dirty email trick favored by the nastiest hackers

# Spearphishing: The dirty email trick favored by the nastiest hackers

HACKERS
5 charged in 'largest hacking and data breach scheme' bust in US

INTERNET
Google Doodle honors Rosalind Franklin, DNA photographer

MICROSOFT
Game on for surveillance? Privacy advocates concerned over new consoles

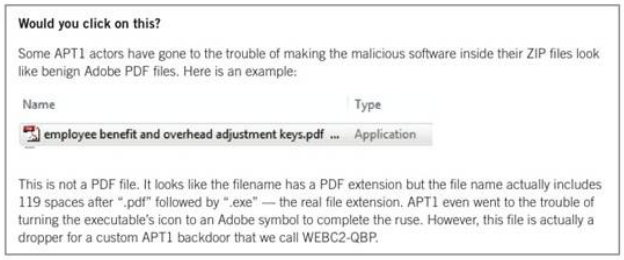
TECHNOLOGY
Pre-caffeine tech: Facebook millions, kneel before Zod!

CONSUMER
Watch out for the 'Change My Address' scams

ART

**Suzanne Choney, NBC News**

Feb. 19, 2013 at 3:06 PM ET




Mandiant Corp.

Just one of the examples of a spearphishing attempt cited in a new report from Mandiant Corp. "APT1" refers "Advanced Persistent Threat," and is Mandiant's name for the Chinese hackers involved in this attempt.

A **new report** says that the Chinese military is secretly obtaining sensitive data from U.S. companies. A key technique is "spearphishing," an approach that tricks a targeted individual to reveal information that can be used to infiltrate the company or government agency that person works for.

Security companies have been warning about spearfishing for the last two to three years, and its use is increasing. But now that it has become top news, thanks to a **report** from U.S. computer-security firm Mandiant Corp. explaining how Chinese operatives tricked workers at Coca-Cola and other major American firms, what is at the top of many people's minds is this: How do you know if you're being spearphished?



## Different than phishing

You probably know to watch out for phishing attempts — broad, massive email efforts to get you to hand over personal financial information like a credit card number or to click on a website link that could allow malware to steal information from your computer. They're usually riddled with spelling errors and terrible formatting.

Spearphishing is subtler, because it's aimed at intelligence gathering. It "often takes the form of key personnel inside an organization being emailed a malicious file," Graham Cluley of **Sophos Security** told NBC News Tuesday.



"It could be, for instance, a boobytrapped PDF file or Word document which when opened — secretly and silently installs spyware onto your computer," he said. "The malicious spyware code can then open a backdoor on your computer, giving hackers remote access to all

the files on your computer, as well as capture every keystroke, in order to steal passwords, and read everything on your screen."

But why would an employee open such an email? The information in the email is crafted to look and sound just right enough so that it's "remarkably easy to dupe someone into clicking on a link or opening an attachment in an email and for their computer to become compromised," Cluley said.

"Imagine you were a reporter covering human rights abuses in China. I simply send you an email (with a boobytrapped attachment), forge my 'from' address so you believe that the email has come from a human rights group, and in the body of the email tell you that attached you'll find shocking details of human rights abuses in China."

"Similarly, if you were a military supplier, I might make my email appear as though it came from a sister company or another supplier."

Dave Jevans, founder and CTO of **Marble Security**, said "spearphishers know that the easiest way to break into a company's network is not to breach their firewalls and intrusion prevention systems, but rather to compromise an employee's computer, smartphone or online passwords."

Employees who use cloud-based, shared document apps like Google Docs can be sitting ducks for spearphishing attempts.

"Google Docs is a very convenient way to fool employees or end users into divulging passwords," Jevans said. For one thing, it is a "trusted website that won't be blocked by Web filters," with invitations to view documents or forms "hosted by a trusted company — Google — not some hacked server in Russia." Also, he said, "Google Docs connections are HTTPS encrypted, and cannot be filtered by Web-filtering gateways to scan for malicious content."

