The “HawkEye” attack: how cybercrooks target small businesses for big money

nakedsecurity.sophos.com/2016/02/29/the-hawkeye-attack-how-cybercrooks-target-small-businesses-for-big-money/

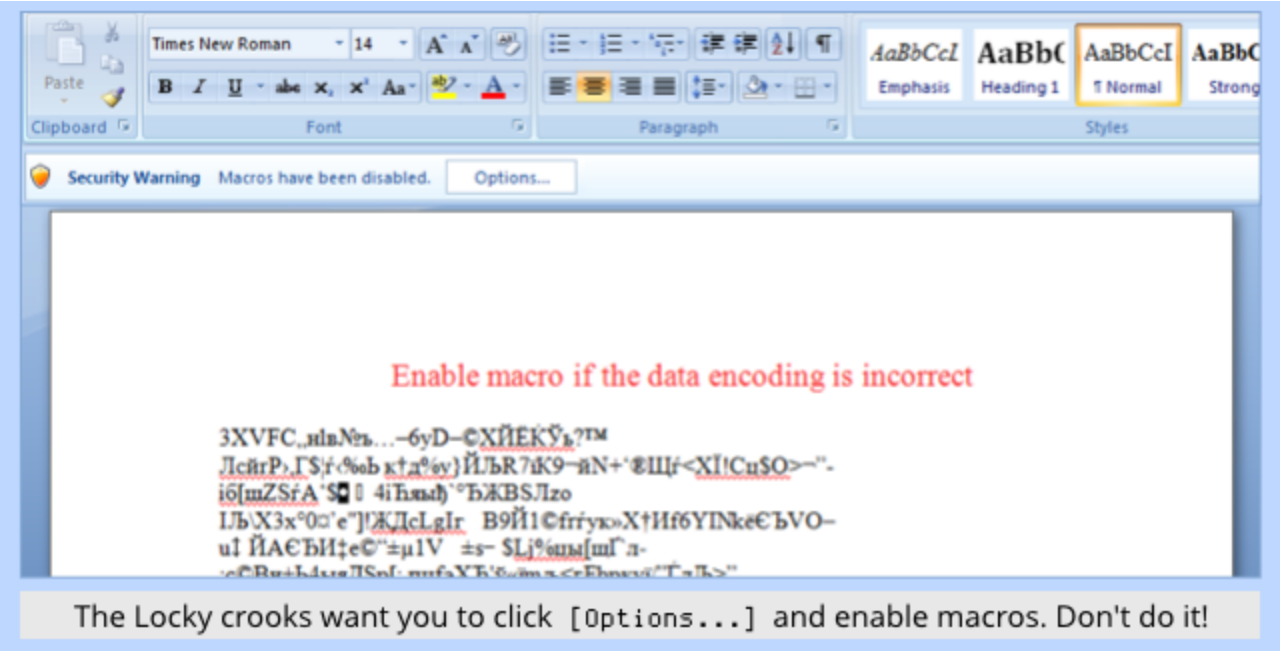
By Paul Ducklin 29 Feb 2016

SophosLabs researcher and regular Naked Security contributor Gabor Szappanos (Szapi) has recently being reviewing the past year’s worth of attack data relating to Microsoft Word document exploits.

He wanted to look at how this branch of cybercriminality has been evolving, and where it’s likely to go in 2016.

To explain: Word document exploits are different to the sort of attack documents you’re probably familiar with from ransomware campaigns.

The recent wave of Locky ransomware attacks, for example, generally relied on sending you a document that contained macros (embedded document programs written in Visual Basic for Applications, or VBA), and asking you to enable macros.



That's a dangerous thing to do, which it why we advise you, "Never do it!", but if you fall for it, you have effectively authorised malware to run, even if you are fully patched.

Word document exploits, on the other hand, generally rely on you being unpatched, but once you've opened a booby-trapped document, it's already too late.

And, let's face it, just opening a document isn't supposed to be dangerous, so you can understand why people take the chance.

The danger comes from missing patches that allow crooks to create cunningly-malformed files that crash your Word application and leave them in temporary programmatic control of your computer.

The booby-trapped document then takes advantage of this temporary control to download and install an item of malware chosen by the crooks.

Flying under the radar

If you are trying to infect as many people as possible to make $200 off each of them as soon and as visibly as you can, you don't have to behave with any subtlety once you're in.

Indeed, ransomware deliberately draws attention to itself once it's activated, by way of encouraging you to pay up.

But if your goal is to tread more softly – to "fly under the radar," as it were – in the hope of infecting just a handful of people from whom you then patiently attempt to steal $200,000 or more at a time, a less in-your-face approach works better.

