


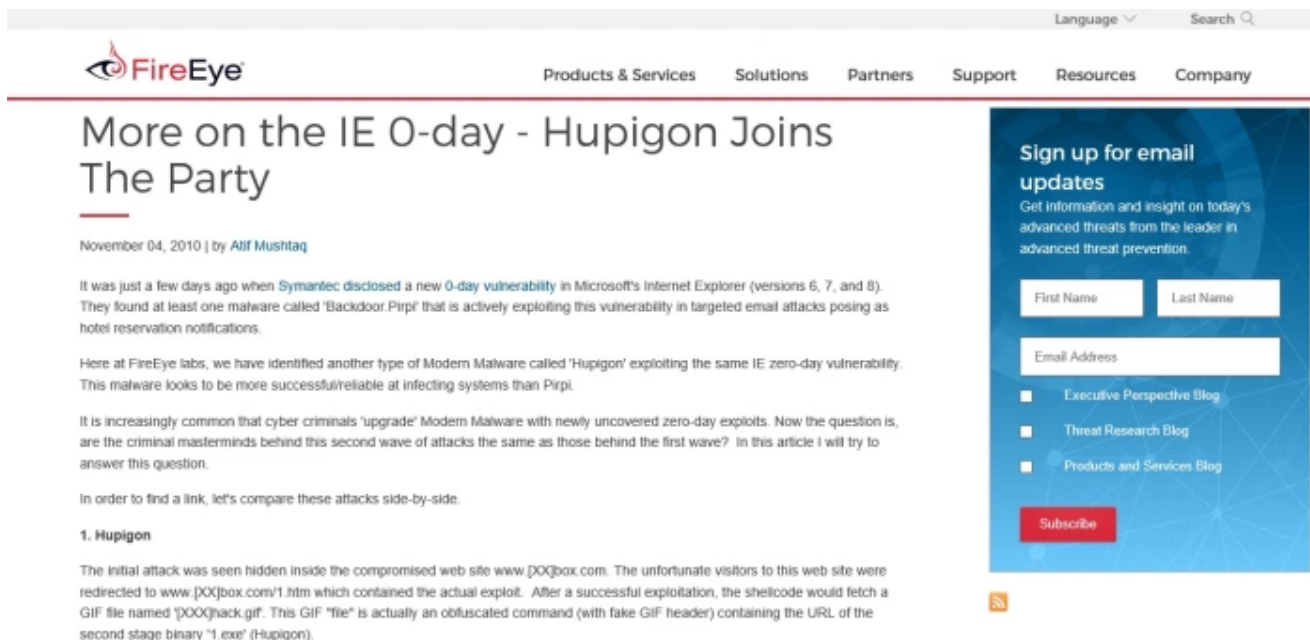
# Who is behind this Chinese espionage group stealing our intellectual property?

 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.



The screenshot shows a FireEye blog post. The header includes the FireEye logo and navigation links: Products & Services, Solutions, Partners, Support, Resources, and Company. The article title is "More on the IE 0-day - Hupigon Joins The Party" by Alif Mushtaq, dated November 04, 2010. The text discusses a new 0-day vulnerability in Microsoft's Internet Explorer (versions 6, 7, and 8) and identifies a type of Modern Malware called 'Hupigon' that exploits this vulnerability. It mentions that Hupigon is more successful than Pirpi and that cyber criminals are upgrading their malware with newly uncovered zero-day exploits. The article is part of a series comparing these attacks side-by-side.

**1. Hupigon**

The initial attack was seen hidden inside the compromised web site www [XX]box.com. The unfortunate visitors to this web site were redirected to www [XX]box.com/v1.htm which contained the actual exploit. After a successful exploitation, the shellcode would fetch a GIF file named [XX]hack.gif. This GIF "file" is actually an obfuscated command (with fake GIF header) containing the URL of the second stage binary '1.exe' (Hupigon).

On the right side of the screenshot, there is a "Sign up for email updates" form with fields for First Name, Last Name, and Email Address, and a "Subscribe" button. Below the form are three checkboxes for "Executive Perspective Blog", "Threat Research Blog", and "Products and Services Blog".

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.

Security Response

+4  
4 Votes

Please take a minute to complete our Security Response survey. [Click here.](#)

## Buckeye cyberespionage group shifts gaze from US to Hong Kong

Several organizations in Hong Kong are being targeted by a cyberespionage group known as Buckeye.

By: **Symantec Security Response** SYMANTEC EMPLOYEE

Created 06 Sep 2016 0 Comments : 简体中文, 繁體中文, 日本語

0 107 0 0 0

Buckeye (also known as APT3, Gothic Panda, UPS Team, and TG-0110) is a cyberespionage group that is believed to have been operating for well over half a decade. Traditionally, the group attacked organizations in the US as well as other targets. However, Buckeye's focus appears to have changed as of June 2015, when the group began compromising political entities in Hong Kong. Since March 2016, the group has appeared to mostly focus on organizations in Hong Kong, sending malicious emails to targets as recently as August 4, and attempting to spread within compromised networks in order to steal information.

Using the combined threat intelligence of Symantec and Blue Coat Systems, we have built a clear and concise picture of how Buckeye has evolved its tactics in recent years. This has allowed us to further enhance our protection capabilities against the group's campaigns.

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.