Canon confirms ransomware attack in internal memo

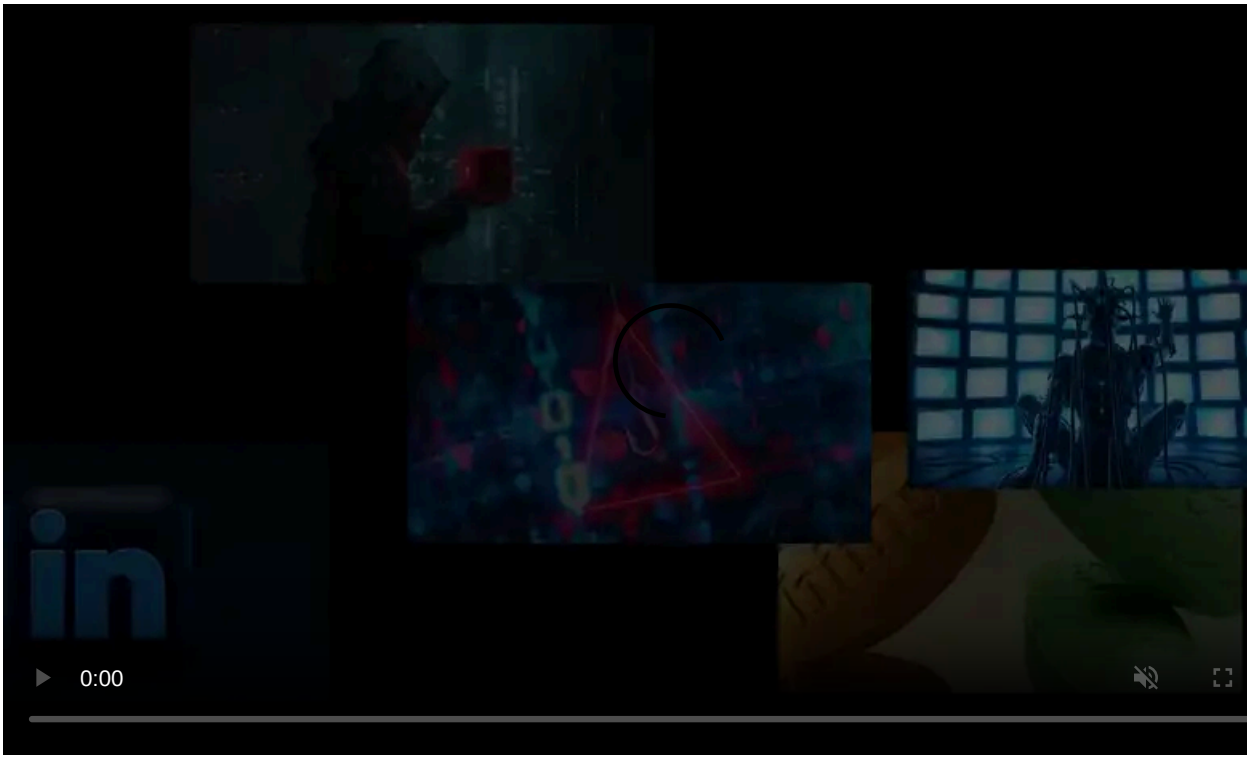
By Lawrence Abrams

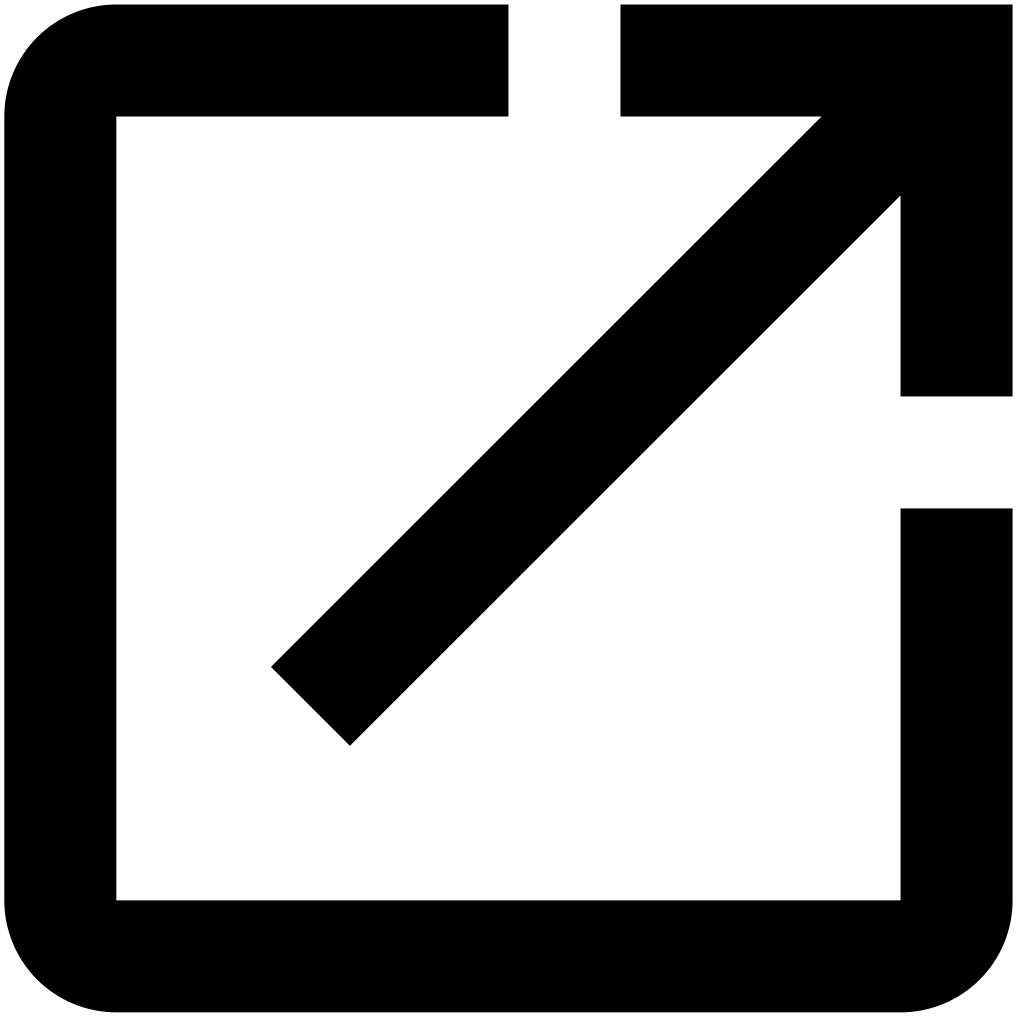
Published: 2020-08-06 · Archived: 2026-04-05 16:01:07 UTC

08/06 update added below. This post was originally published on August, 5th, 2020.

Canon has suffered a ransomware attack that impacts numerous services, including Canon's email, Microsoft Teams, USA website, and other internal applications. In an internal alert sent to employees, Canon has disclosed the ransomware attack and working to address the issue.

BleepingComputer has been tracking a suspicious outage on Canon's image.canon cloud photo and video storage service resulting in the loss of data for users of their free 10GB storage feature.

