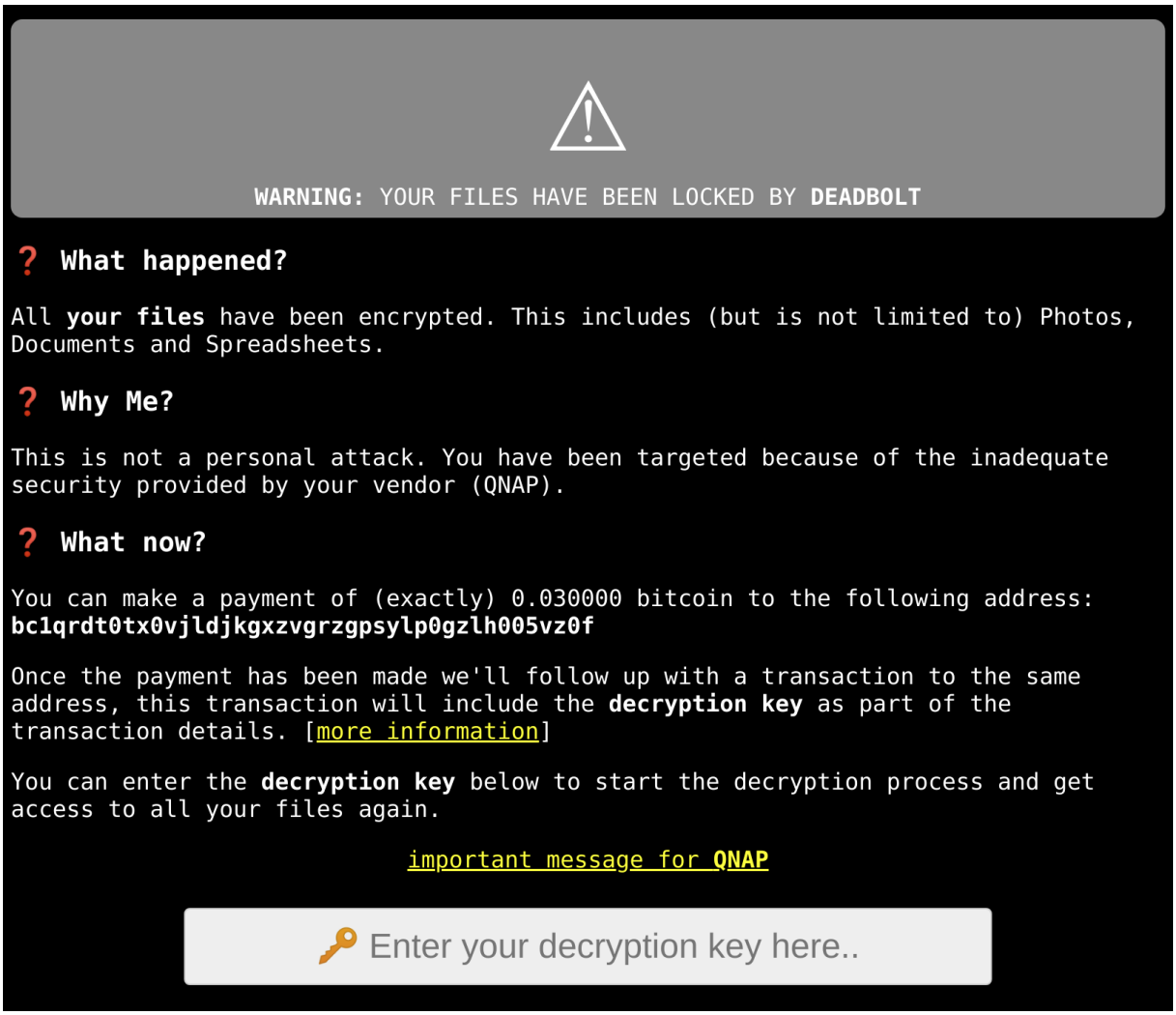
Mark Ellzey Senior Security Researcher
Posted on January 27, 2022

Authors: *Mark Ellzey, Aidan Holland*, *Ryan Lindner*

Introduction

On Jan. 25, 2022, several media outlets reported a ransomware attack targeting the Network Attached Storage (NAS) vendor QNAP. The news circulated soon after QNAP released a warning statement pleading with customers to "fight ransomware together" by disabling features on consumer routers and the QNAP devices themselves.