**No easy fix**

Battling spearphishing is an ongoing effort, with no easy-fix solutions in sight.

"It's a massive problem," Kurt Baumgartner, Kaspersky Lab senior researcher, told NBC News Tuesday. Jevans, of Marble Security, called spearphishing "one of the most dangerous of all the advanced persistent threats" that exist.


TRIDENT D-5 MISSILE TECHNICAL REPORT From:
Subject: TRIDENT D-5 MISSILE TECHNICAL REPORT
From:
To:
Date: 2010-06-23 17:21:25
Dear all,
Attached Trident D-5 Missile Explosive Propellant Hazards.
(Please note that this summary does not discuss the conventional explosive material inside the Trident w76 and w88 nuclear warheads, which is an additional hazard.This previously unpublished report was prepared in support of our environmental lawsuit against the Trident D-5 missile upgrade at Bangor, filed in federal court on June 11,2009)

Sophos Security
Spearphishing email intercepted by Sophos Security.

In 2010, Sophos Security said it **intercepted an attack** against a firm tied to the defense indutry in which emails "carried a malicious PDF file claiming to be about the Trident D-5 missile, launched from nuclear submarines."

A report from McAfee Labs at the end of 2011 noted the worrisome rise in spearphishing, saying the problem "doesn't really lend itself to

a pure technology solution. The best defense against spearphishing is employee — particularly executive employee — education. Next-generation firewall technology can also help prevent employees from accessing rogue sites."

Baumgartner told NBC News on the "human side, the old adage 'do not open suspicious emails or links,' is, well, old. While it's sensible advice, it's proven to be ineffective because you are dispensing that advice to people." And people, of course, don't always pay close enough attention.

Security vendors, he said, "have improved their product capabilities as well," but still, "the attackers sometimes up their game to beat all of those technologies. So you can stop 'it,' but at some level you can't always stop 'it.'

"For some organizations and targets, learning how to best tolerate and maintain intrusions becomes an attractive option," he said. Tools to expel invaders, or minimize exposure once they are in, may prove to be more important than just relying on "defensive technology protecting against spearphishing components," he said.

Cluley, of Sophos, says companies and agencies can "reduce the chances of a targeted attack" being successful by keeping software such as PDF readers, Web browsers, word processing software and the computer's operating system itself as up-do-date as possible, with the latest patches.

"Furthermore, you should run a layered defense — that means not just using up-to-date anti-virus software, but also firewalls, email filtering technologies, data-loss protection technology and strong encryption to secure your most sensitive data," he said.

And back to that human element?

"Also, it's amazing how many people re-use passwords, and use the same weak password in multiple places," Cluley said. "That means if you get hacked in one place, and your password is compromised, it may also unlock accounts elsewhere on the Net."

All of these steps "can reduce your chances of suffering from a targeted attack," he said. "But ultimately, there's no 100 percent technological solution, as human beings can still make bad decisions. And that's why it's important to train users about threats, and warn them to be suspicious of unsolicited links and attachments and to always report suspicious activity."




**Video:** The explosive allegations that a branch of the Chinese military is reaching into American life by robbing our computers blind is the kind of computer espionage and electronic warfare we've been warned about. NBC's Andrea Mitchell spoke with Kevin Mandia, the Founder and CEO of Mandiant, who said, 'It was time to let the world know it's actually not just from China --it's the Chinese government that's sanctioning these attacks.'




**Video:** A new report confirmed by U.S. intelligence officials has pinpointed a building in Shanghai where those working for the Chinese military launched cyberattacks against 141 US companies spanning 20 industries. NBC's Andrea Mitchell reports.

*Check out Technology, GadgetBox, Digital Life and In-Game on* **Facebook**, *and on* **Twitter**, *follow Suzanne Choney.*

Security | email | China | spearphishing | phishing | attack | threat





RELATED STORIES

**US looking at action against China cyberattacks**

**China tightens Internet controls, legalizes post deletion**

**2012: The year malware surged 'dramatically'**