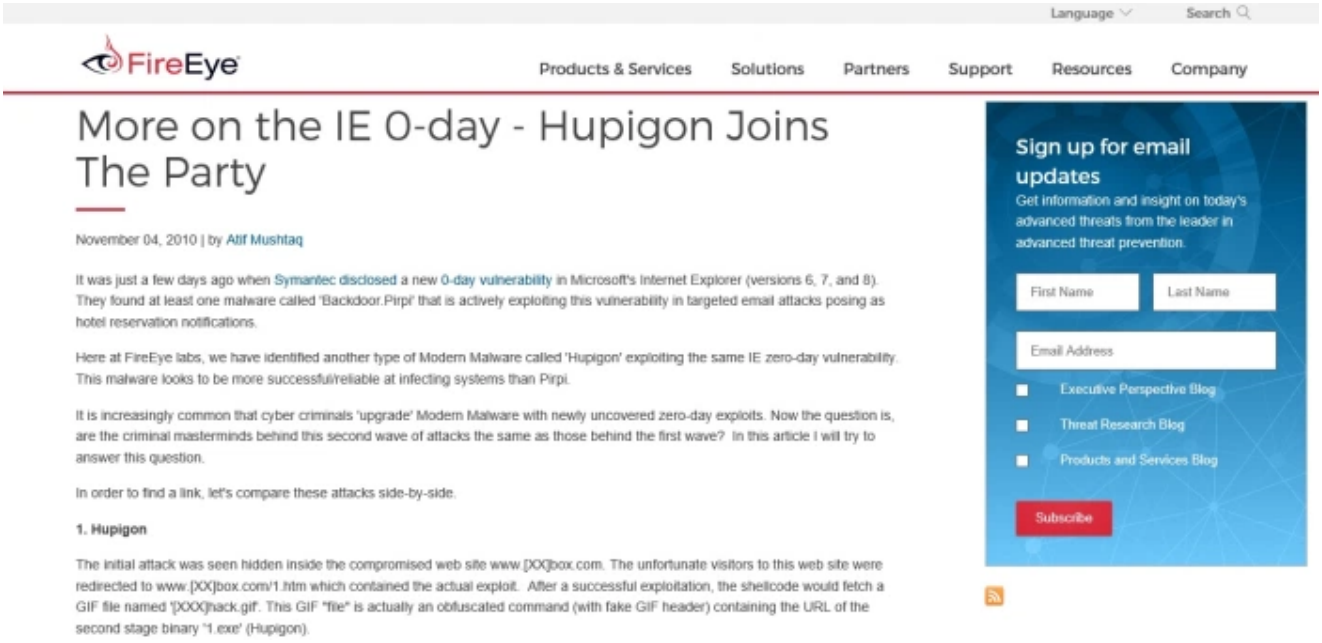
Who is behind this Chinese espionage group stealing our intellectual property?

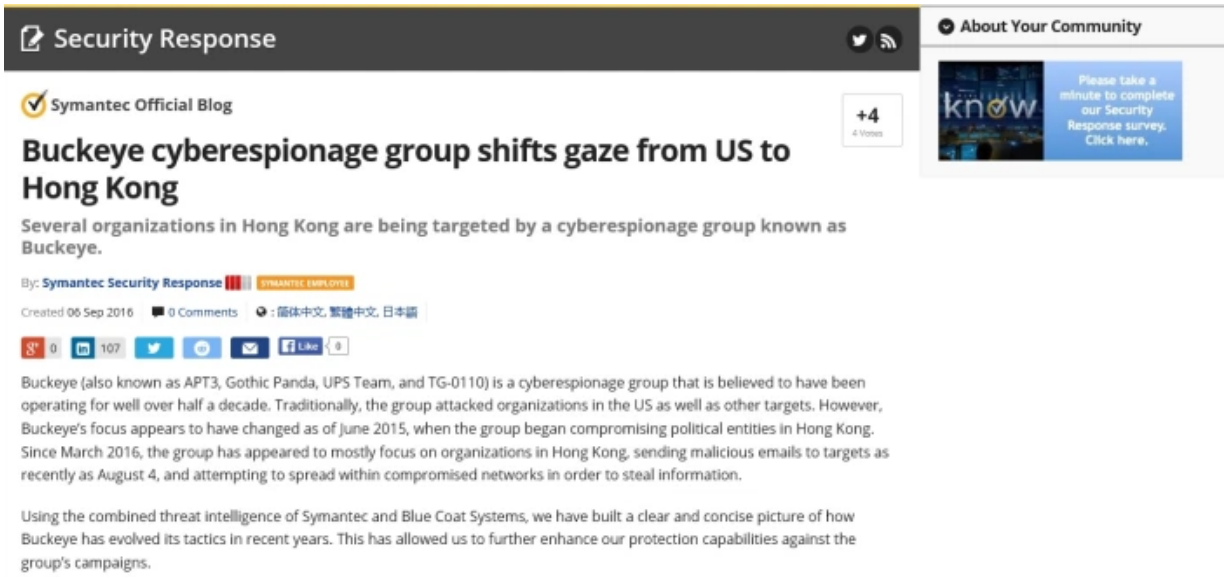
intrusiontruth.wordpress.com/2017/04/26/who-is-behind-this-chinese-espionage-group-stealing-our-intellectual-property

intrusiontruth April 26, 2017

APT3 – also known as Gothic Panda, Buckeye, UPS Team and TG-0110 – was first reported in 2010 by FireEye in their report Hupigon Joins The Party. It is blamed for using a Remote Access Trojan named Pirpi in attacks against the US and UK. The Trojan is usually delivered through malicious attachments or links in spear-phishing e-mails and the group have a history of innovating new browser-based zero-day exploits. FireEye claim that it is one of the most sophisticated threat groups tracked by their Threat Intelligence arm.



APT3's targets are in a wide range of sectors including government entities, research institutions, technology, aerospace and defence, transport, manufacturing and telecommunications. Their geographical focus until 2015 was the US and UK, but in June 2015 Symantec reported that the group had also begun to infect organisations in Hong Kong (see Buckeye cyberespionage group shifts gaze from US to Hong Kong). These infections increased significantly in March 2016.



After exploiting a target, the group hop to additional hosts on the network and install backdoors before searching for intellectual property or other confidential information worth stealing. It forms part of a programme for Intellectual Property theft that costs western economies billions. British companies lose £9.2 billion a year and, were China to respect US IP law, 2.1 million additional jobs could be created.

The InfoSec community finds it difficult to track the command and control infrastructure used by APT3, but we intend to show that it is possible, using domain registration data, to identify the individuals responsible for the APT, the company behind them and the government institution issuing the tasking.

In our next post we will introduce you to the man responsible for purchasing some of APT3's infrastructure. We identified him by following a trail of metadata from APT3 tools and domain names that led to him, his colleagues and his company.

Read our next post on APT3 for the truth behind this intrusion.