In other words, you don't draw attention to yourself or to the malware you've implanted at all.

The Hawkeye attack

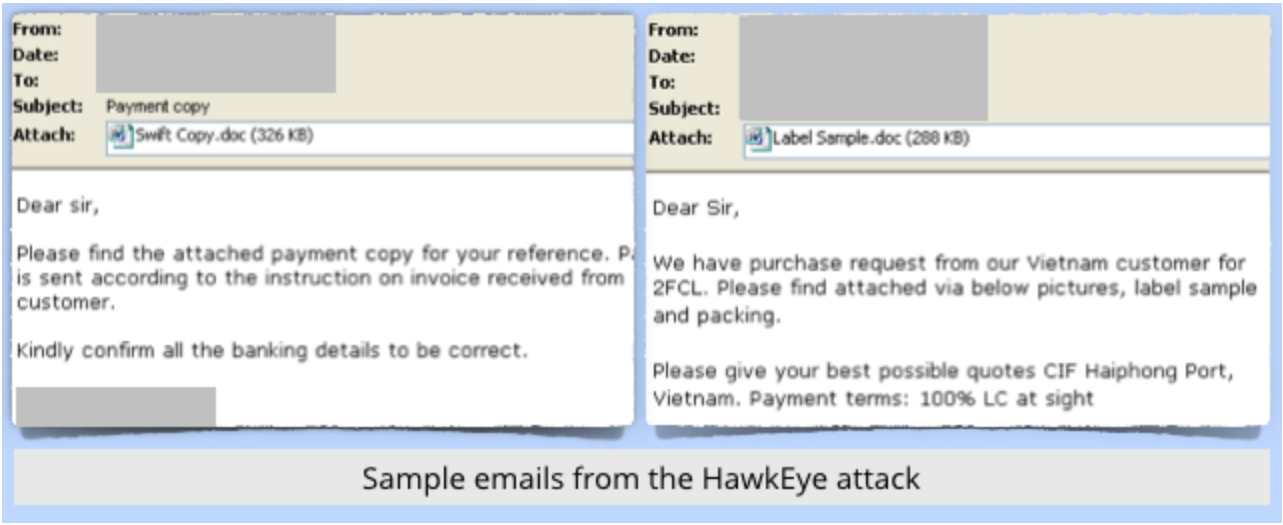
One attack that Szapi thought made for educational reading is known as *Hawkeye*.

Even if you've heard of it before, it's still worth reminding yourself how the scam works, which is something like this:

- **Buy booby-trapped documents that use the Microsoft Word Intruder (MWI) exploit tool.** If opened on an unpatched version of Windows, these documents automatically install chosen malware on the victim's computer, with no user clicks required.
- **Buy a commercially-available keylogger and configure the booby-trapped files to download and install it.** (This case used the now-defunct Hawkeye keylogger.)

HawkEye configurator showing the range of data that the keylogger can search and steal

- **Pick a broad industry sector**, e.g. leather and leather products.
- **Send a small number of scam emails** (typically a few thousand in total) pretending to be quotation requests or payment information, each containing a booby-trapped MWI document.



Sample emails from the HawkEye attack

- **Infect victims with the keylogger** and wait until they type in their email passwords.
- **Use the stolen email passwords to watch their inboxes**, until you see that a customer has been invoiced and is about to pay.

