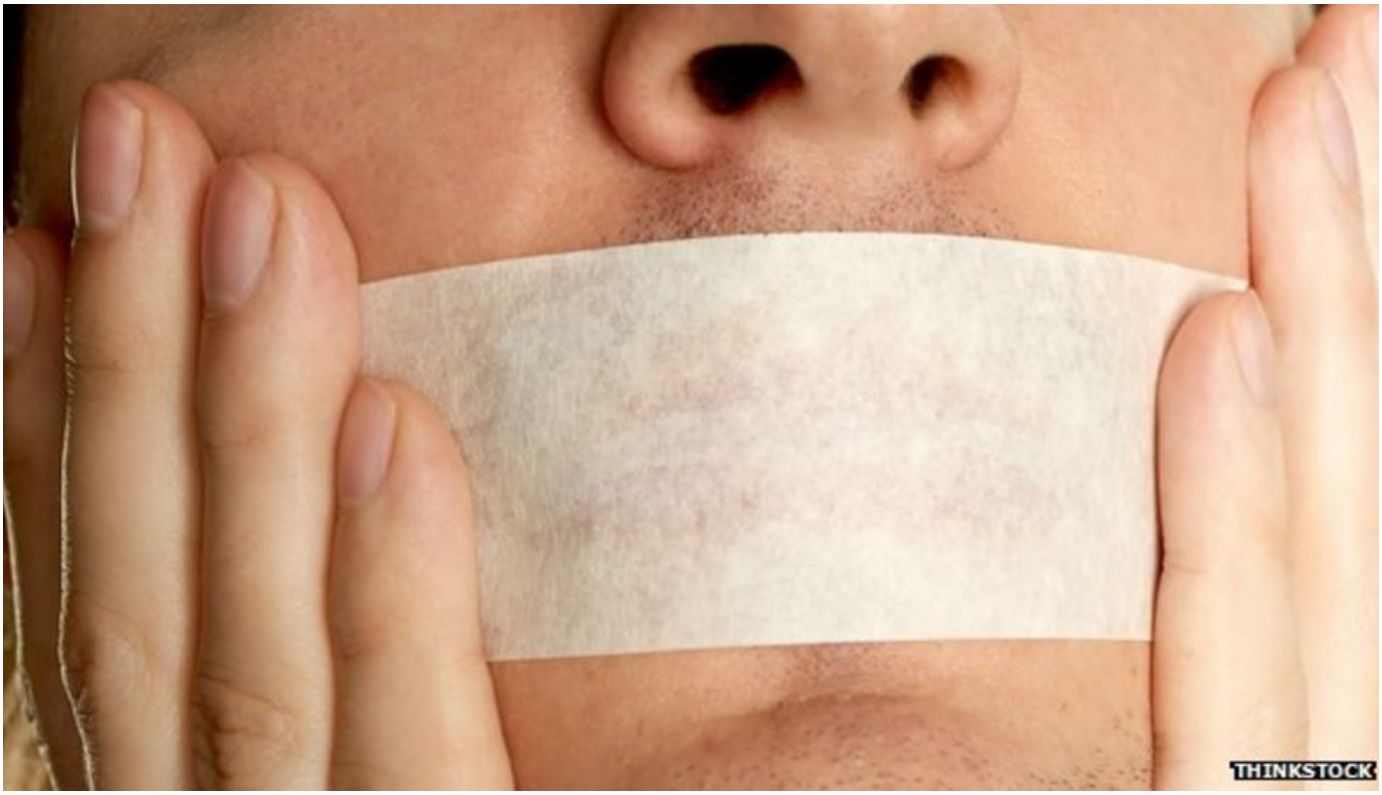
The Comment Group: The hackers hunting for clues about you

By Dave Lee
Technology reporter, BBC News

12 February 2013



Clues given out by employees of companies being targeted by hackers are being used to gain access

If you had an email that looked like it was from your boss asking how your recent holiday went, would you open it? Most probably - and hackers know it.