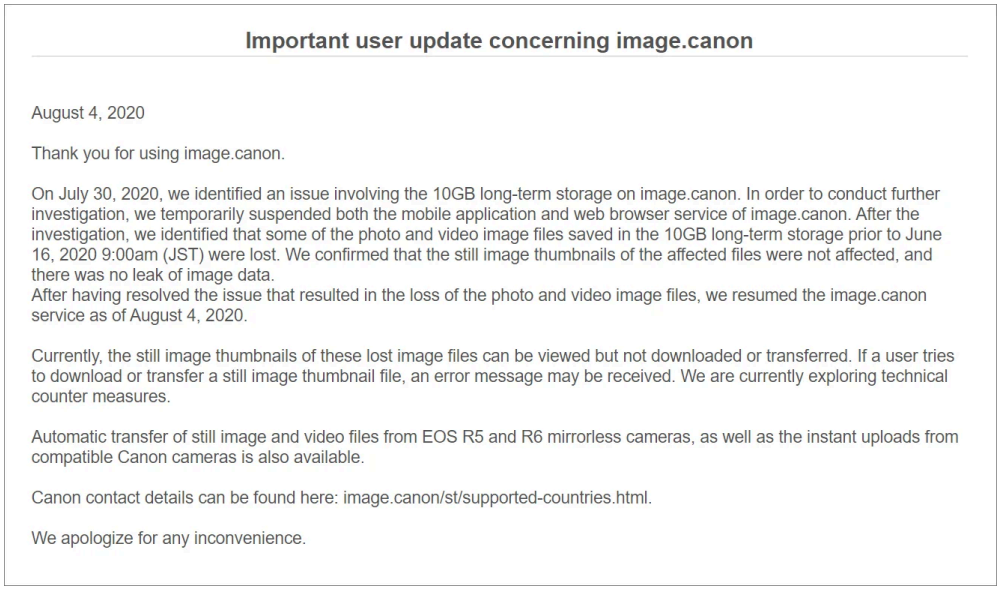

0:00



Visit Advertiser websiteGO TO PAGE

The image.canon site suffered an outage on July 30th, 2020, and over six days, the site would show status updates until it went back in service yesterday, August 4th.

However, the final status update was strange as it mentions that while data was lost, "there was no leak of image data." This led BleepingComputer to believe there was more to the story and that they suffered a cyberattack.



Important user update concerning image.canon

August 4, 2020

Thank you for using image.canon.

On July 30, 2020, we identified an issue involving the 10GB long-term storage on image.canon. In order to conduct further investigation, we temporarily suspended both the mobile application and web browser service of image.canon. After the investigation, we identified that some of the photo and video image files saved in the 10GB long-term storage prior to June 16, 2020 9:00am (JST) were lost. We confirmed that the still image thumbnails of the affected files were not affected, and there was no leak of image data.
After having resolved the issue that resulted in the loss of the photo and video image files, we resumed the image.canon service as of August 4, 2020.

Currently, the still image thumbnails of these lost image files can be viewed but not downloaded or transferred. If a user tries to download or transfer a still image thumbnail file, an error message may be received. We are currently exploring technical counter measures.

Automatic transfer of still image and video files from EOS R5 and R6 mirrorless cameras, as well as the instant uploads from compatible Canon cameras is also available.

Canon contact details can be found here: image.canon/st/supported-countries.html.

We apologize for any inconvenience.

Image.canon outage notice
Source: BleepingComputer

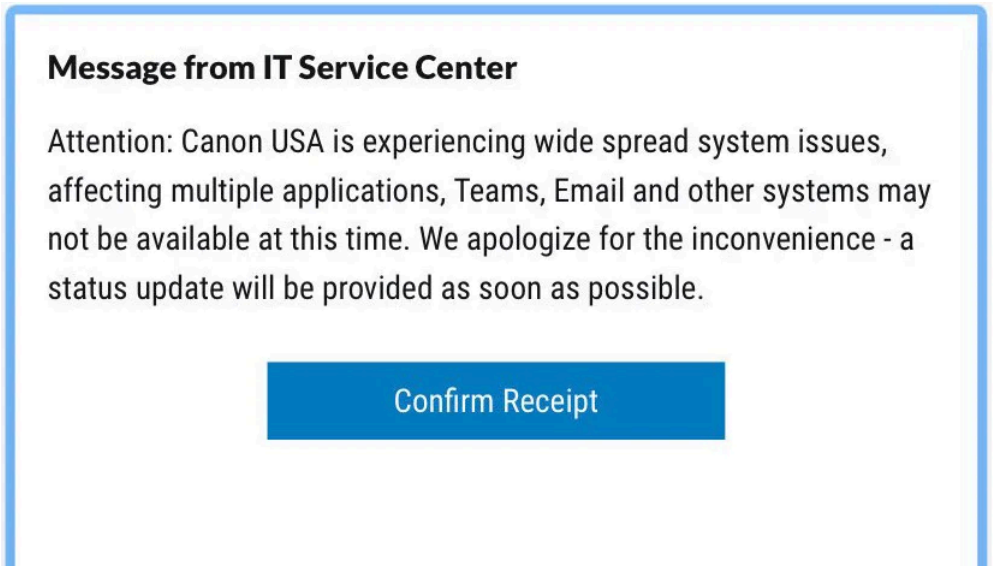
When we contacted Canon about this outage, they referred us to the notice on the image.canon site.

If you work at Canon or know someone working there with first-hand information on this incident, you can confidentially contact us on Signal at +16469613731.

Canon suffers ransomware attack

Today, a source contacted BleepingComputer and shared an image of a company-wide notification titled "Message from IT Service Center" that was sent at approximately 6 AM this morning from Canon's IT department.