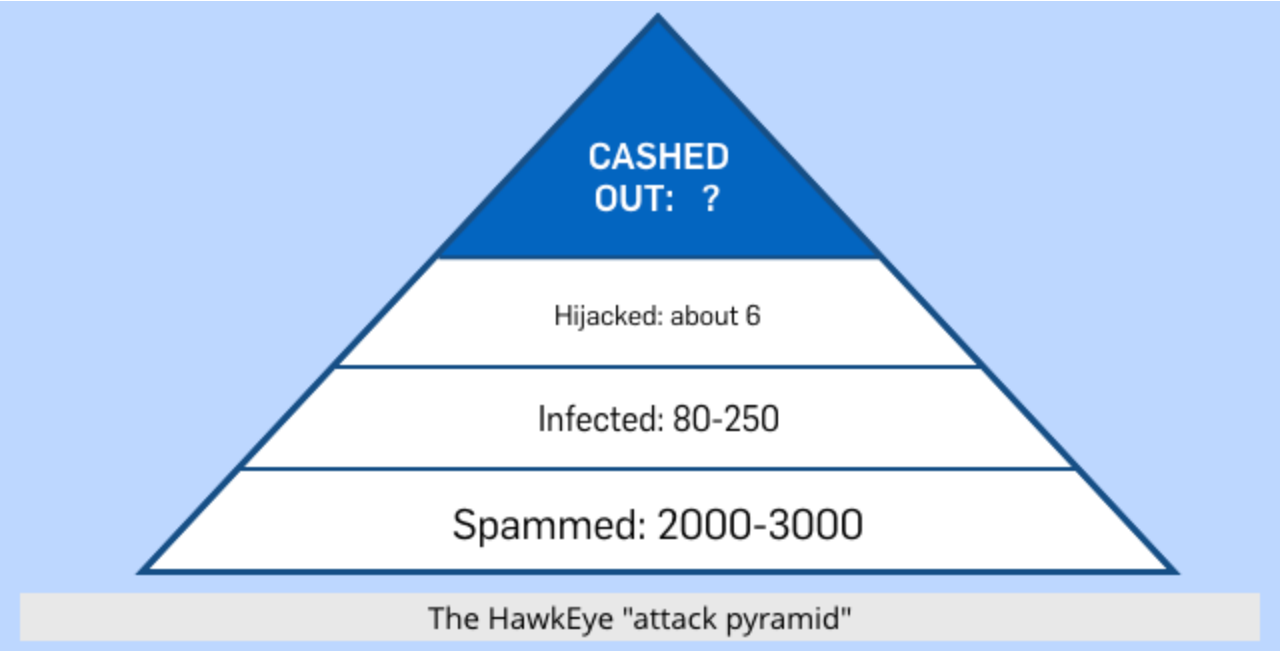
Example text log uploaded by HawkEye during operation

- **Email the customer from the hijacked account**, instructing the customer to use a new account number for future payments.
- **Take the money yourself** and quickly move it where it can't easily be found or recovered.

Unlike ransomware campaigns where the crooks aim to make millions of dollars out of hundreds of thousands of victims, $100-$400 at a time, this sort of attack works as a sort of reversed pyramid, where very low attack volumes are needed at each level of the pyramid.

As Szapi describes:

> In the first campaign, the crooks sent out about five waves of spam with the malicious Word document. Each wave had about 500 targets. The infection statistics show that as a result of this spam they ended up with 80-150 infected computers.
>
> From these infected victims, the crooks went on to identify at least six victims whom they followed up with payment hijacking messages. They chose cutomers with high-value unpaid invoices, ranging from $200,000 to $900,000.
>
> We don't know the success rate of the attempted payment hijacks. But even if only one hijack succeeded (a reasonable assumption because they continued in this vein with eight campaigns over several months), that's a huge return.



The HawkEye "attack pyramid"

Worst of all, this is effectively a high-tech crime available to low-tech criminals.

They bought in the necessary booby-trapped documents; bought in the keylogger; paid someone to send very small quantities of spam; and then they settled down to carry out old-fashioned, targeted deception and fraud.

Just one or two criminals, working unaided, and with enough patience to go after a small number of high-value victims, could easily operate a scam of this sort.

And although it's easy to say, "As a debtor about to pay a huge invoice, I'd never fall for this sort of scam," remember that the email giving the updated remittance advice – the payment hijack itself – may very well come from the same person who sent you the company's account number when you first signed up as a customer.

That's one reason the crooks use the reversed pyramid approach described above.

They don't need to send payment hijack emails from every hacked email account, only from the email accounts that are likely to be believed by the recipients.

What to do?

- **Patch promptly.** The booby-trapped documents in this attack relied on a security hole that had been patched years before.
- **Keep your security software up-to-date.** A good anti-virus can block attacks like this at several points, and you win if you can stop any one of them, starting with the original inbound email.
- **Beware of unsolicited attachments.** This can be hard if your job is business development and the email is a Request For Quotation, but avoid opening just any old document.
- **Consider using a stripped-down document viewer.** Microsoft's own Word Viewer, for example, is usually much less vulnerable than Word itelf because it's much simpler. (It doesn't support macros, either, which protects against Locky-type attacks, too.)
- **If your email software supports it, use 2FA.** That's short for two-factor authentication, those one-time codes that come up on your phone on a special security token. With 2FA, just stealing your email password isn't enough on its own.
- **Have a two-person process for important transactions.** Paying large invoices and changing remittance advice shouldn't be too easy. Require separate approval from a supervisor, so you always get a second opinion when large sums are at stake.

LEARN MORE ABOUT 2FA

(Audio player above not working? Download MP3, listen on Soundcloud or access via iTunes.)