Faxploit: Retro hacking of fax machines can spread malware

20th Century tech causing problems in the 21st

Video Corporations are open to hacking via a booby-trapped image data sent by fax, a hacker demo at DEF CON suggests.

The hack - discovered by security researchers at Check Point - relies on exploiting flaws in the communication protocols used in tens of millions of fax-capable devices globally, such as all-in-one fax-enabled printers.

Vulnerabilities in the protocols that faxes and all-in-one printers use to send & receive faxes create a mechanism for miscreants to create an image file that bundles malware. This booby-trapped image can be sent to a targeted fax device.

The team demonstrated the vulnerabilities in the popular HP Officejet Pro All-in-One fax printers during a presentation at DEF CON hacker event in Las Vegas on Sunday.

Prior to the presentation, Check Point shared its findings with HP, which responded by developing a software patch for its printers. HP's advisory admits that, if left unaddressed, the security flaws created a means for hackers to push malware onto vulnerable Inkjet printers (many models are affected).

Two security vulnerabilities have been identified with certain HP Inkjet printers. A maliciously crafted file sent to an affected device can cause a stack or static buffer overflow, which could allow remote code execution.

The same protocols are also used by many other vendors' faxes and multifunction printers, and in online fax services such as fax2email, so it is likely that these are also vulnerable to attack using the same method, according to security researchers.

Hanging on the telephone

Fax may seem like an obsolete technology that only comes into its own on football's transfer deadline day. However there are still over 45 million fax machines in use in businesses globally, with 17 billion faxes sent every year.

The NHS in the UK alone has over 9,000 fax machines in regular use, according to figures cited by Check Point. Fax machines are also widely used in sectors such as healthcare, legal, banking and real estate.

In many jurisdictions, emails are not considered as evidence in courts of law, so fax is used when handling certain business and legal processes. Nearly half of all laser printers sold in Europe are multifunction devices with fax capability.

“Many companies may not even be aware they have a fax machine connected to their network, but fax capability is built into many multifunction office and home printers,” said Yaniv Balmas, group manager security research at Check Point.

Tom B, red team leader at security consultancy ThinkMarble, said that even though hacking a combined fax machine and printer is possible, other attacks are more likely in practice; at least outside the arena of targeted assaults where money is no object.

"Receiving a fax is essentially like receiving a telephone call – they are generally traceable," he argued. "Furthermore, phone calls also cost money. Phoning millions of fax machines to find a vulnerable model is expensive, and this will dissuade the common cybercriminal."

“While the exploitation of fax machines will be seldom seen in the wild, it is highly recommended that fax machines/printers/all in one devices are periodically updated and patched in-line with common cyber security best practices. It is our experience that network peripherals are often installed and forgotten about, leaving them vulnerable,” he concluded.

The area of security research is not entirely new - a bug in Epson multifunction printer firmware that posed a backdoor risk was discovered back in 2016, for example. Other examples are thin on the ground. The new research does however serve as a reminder that networked devices as well as PCs and servers, need patching.

To minimise the security risk, Check Point advises that organisations check for available firmware updates for their fax devices and apply them. Organisation are also urged to place fax devices on a secure network segment separated from applications and servers that carry sensitive information. Segmentation will limit the ability of malware to spread across networks. ®