One group in particular has used this simple technique to devastating effect, using it to spy on some of the world's biggest corporations. But who are they, and what are they looking for?

When security experts looked into some of the highest profile hacks in recent years - one particular criminal group kept on coming to their attention.

The Comment Group, which industry insiders say is based in China, offer hacking for hire - be it for individuals, corporations or governments.

It got its name from what was once its trademark technique - implanting dodgy links to malicious malware within the comments sections of popular websites.

But more recently, the Comment Group has become known for being particularly adept in one other important discipline of hacking: straightforward research.

"They find the weakest link in the company," explains Jaime Blasco, from security specialists Alienvault.

"What they do is collect intelligence about the companies,"

"They try to find information from the internet, from other employees, from intranets, from Google… whatever."

Nuclear attack

It is an approach that has been devastatingly effective.

The group has been credited as being behind a vast range of attacks - everything from gaining access to user accounts at the EU to, according to Bloomberg, targeting a nuclear power plant that was situated near to a fault line.

In a document published by Wikileaks, the US government regarded the Comment Group - which it referred to as Byzantine Candor - as being one of the most serious of all hacking threats originating from China.

One of the leaked diplomatic cables referred to one attack via email on US officials who were on a trip in Copenhagen to debate issues surrounding climate change.

"The message had the subject line 'China and Climate Change' and was spoofed to appear as if it were from a legitimate international economics columnist at the National Journal."

The cable continued: "In addition, the body of the email contained comments designed to appeal to the recipients as it was specifically aligned with their job function."

Soft drinks

One example which demonstrates the group's approach is that of Coca-Cola,

which towards the end was revealed in media reports to have been the victim of a hack.

And not just any hack, it was a hack which industry experts said may have derailed an acquisition effort to the tune of $2.4bn (£1.5bn).

The US giant was looking into taking over China Huiyuan Juice Group, China's largest soft drinks company - but a hack, believed to be by the Comment Group, left Coca-Cola exposed.

The Coca-Cola hack had all the hallmarks of the Comment Group

How was it done? Bloomberg reported that one executive - deputy president of Coca-Cola's Pacific Group, Paul Etchells - opened an email he thought was from the company's chief executive.

In it, a link which when clicked downloaded malware onto Mr Etchells' machine. Once inside, hackers were able to snoop about the company's activity for over a month.

The Chinese government binned the acquisition soon after - citing competition concerns.

Coca-Cola has not officially commented on the hack. In a statement, the company told the BBC: "Our Company's security team manages security risks

in conjunction with the appropriate security and law enforcement organizations around the world.

"As a matter of practice, we do not comment on security matters."

But Alienvault's Mr Blasco explained how the attack was typical of the Comment Group's style.

"This Comment Group has been targeting a lot of companies that were in the process of being acquired or that a US company was trying to acquire in China," he said.

"I have seen that in dozens of industries. They are trying to gain access to financial information, and also they are compromising not only the companies but all the third parties, like lawyers, that are helping that company."

Those third parties could include anyone with even the loosest connection to the company under attack.

This month's revelation by the New York Times that it had been hacked bore many of the Comment Group's hallmarks.

It happened, the newspaper said, just as journalists were planning a major piece on the former Chinese premier, Wen Jiabao.

Highly organised

When you hear someone describing the Comment Group, it sounds like almost like any other firm, with groups of employees all assigned to different crucial bits of the business.

But rather than accounts, HR and sales - the Comment Group's components are designed to maximise efficiency in stealing information, Mr Blasco says.

"They have the guys working on exploits, you have the guys that are changing or programming the malware to gain access to the systems, and then you have the guys that are the operators.

"They don't know a lot about computers, what they do is operate the malware - they try to find the specific information, they collect intelligence from the victims and save that information for whatever purpose."

But it's in the research department where the Comment Group really stands out.