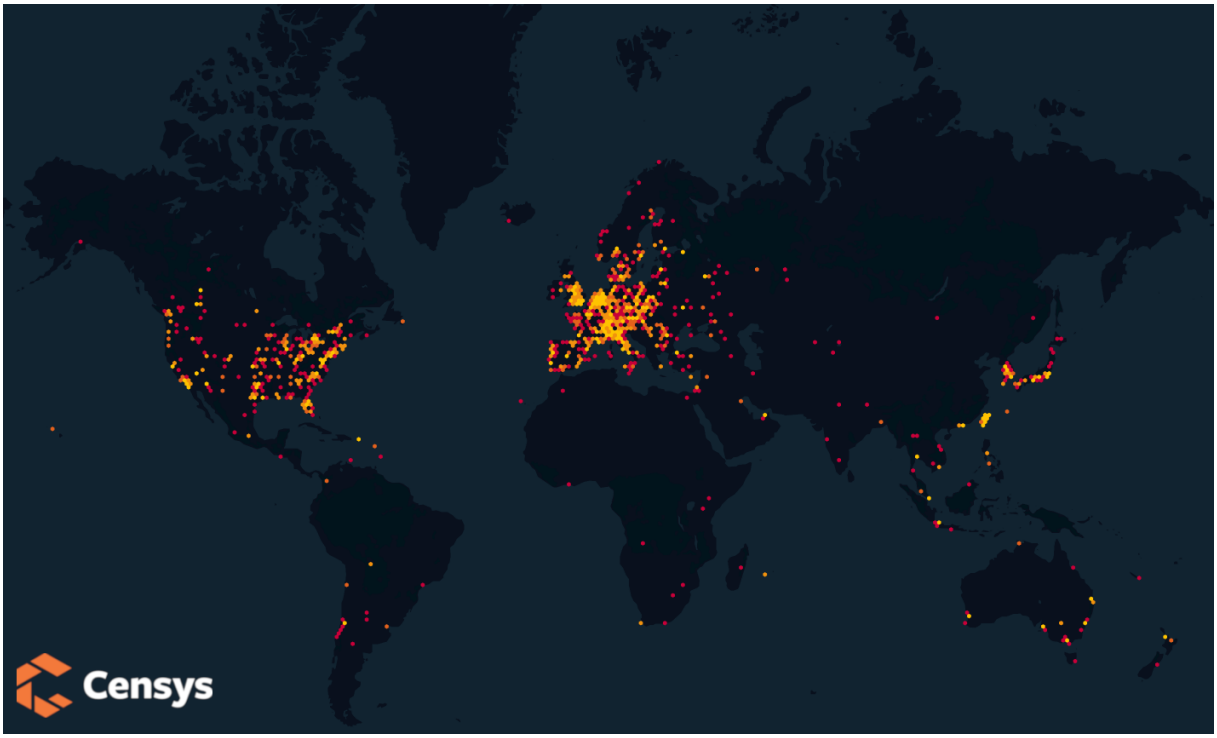
The following screenshot shows the hacked webpage users were greeted with when logging into their local QNAP NAS devices:



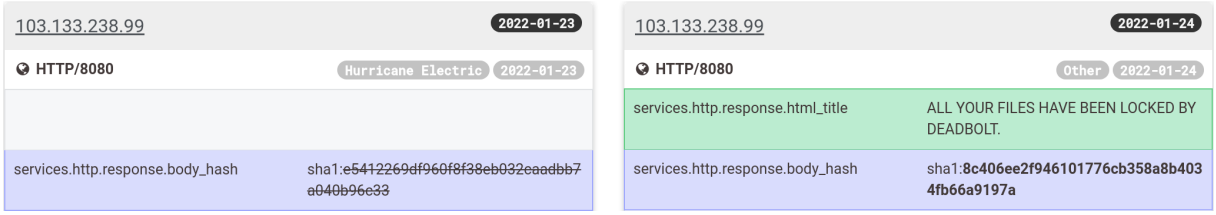
The group behind this coordinated attack calls themselves “DeadBolt,” and before a few days ago, the group was seemingly non-existent. Although on Jan. 7, 2022, SANS Newsbites reported an eerie, sparse prelude to this event:

“QNAP urged its customers to take steps to secure their devices to protect them from active ransomware and brute force attacks targeting network-attached devices.”

