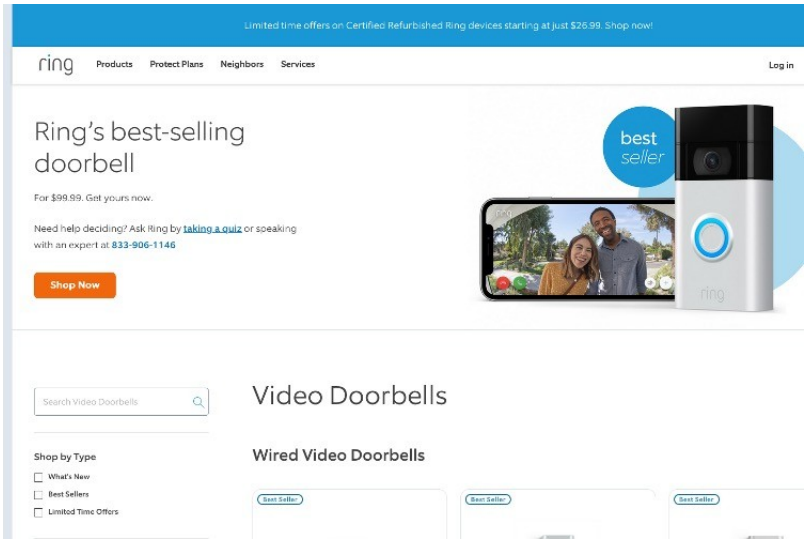
New American

Written by **Joe Wolverton, II, J.D.** on March 16, 2023

Ransomware Group Claims to Have Hacked Ring Security Camera Data

Technological terrorists claim to have seized the data from Amazon's popular "Ring" smart doorbell and surveillance devices and are threatening to release that data over the internet unless Amazon meets their demands.



ring.com

As reported by Vice:

> "There's always an option to let us leak your data," a message posted on the ransomware group's website reads next to Ring's logo. The ransomware group claiming responsibility for the attack is ALPHV, whose malware is known as BlackCat.
>
> Like other ransomware groups, ALPHV goes beyond just locking a victim's files, and has a website where it names and shames its victims in an attempt to extort them. If those targets don't pay, ALPHV threatens to publicly release data stolen from them. ALPHV's site stands out in that the section of its site which publishes hacked data, called "Collections," is easier to search than some other hacking group's sites.

ALPHV has a history of such attacks, having previously released medical data, as well as data hacked from a hotel chain.

For those readers unfamiliar with the term, ransomware is a type of malicious software (malware) that encrypts a victim's files or computer system and demands payment, usually in the form of cryptocurrency, in exchange for the decryption key. Ransomware typically spreads through email attachments, infected software downloads, or vulnerabilities in a computer system's security. Once the ransomware has infected a victim's system, it can quickly spread to other connected devices or networks. The attackers behind the ransomware will then demand payment in exchange for restoring access to the victim's files or system. Ransomware attacks can be devastating, as they can result in the loss of important data or the disruption of critical systems.

In this case, the ALPHV group reports that it has seized control of the data from Ring cameras and that if Amazon doesn't accede to their terms, then ALPHV will release the Ring camera data on the internet, putting the video and audio data of millions within the reach of anyone with access to a computer.

For its part, Ring claims that it's seen no evidence that customer data have been compromised. Ring admits, however, that a third-party vendor has been the victim of a ransomware account and that Ring/Amazon is working with that company to minimize the damage. Ring insists that the third-party vendor has no access to customer data.

Regardless of such reassurances, this isn't the first time data from Ring cameras have suffered serious security breaches.

In 2020, an Amazon software engineer called for the shutdown of Ring, explaining that the service is incompatible with privacy.

Max Eliaser, the Amazon employee insisting that the connected Ring doorbells and cameras should be shelved, posted an explanation on Medium. "The deployment of connected home security cameras that allow footage to be queried centrally are simply not compatible with a free society. The privacy issues are not fixable with regulation and there is no balance that can be struck. Ring should be shut down immediately and not brought back," he wrote.

Eliaser isn't alone in raising a warning voice about the potential threats to privacy posed by the popular doorbell camera. The Electronic Frontier Foundation (EFF) published a report revealing substantial breaches to the privacy of users of the Amazon-owned "smart" technology. EFF's report showed the smart device is a lot savvier than users likely realize:

> Ring doorbell app for Android found it to be packed with third-party trackers sending out a plethora of customers' personally identifiable information (PII). Four main analytics and marketing companies were discovered to be receiving information such as the names, private IP addresses, mobile network carriers, persistent identifiers, and sensor data on the devices of paying customers.

While Amazon does not publish sales numbers, industry insiders estimate that the online retailer has sold over 1.7 million units of the Ring devices, which is more than its next four competitors combined.

Thus the hacking and holding of customer data by a ransomware group proven in the past to follow through on their threats to release personal data on the internet is particularly alarming.

Believe it or not, Ring cameras have had other very serious security shortcomings exposed recently.

Regarding the Ring doorbell app, an EFF investigation disclosed that a shocking amount of personal data is shared with third-party companies without notice to the user:

> AppsFlyer, a big data company focused on the mobile platform, is given a wide array of information upon app launch as well as certain user actions, such as interacting with the "Neighbors" section of the app. This information includes your mobile carrier, when Ring was installed and first launched, a number of unique identifiers, the app you installed from, and whether AppsFlyer tracking came preinstalled on the device. This last bit of information is presumably to determine whether AppsFlyer tracking was included as bloatware on a low-end Android device.
>
> Most alarmingly, AppsFlyer also receives the sensors installed on your device (on our test device, this included the magnetometer, gyroscope, and accelerometer) and current calibration settings.

As unbelievable as that relationship is, AppsFlyer is not the biggest benefactor of Ring's data sharing scheme.

More from EFF's report:

> Ring gives MixPanel the most information by far. Users' full names, email addresses, device information such as OS version and model, whether bluetooth is enabled, and app settings such as the number of locations a user has Ring devices installed in, are all collected and reported to MixPanel. MixPanel is briefly mentioned in Ring's list of third party services, but the extent of their data collection is not.
>
> What makes this data-sharing arrangement even more menacing is that the method of encryption used by Amazon makes it difficult for someone trying to detect the presence of the programs that gather and send the data. Security companies or researchers that might be looking for such security breaches would find these barricades, impediments that would likely discourage digging any deeper.

Beyond the app-based breach of privacy, the Ring devices create situations where surveillance can be conducted on people who don't have the service and who cannot keep themselves from being watched by those who do.

Amazon's Ring home security service has entered into contracts with over 200 police departments, and the tech giant admits to giving law enforcement expansive access to the video and audio collected by the service's surveillance devices, without the permission of the customer!

A visit to Amazon's Ring Security System's product page reveals to possible customers — and those worried about personal privacy — all the data that Amazon is making available, without prior permission or notice of Ring customers, to police departments:

• Monitor your property in HD video, and check-in on home at any time with Live View on-demand video and audio.

• Hear and speak to people on your property from your mobile device with the built-in microphone and speakers.

• Activate the siren from your phone, tablet, and PC to scare away any suspicious people caught on camera.

So, is this the data that ALPHV has and is threatening to release? No one knows and they aren't saying.

But the more relevant question is, will all these security breaches and data hacks convince anyone to think twice about allowing Amazon access to their home?

A cybersecurity company has verified independently that the ALPHV collective does list Ring data among the data it currently has in its database.