"They're looking really for any snippets of information that will give them and initial foothold in their target organisation," explained David Emm, a senior researcher for Kaspersky Lab.

"Now instantly that puts in the frame anybody in an organisation who is publicly facing - because they're the ones who tend to generate more snippets of information out there."

Mr Emm said that the real skill in all this is to make messages as natural and authentic as possible, with real-world cues to suck in the victim.

Anyone with even the smallest bit of computing experience will know to steer clear of your typical lazy spam - the cliched "Nigerian Prince" is not fooling anyone anymore.

"We all face spam," Mr Emm told the BBC.

"They're an irritation - and you're not going to do anything with it except junk it. But actually, if it's come from somebody who's trusted - then you are more likely to take it seriously.

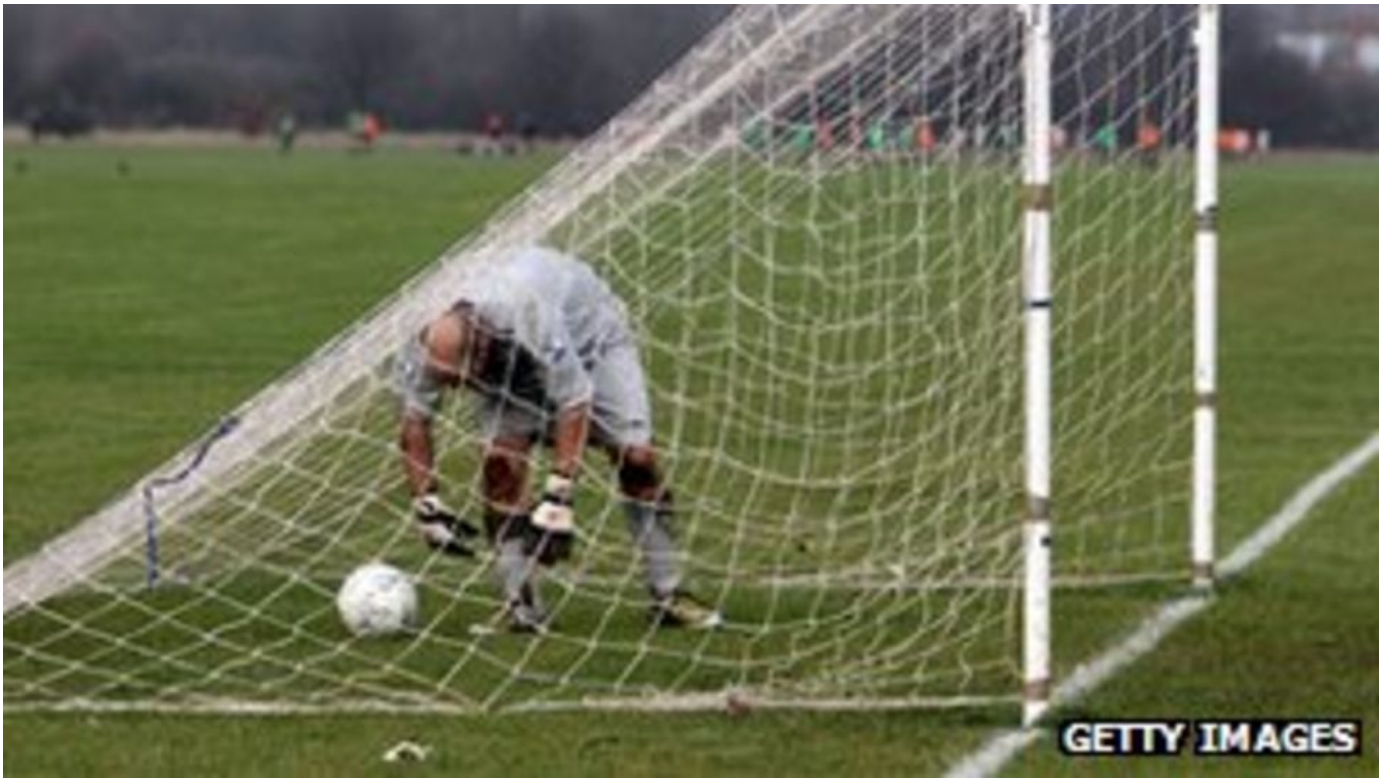
"If it doesn't look like a routine piece of spam, but it looks like John in the IT department and he's doing a random check, I'm more likely to respond to it."