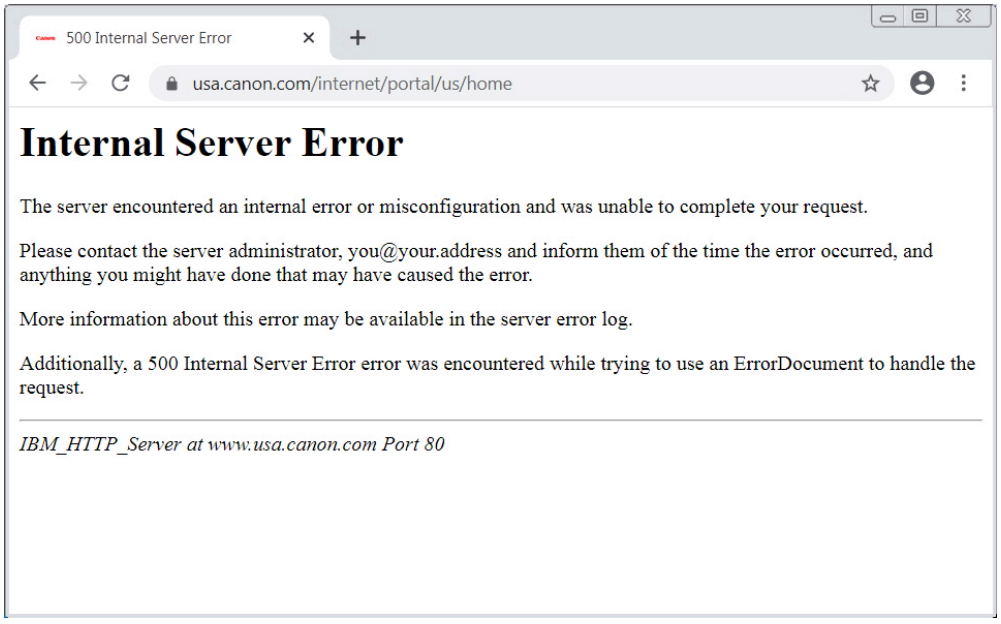
This notification states that Canon is experiencing "wide spread system issues affecting multiple applications, Teams, Email, and other systems may not be available at this time."



Notice from Canon's IT department

Source: BleepingComputer

As part of this outage, Canon USA's website is now displaying errors or page not found errors when visited.



Canon USA website is down

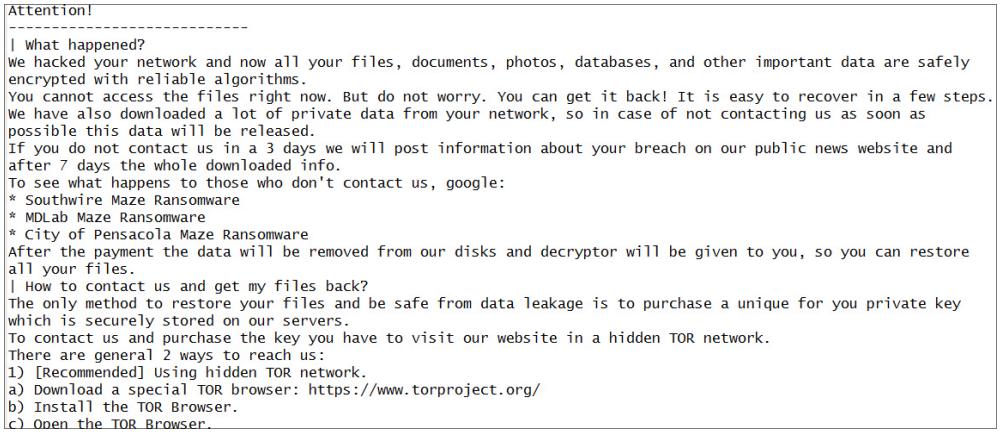
Source: BleepingComputer

The list of Canon domains that appear to be affected by this outage, include:

```
 www.canonusa.com
www.canonbroadcast.com
b2cweb.usa.canon.com
canondv.com
canobeam.com
canoneos.com
bjc8200.com
canonhdec.com
bjc8500.com
usa.canon.com
imagerunner.com
multispot.com
```

```
canoncamerashop.com
canoncctv.com
canonhelp.com
bjc-8500.com
canonbroadcast.com
imageland.net
consumer.usa.canon.com
bjc-8200.com
bjc3000.com
downloadlibrary.usa.canon.com
www.cusa.canon.com
www.canondv.com
```

