July 2017

Cyber Matters

Your essential guide

In this issue:

01704 542 420
info@p-ccomms.com

The Route(r) Of All Problems

A large number of the latest serious security threats have been linked to the ‘Vault 7’ files that WikiLeaks has been releasing over recent weeks. These leaks have provided details of many of the tools and exploits used by US intelligence agencies, and the latest batch includes router vulnerabilities that the CIA have allegedly been using for years to manipulate routers from manufacturers including D-Link and LinkSys. The released documents detail the CIA's modification of the router's firmware, dubbed FlyTrap, which is commonly used in private homes, public spaces and many small to medium sized businesses. It can monitor internet traffic and capture information such as email addresses, chat usernames, MAC addresses and VoIP numbers. Additionally, FlyTrap can be installed remotely and allow its controller to redirect internet traffic to arbitrary sites.

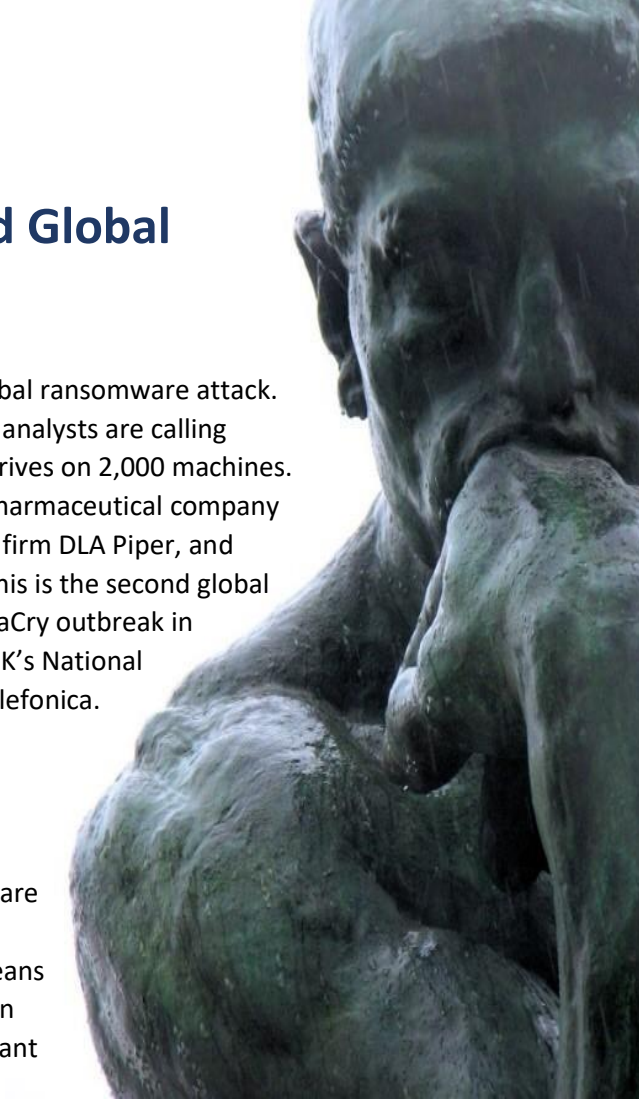
What can I do?

Virgin Media released a security patch last month to fix the issue and we encourage users toensure their devices are updated at the earliest opportunity. However, this vulnerability is not limited to Virgin. Many other routers are also potentially at risk. As a general rule, routers are sentto customers with a default wi-fi password already set up. Some use a long password with mixture of upper and lower-case letters, numbers and sometimes symbols. But others use short passwords with a limited selection of characters, and many follow a pattern than can be identified by attackers. In the case of the Virgin Media Super Hub 2, it used passwords that were just eight characters long, and used only lower-case letters. That gives cyber-criminals a framework to help them crack passwords quickly, using a dedicated computer.

Virgin Media Routers Vulnerable

At the same time, researchers have uncovered a vulnerability in Virgin Media home broadband routers which could allow attackers to gain access to the device's administrator panel. They discovered that the encryption key used for custom configurations of the routers is the same for all hubs across the UK. The Super Hub 2 and Super Hub 2AC (both of which are made by Netgear) are affected. This means an attacker with access to the administrative interface of a user's hub could download a configuration file, add additional instructions to enable remote access and restore the file to the hub. This process allows remote access to the router and can potentially be used to monitor internet traffic from any device attached to the router including computers and phones.

