Case Study
Scottish Water

"The Fujitsu Cyber Threat Intelligence service has allowed Scottish Water to strengthen our overall security posture and provides us with the level of detection and prevention services that meets our needs."

Tom Porteous, Head of Customer Services, Scottish Water

The customer

Country: United Kingdom
Industry: Utilities
Founded: 2002
Employees: 3,600
Website: www.scottishwater.co.uk

The challenge

When Scottish Water users accidentally introduced a new virus to its network, the company needed to act fast to minimise the damage and quickly remove the new strain of crypto-malware.

The solution

Scottish Water activated the Fujitsu Cyber Threat Intelligence service, which immediately identified the source of the unknown malware variant, cleaned infected devices and worked with Symantec to create a signature that would block it.

The customer

Scottish Water provides drinking water to 2.45 million households and 154,000 business customers in Scotland. Every day it supplies 1.3 billion litres of drinking water and takes away 840 million litres of waste water from customers' properties and treats it before returning it to the environment. It is a publicly owned company, answerable to the Scottish Parliament and the people of Scotland, and employs over 3,600 people.

The challenge

In common with any modern organisation, Scottish Water is vulnerable to malware, viruses and online threats. That's why the company has been using Fujitsu's security services for over six years. More recently, Scottish Water added the Cyber Threat Intelligence (CTI) Managed Security Service, which proved particularly useful when a brand new virus breached the company's firewall.

"An email was received by Scottish Water users from a known external sender containing a URL, which was then visited by a user. The website in question, unbeknownst to the recipient of the email, was hosting scripts, that triggered a chain of requests from the website," explains Tom Porteous, Head of Customer Services at Scottish Water. "These contained hidden malware that spread through a Scottish Water site, making it inoperable from an overall IT perspective."

Even though Scottish Water's security controls and antivirus software were completely up to date, this virus, known as Teslacrypt, did not match any known signatures. It works by encrypting files on infected machines and then demanding a ransom in bitcoin currency to unlock the devices.

"This recent security breach related to a zero-day virus – also known as next-generation malware," adds Porteous. "This is a previously unknown computer virus for which specific antivirus software signatures are not yet available, meaning we had absolutely no protection against this virus as the security software industry knew nothing about it."

That led Scottish Water to invoke the 'BREAK GLASS incident process', giving it direct access to Fujitsu's 24/7 CTI Team.

The benefit

- Enhances information security defences through continuous monitoring and proactive response, protecting infrastructure and services
- Minimises the network exposure to threats
- Ensures the malware could not cause further damage to the network
- Enables the quick creation of a script that would block the virus in the future
- All infected devices were cleaned and returned to the users
- Provides context to the business in terms of the threat and subsequent damage

The solution

The Fujitsu Cyber Threat Intelligence Team enhances Scottish Water's defences using intelligence-driven security analytics. It correlates across multiple security products with strategic partners and other market leading vendors to provide the context the company needs to understand the threat.

By working closely with Scottish Water, Fujitsu was able to ascertain the external website where the payload was being delivered from, assess the relevant risks and work with an antivirus vendor to develop a script that could block it including ensuring further channels for the malware were blocked on the customer network.

"Rapid response and action from Fujitsu's Security Operations Centre (SOC), enabled it to identify both the signature of the virus and the host that deployed it. This proved to be successful, as we isolated the site immediately from our wide area network," says Porteous. "Promptly on identification of the virus signature, Fujitsu was able to pass this to our virus protection vendor Symantec so, in turn, it could develop and deploy both a fix and future protection. The host was quickly identified thereafter and our network was configured to block the suspect website so no further access into Scottish Water could be made."

In addition, Fujitsu performed a scan across the entire network drive and all employee exchange mailboxes to establish how widely the infection had circulated. During the incident, an end-user working from home had received the same email, visited the website and been immediately infected. This incident was captured quickly and both the end-user and their device were disabled from the network before being cleaned.

Products and services

- Fujitsu Cyber Threat Intelligence and threat response Managed Security Service

The benefit

Thanks to the rapid response of the Fujitsu CTI team, the threat was eliminated and contaminated devices were quickly disinfected, allowing Scottish Water to continue its business. Having identified the virus, Fujitsu was also able to run a further scan with more detailed accuracy across the entire Scottish Water network, all end-user devices and the data centre infrastructure.

During this scan, Fujitsu identified a number of users who had received the suspect email leading to the host website. These were deleted and appropriate scans run on every end-user device to ensure no infection. No further virus payloads were identified and further mails were prevented from being delivered.

"Fujitsu's CTI service has allowed Scottish Water to strengthen our overall security posture and provides us with the level of detection and prevention services that meets our needs," continues Porteous. "The response and recovery services have been very successful and, although there is no perfect protection in the cyber world today, Scottish Water can rely on Fujitsu's capabilities."

Conclusion

Having successfully averted a potential disaster, neither Fujitsu nor Scottish Water are complacent, knowing that new threats emerge on a daily basis.

"We expect sophisticated attacks to be launched against our systems and have prepared for this eventuality by leveraging Fujitsu's expertise in this area," concludes Porteous. "In practice, such attacks are rare, however, by keeping abreast of the latest attacks and attacker techniques, we can verify that our systems are capable of detecting and repelling such threats, thanks to Fujitsu.

"Understanding how attacks can occur, implementing the right procedures and developing a clear response strategy can help organisations counteract future threats and recover from incidents more quickly. Fujitsu's expertise in this area has proved successful with Scottish Water and we endorse its strong capabilities in this area."

Tom Porteous, Head of Customer Services, Scottish Water

Contact
FUJITSU UK
Address: 22 Baker Street, London, W1U 3BW
Phone: +44 (0) 870 242 7998
E-mail: askfujitsu@UK.fujitsu.com
Website: www.fujitsu.com/UK
2016-01-25