Since then, BleepingComputer has obtained a partial screenshot of the alleged Canon ransom note, which we have been able to identify as from the Maze ransomware.



```
Attention!
----------------------------
| What happened?
We hacked your network and now all your files, documents, photos, databases, and other important data are safely
encrypted with reliable algorithms.
You cannot access the files right now. But do not worry. You can get it back! It is easy to recover in a few steps.
We have also downloaded a lot of private data from your network, so in case of not contacting us as soon as
possible this data will be released.
If you do not contact us in a 3 days we will post information about your breach on our public news website and
after 7 days the whole downloaded info.
To see what happens to those who don't contact us, google:
* Southwire Maze Ransomware
* MDLab Maze Ransomware
* City of Pensacola Maze Ransomware
After the payment the data will be removed from our disks and decryptor will be given to you, so you can restore
all your files.
| How to contact us and get my files back?
The only method to restore your files and be safe from data leakage is to purchase a unique for you private key
which is securely stored on our servers.
To contact us and purchase the key you have to visit our website in a hidden TOR network.
There are general 2 ways to reach us:
1) [Recommended] Using hidden TOR network.
a) Download a special TOR browser: https://www.torproject.org/
b) Install the TOR Browser.
c) Open the TOR Browser.
```

Partial Maze ransomware note

Source: BleepingComputer

Maze claims to have stolen 10TB of data from Canon

After contacting the ransomware operators, BleepingComputer was told by Maze that their attack was conducted this morning when they stole "10 terabytes of data, private databases etc" as part of the attack on Canon.

Maze declined to share any further info about the attack including the ransom amount, proof of stolen data, and the amount of devices encrypted.

While we first thought that the image.canon outage was related to the ransomware attack, Maze has told us that it was not caused by them.

Maze is an enterprise-targeting human-operated ransomware that compromises and stealthily spreads laterally through a network until it gains access to an administrator account and the system's Windows domain controller.

During this process, Maze will steal unencrypted files from servers and backups and upload them to the threat actor's servers.

Once they have harvested the network of anything of value and gain access to a Windows domain controller, Maze will deploy the ransomware throughout the network to encrypt all of the devices.

If a victim does not pay the ransom, Maze will publicly distribute the victim's stolen files on a data leak site that they have created.

Maze has claimed responsibility for other high-profile victims in the past, including LG, Xerox, Conduent, MaxLinear, Cognizant, Chubb, VT San Antonio Aerospace, the City of Pensacola, Florida, and more.

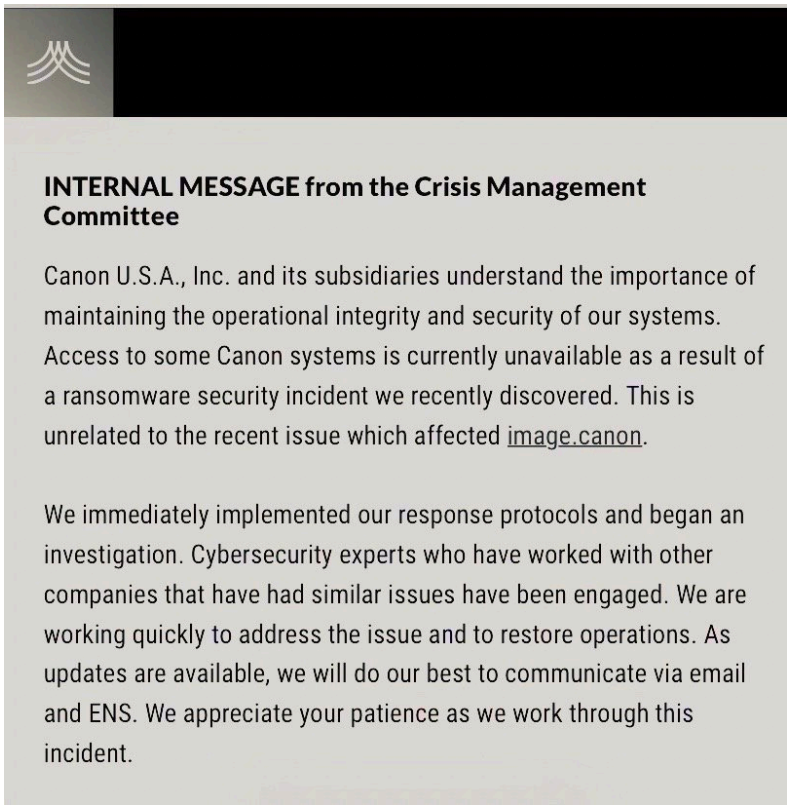
In a statement to BleepingComputer, Canon says they are "currently investigating the situation."