Down by the waterhole

Mr Emm also detailed another disturbing tactic utilised by the Comment Group, and others, which is very hard to defend against.

"It is known as waterholing," he explained. "Which basically involves trying to second guess where the employees of the business might actually go on the web.

"If you can compromise a website they're likely to go to, hide some malware on there, then whether someone goes to that site, that malware will then install on that person's system."



Even being part of a local football league could leave employees open to attack

These sites could be anything from the website of an employee's child's school - or even a page showing league tables for the corporate five-a-side football team.

"If that's known, they're known to be in a league in a particular region, then an attacker can compromise a website they visit about that."

With such intricate attack strategies, it poses as huge problem for companies trying to defend themselves from harm.

Mr Emm said he believed that more needs to be done to show employees how to be diligent.

"One of the issues is that within business, maybe we don't take awareness seriously," he said.

"It's not like training - it's more akin to how we educate our children about crossing the road or staying safe. You don't want them to always approach crossing the road with the same routine.

"You want to actually have a road safety mindset which makes them think about roads coming in different shapes and sizes - but actually they're aware of what to look for.

"It's the same with security."

Top Stories

Biden addresses the US on Afghanistan

The US president is expected to defend the Afghanistan pull-out in his speech.

20 August

Reprisals cast doubts over the Taliban's amnesty

2 hours ago

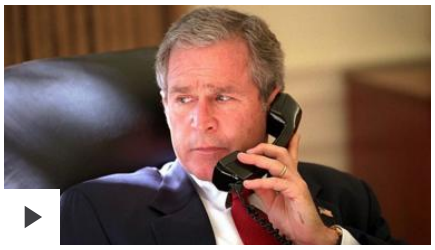
Thousands leave as fire closes in on Lake Tahoe

3 hours ago

Features

Elizabeth Holmes: The boss accused of duping Silicon Valley

The students amassing degrees to stay in Europe



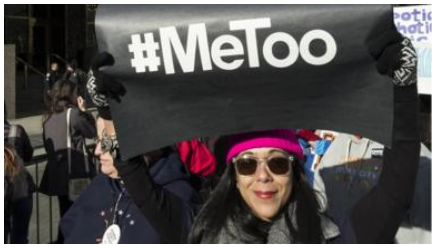
From Bush to Biden: One war, four US presidents

Fleeing the Taliban over land into Pakistan

The para-athlete taking tornado kicks to Tokyo

BBC Travel: In the steps of history's forgotten explorers

The musicians who became Instagram stars in pandemic



Can apps move the #MeToo movement forward?

Covid crisis causes fury in Aboriginal communities

Elsewhere on the BBC

Football phrases

15 sayings from around the world

Most Read

Cars plunge into hole after deadly road collapse 1

Thousands leave as fire closes in on Lake Tahoe 2

'If you let go, I'll shoot you in the face' 3

Sarah Rainsford: My last despatch before Russian expulsion 4

Reprisals cast doubts over the Taliban's amnesty 5

BBC News Services

On your mobile

On smart speakers

Get news alerts

Contact BBC News

Home | News | Sport | Reel | Worklife | Travel | Future | Culture | Music | TV | Weather | Sounds

Geronimo the alpaca killed as legal row ends 6

Elizabeth Holmes: The boss accused of duping Silicon Valley 7

Irish population tops 5m for first time since 1851 8

Afghanistan: What was left behind by US forces? 9

Naked Attraction bus campaign to end 10