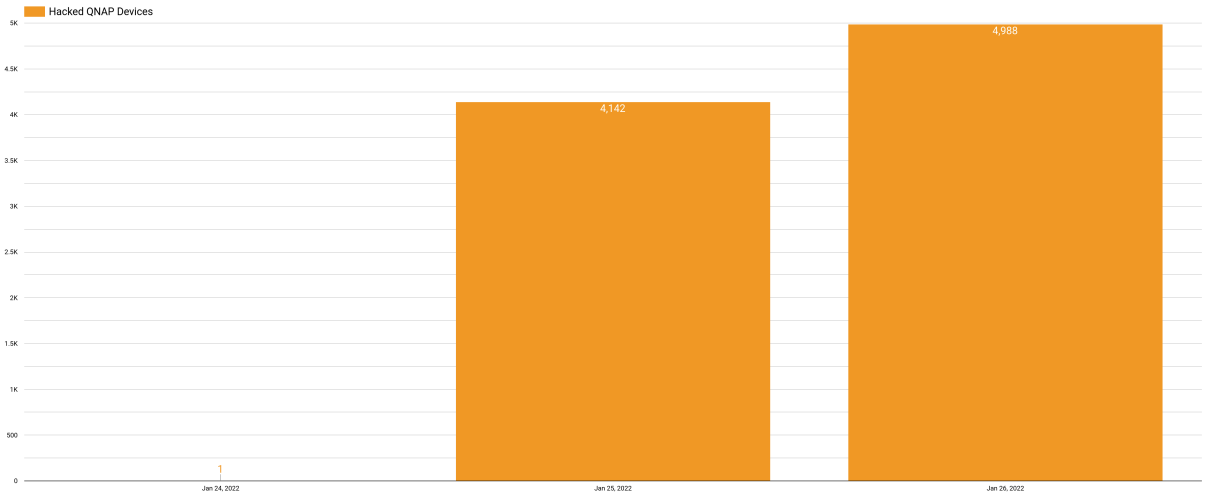
A View from the Censys



Above is a geographical heatmap of QNAP devices which have been infected by the DeadBolt ransomware.
Because Censys maintains a historical view of all assets on the internet and provides a rich interface for visualizing service differences between two dates, we were able to identify a single host with this ransomware around Jan. 23.



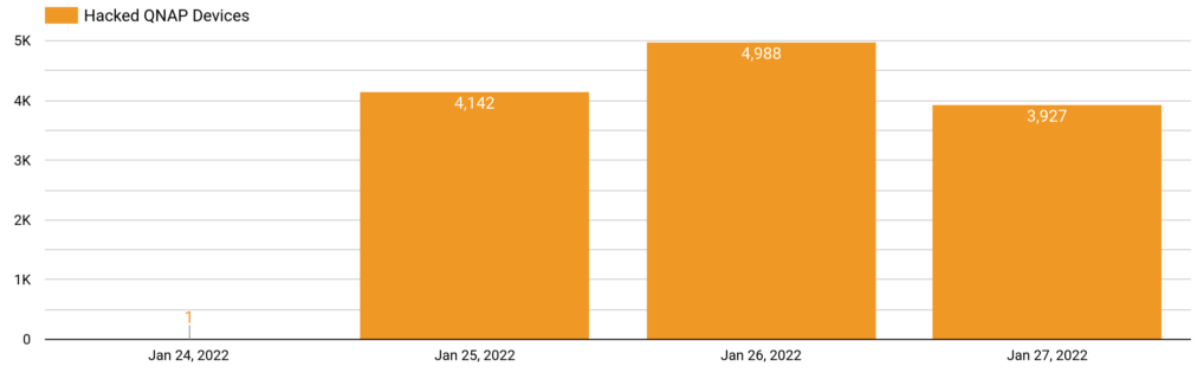
But over the last few days, we've seen steady growth in the number of devices that have been successfully infected. As of January 26, 2022, Censys found over 130,000 QNAP NAS devices, and of those, 4,988 services exhibited the telltale signs of this specific piece of ransomware.



Along with the self-explanatory HTML title, "ALL YOUR FILES HAVE BEEN LOCKED BY DEADBOLT," the HTTP response body includes a unique Bitcoin address where the victim is urged to send 0.03BTC (equivalent to USD 1,100) to unlock their newly hacked device. If the attackers successfully get a 100% return from this attack, that would net the hackers a prize pool of $4,484,700 US dollars.

Alternatively, QNAP was given the option to pay a flat sum of 50BTC ($1,805,640) to receive a master key to decrypt all customer data. It is unknown whether QNAP will cave to these demands, and even if they do, there are fears that the key is fake.

Update: 01-28-2022



Overnight, the number of services with the **DeadBolt ransomware dropped by 1,061 down to a total of 3,927 infected services on the public internet**.

The exact reason for this drop is unknown at the moment, and we are continuing to monitor the situation. But earlier today, Malwarebytes reported that QNAP released a (forced)

automatic update for their Linux-based operating system called “QTS” to address the vulnerability. This update reportedly removed the ransomware executable and reverted the web interface changes made by the ransomware.

Lies and Subterfuge

Once payment has been received, the ransomware group claims to make a second transaction to the same BTC address, this time including the key used for decrypting the user’s files. The following is a quote from the ransomware help page:

“Our decryption key delivery process is 100% transparent and honest. The decryption key will be delivered to the bitcoin blockchain inside the OP_RETURN field. You can retrieve it by monitoring the address you made your payment to for new transactions containing the OP_RETURN field.”

But it all might be a lie. Over on the QNAP support forums, one desperate user reported that they had successfully paid the ransom, but the decryption key they received was invalid.

What can I do about it?

QNAP suggests that customers disable port-forwarding and UPnP and follow these instructions on their website.

Censys will release a set of fingerprints and risks for ASM customers, which will alert when an internet-exposed QNAP device is running on a customer network. Experts suggest that administrators keep devices like this behind a firewall, far from the grubby reaches of the public internet.

All other users should visit https://search.censys.io/me to determine what services they expose to the public internet.