Canon discloses ransomware attack to employees

Update 08/06/20: BleepingComputer has obtained a screenshot of an internal message sent by Canon to employees that discloses the ransomware attack.

This message further states that they have hired an outside cybersecurity company to aid in their recovery.

"Canon U.S.A, Inc. and its subsidiaries understand the importance of maintaining the operational integrity and security of our systems. Access to some Canon systems is currently unavailable as a result of a ransomware incident we recently discovered. This is unrelated to the recent issue which affected image.canon."



INTERNAL MESSAGE from the Crisis Management Committee

Canon U.S.A., Inc. and its subsidiaries understand the importance of maintaining the operational integrity and security of our systems. Access to some Canon systems is currently unavailable as a result of a ransomware security incident we recently discovered. This is unrelated to the recent issue which affected image.canon.

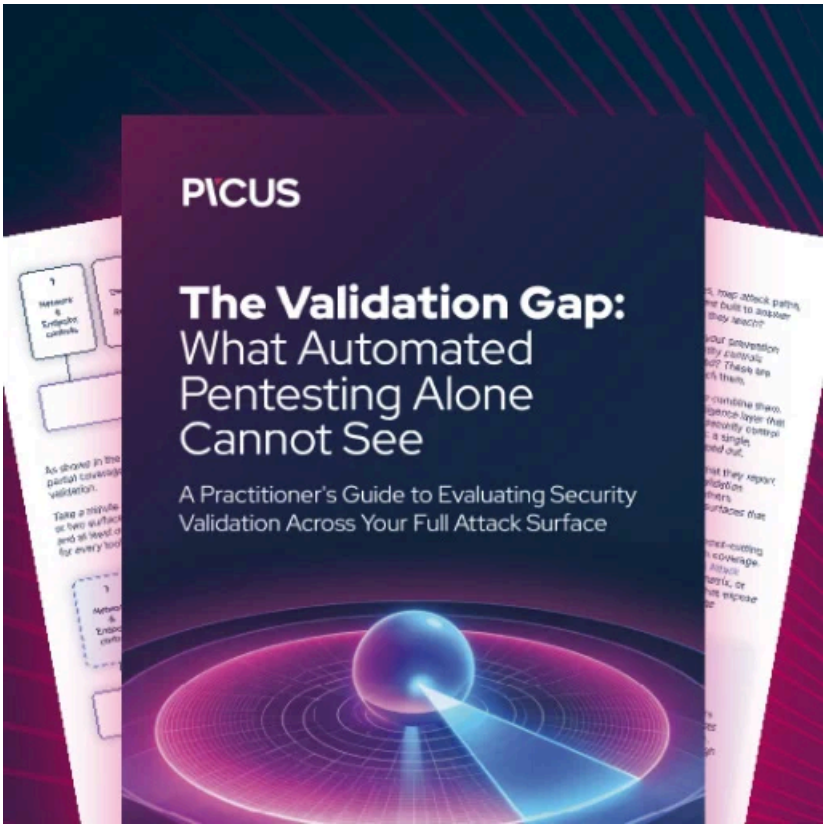
We immediately implemented our response protocols and began an investigation. Cybersecurity experts who have worked with other companies that have had similar issues have been engaged. We are working quickly to address the issue and to restore operations. As updates are available, we will do our best to communicate via email and ENS. We appreciate your patience as we work through this incident.

Internal notice sent to employees

In response to our query, Canon continues to state "We are currently investigating the situation. Thank you."

This is a developing story and will be updated as more information is available.

Update 8/5/20: Article updated to reflect that the image.canon outage was not related to the Maze ransomware attack.
Update 8/6/20: Canon has internally notified their employees of the ransomware attack.



[Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/canon-hit-by-maze-ransomware-attack-10tb-data-allegedly-stolen/