Smarter, Better, Stronger – Second Global Ransomware Attack



Businesses and government systems have been hit in a new global ransomware attack. The malware, a variation of the Petya ransomware which some analysts are calling 'GoldenEye' or 'NotPetya', has so far encrypted files and hard drives on 2,000 machines. High-profile victims include Danish shipping giant Maersk, US pharmaceutical company Merck, international advertising conglomerate WPP, global law firm DLA Piper, and multiple private and public institutions in Ukraine and Russia. This is the second global ransomware attack in the last two months. It follows the WannaCry outbreak in May that affected more than 150 organisations, including the UK's National Health Service, German railways and Spanish telephone firm Telefonica.

What Now?

The attack is likely to persist for some time given the fact there are no decryption keys to restore PCs with infected filesystems, no way to pay the ransom, and the diversity of delivery options means that no single patch can necessarily provide complete protection against it. Notwithstanding this, you should still install the relevant patches as a matter of urgency.

Further mitigation advice includes:

• The ransomware runs on boot, meaning that if you can disrupt a system before Windows boots, or if you encounter a "Check Disk" message, you can avoid having your files encrypted by quickly powering down;

• Administrators can stop the spread within a network from the Windows Management Instrumentation by blocking the file C:\Windows\perfc.dat from running. Administrators can use Microsoft's Local Administrator Password Solution to protect credentials that grant network privileges;

• Ensure you are suspicious of any unexpected documents you receive via email. No matter how enticing an attachment or embedded link may be, always verify the source before taking any further action;

• Ensure you (and your company) have a robust backup regime so that important files are backed-up. This includes ensuring that any external storage devices are not always connected to your network to prevent any infections from spreading;

• Consider awareness campaigns and staff training to ensure your employees are aware of the risks;

• Additionally, make sure that you have an effective anti-virus solution and that you conduct regular penetration tests on your systems.

ICO Fires Warning to SMEs with £60,000 Fine

In a clear warning to SMEs, the Information Commissioners Office (ICO) has issued Boomerang Video Ltd with a fine of £60,000 after it failed to take basic steps to stop its website being attacked.
The video game rental firm's website was subject to an SQL injection attack in 2014 in which 26,331 customer details could be accessed. The attacker used a common technique known as SQL injection to access the data.

The ICO found that the company had failed to carry out regular penetration testing on its website, failed to ensure the password for the account on the WordPress section of its website was sufficiently complex, had some information stored unencrypted and, that which was encrypted, could be accessed because it failed to keep the decryption key secure.

Sally Anne Poole, ICO enforcement manager, issued a clear warning to SMEs: "Regardless of your size, if you are a business that handles personal information then data protection laws apply to you…and under the new General Data Protection Legislation (GDPR) coming into force next year, those fines could be a lot higher." The ICO has a range of guidance available to help businesses ahead of the implementation of GDPR on 25 May 2018. This includes website pages dedicated to the data protection reform legislation, and an updated toolkit for SMEs that includes a checklist to help organisations in their GDPR preparations.

What is SQL injection?

An SQL query is one way an application talks to a database. SQL injection occurs when an application fails to sanitise untrusted data in a database query. An attacker can use specially-crafted SQL commands to trick the application into asking the database to execute unexpected commands. Examples of a successful attack exploit include the ability to read sensitive data from the database, modify database data and execute administration operations.

GOT A NEWS TIP FOR CYBER MATTERS? JOIN THE CONVERSATION
PLEASE SEND YOUR COMMENTS TO INFO@P-CCOMMS.COM

Research Suggests 84% of UK SMEs Are Unaware of GDPR

GDPR will come into force on 25 May 2018, yet according to latest research only 14% of small business owners and 31% of senior executives were able to correctly identify the fine associated with the new regulation – up to €20m or 4% of global turnover. Businesses unaware of the forthcoming legislation and its implications are not only putting themselves at risk of severe financial penalties, but also the reputational damage caused by adverse publicity associated with falling foul of the law.

As we approach May 2018, it's crucial that organisations of all sizes begin to take a proactive approach in preparing for the incoming regulations. The first priority for all companies should be to gain a complete picture of all data that is collected, stored or processed that contains EU citizen information. This will inform decisions on implementing stricter internal data protection procedures such as staff training, internal processing audits and reviews of HR policies, to ensuring greater transparency around the use of personal information. Companies must ensure that adequate means of protecting that data have been implemented, such as access being restricted to authorised personnel, proper authentication being used and proper procedures for backing up and archiving data and data sanitisation policies being implemented to remove data when it is no longer needed or requested by customers. In addition, any third parties that have access to the data must be evaluated to ensure they too have adequate controls in place.

Thank you for downloading this guide.

Please feel free to contact us on the details below if you have any questions or comments, or would like advice on any of your own cyber security issues.

01704 542 420
info@p-ccomms.com