Case study

When London Airport was targeted by a destructive cyberattack, HP printers detected the threat

Official wrap-up report for the data breach

Industry
Aviation

Objective
Identify weak links in cybersecurity practices and address them

Approach
Developed a comprehensive security plan in partnership with HP security experts

IT matters
- Applied security measures to IoT endpoints
- Enabled built-in security features in HP printers
- Improved security monitoring throughout network

Business matters
Improved cybersecurity to protect critical international infrastructure and maintain passenger safety

Overview

London Airport* serves more than 300,000 passengers each day as they travel to 94 countries around the globe. Nearly 50,000 people from 300 companies work at the airport, making it virtually a condensed city.

As the airport has grown, its infrastructure has become increasingly connected and automated. Internal systems from HVAC to lighting to printers are now on the airport's network. Printing, scanning, and copying is performed by a fleet of 60+ HP MFPs spread throughout the campus.

On April 23, 2018, the cyberterrorist known only as "The Wolf" used the airport's connected lighting systems to gain access and spread his malware across the network. As he is known for his exploits using under-secured endpoints, the IT security experts immediately turned to threat logs from their HP Enterprise printers as part of the investigation to isolate and stop the attack. Surprisingly, the logs contained clues from The Wolf as to where the intrusion originated. Afterward, London Airport turned to HP to further advance their endpoint security.

What happened

Once The Wolf found a vulnerability, likely by phishing emails to users on the network, he could infect the IoT lighting system with malware. He could then extend his malware through the network, creating footholds in other unmonitored endpoint devices.

By hiding their presence in unmonitored IoT devices, The Wolf's team could remain undiscovered by the network monitoring systems while they developed multiple launch points for a massive destructive attack.

Airport management found themselves desperately trying to shut down multiple systems while keeping critical infrastructure like planes and passengers moving.

Responding to the attack

The Wolf had been hired to attack the airport's network. Airport IT security staff *thought* the airport's network was well-protected against hackers, but they lacked visibility to threats hiding in IoT devices.

Fortunately, the airport's HP Enterprise printers included HP Connection Inspector, which stopped the malware when it made suspicious attempts to "call home" to the hackers' command and control servers.

The actions were captured in the printer syslogs. Once the IT staff realised something was wrong, they checked the syslogs for details about the attack. But time is of the essence when malware is spreading through the network. If the IT security staff had connected the printers' threat detection syslogs to their security information and event monitoring (SIEM) system, they would have been alerted immediately when the intrusion occurred.

Stronger security than ever

After the breach, IT staff reviewed security practices with their managed print services provider and HP Security Advisors.

By installing HP Enterprise printers, London Airport was already on the right track. Only HP Enterprise printers and MFPs offer run-time intrusion detection and HP Connection Inspector to detect and stop malware during operations and force a reboot. At startup, HP Sure Start checks the BIOS and can self-heal if the code has been compromised, while whitelisting checks the firmware.

The managed print services provider deployed HP JetAdvantage Security Manager to automatically check security settings each time a printer is rebooted and reset any altered settings.

The airport IT security staff also took the step of connecting the printer syslogs to their SIEM tool. Unlike printers from other manufacturers, HP devices can supply threat-specific logs to many SIEM tools so IT staff can get real-time alerts on possible security incidents. This turns HP printers into invaluable "eyes" on their network.

Conclusion

Because of the airport's HP Enterprise printers and the clues left behind by The Wolf, the security team was able to isolate the attack quickly enough to avoid disrupting operations, negative publicity, noncompliance fines, and brand damage.

By employing stronger security practices and taking full advantage of the built-in security features of their HP printers, the airport has tightened security throughout the network.

**London Airport is a fictional organisation targeted in a large cyberattack in HP Studio's film, "THE WOLF: TRUE ALPHA."*

For more information on HP solutions:
Print security: hp.com/go/reinventsecurity
PC security: hp.com/go/ComputerSecurity

To view "The Wolf" films, visit:
hp.com/thewolf

Sign up for updates
hp.com/go/getupdated

Share with colleagues

4AA7-3560EEW, August 2018